

Mayor
Melinda Bales

Mayor Pro Tem
Stacy Phillips

Commissioners
Dan Boone
Rob Kidwell
Amber Kovacs
Lance Munger
Derek Partee



Town Manager
Anthony Roberts

Deputy Town Manager
Jackie Huffman

Assistant Town Manager
Bobby Williams

Town Attorney
Emily Sloop

Town Clerk
Janet Pierson

AGENDA
Regular Town Board Meeting
August 7, 2023 - 6:00 PM
TOWN HALL (101 Huntersville-Concord Road)

Live Stream available via YouTube
@townofhuntersvillenc28078

- 1. Pre-meeting - 5:30 p.m.**
 - 1.A. Public Records and Social Media Policy. *(Emily Sloop)*
- 2. Call to Order**
- 3. Invocation/ Moment of Silence**
- 4. Pledge of Allegiance**
- 5. Staff Questions**
- 6. Public Comments, Requests, or Presentations**
- 7. Agenda Changes/Adoption of Agenda**
- 8. Consent Agenda**
 - 8.A. Adopt Ordinance to temporarily close certain state-maintained roads for the Veterans Day Parade and Event. *(Michael Jaycocks)*
 - 8.B. Approve Tax Collector's Settlement for Fiscal Year 2023 (Tax Year 2022) and adopt Order of Collections for Fiscal Year 2024 (Tax Year 2023). *(Pattie McGinnis)*
 - 8.C. Approve budget amendment recognizing grant revenue received from the North Carolina Recreation and Park Association in the amount of \$2,856 and appropriate to Parks & Recreation Training to provide for four Parks & Recreation employees to complete a Diversity, Equity & Inclusion Certification through UNC-Charlotte. *(Tracy Houk)*

- 8.D. Ratify previous action of the Town Board taken in Closed Session allowed under the North Carolina Open Meetings law to award a 2 percent merit increase effective August 1, 2023, and a \$10,000 bonus for the Town Manager based on market analysis and performance evaluation. (*Mayor Bales*)
- 8.E. Award contract for underground and directional boring services for FY24 to Lamberts Cable Splicing, LLC. (*David Lucore*)
- 8.F. Approve Huntersville Police Dispatch contract with Charlotte-Mecklenburg Police Department. (*Chief Barry Graham*)
- 8.G. Call a public hearing for Tuesday September 5, 2023 at 6:00 P.M. at Huntersville Town Hall, 101 Huntersville-Concord Road, Huntersville, NC, on Petition #R23-08, Dearness Gardens, a request by Ken Forster, to rezone six parcels totaling +/- 10.07 acres generally located at 13501 Old Statesville Road from existing Highway Commercial - Conditional District and Neighborhood Residential to Highway Commercial - Conditional District and Neighborhood Residential for boundary and site amendments. (*Jesse James*)
- 8.H. Call a public hearing for Tuesday, September 5, 2023 at 6:00 p.m. at Huntersville Town Hall, 101 Huntersville-Concord Road, Huntersville, NC, on Petition #R23-09, Golden Cow, a request by H2H Holdings, LLC to rezone from the existing Town Center to Town Center - Conditional District for a one-story retail development. (*Jesse James*)
- 8.I. Call a public hearing for Tuesday, September 5, 2023 at 6:00 p.m. at Huntersville Town Hall, 101 Huntersville-Concord Road, Huntersville, NC 28078 to receive public input on traffic calming measures on Swansboro Lane. (*Lora Mastrofrancesco*)

9. Public Hearings

- 9.A. Conduct public hearing on Petition #R23-01, Beatties Ford Family Entertainment, a request by Jonathan Eury to rezone +/-2.513 acres generally located at the intersection of Beatties Ford Road and Broadway Street from Rural to Highway Commercial - Conditional District for indoor and outdoor recreation and commercial uses. (*Nathan Farber*)
- 9.B. Conduct public hearing on Petition #R23-07, EPCON – Beatties Ford Road, a request by EPCON Communities Carolinas, LLC to rezone six parcels totaling 78.7-acres generally located at 15201 Beatties Ford Road (South of NC 73 and east of Gilead Road & Beatties Ford Road intersection) from existing Rural to Transitional Residential - Conditional District zoning district for a 118-lot, single-family home subdivision. (*David Peete*)

10. Other Business

- 10.A. Consider adopting Resolution Order to Abandon and Close a Portion of Mt. Holly-Huntersville Road. (*Lora Mastrofrancesco*)
- 10.B. Consider approving purchase agreement for electric distribution substation property. (*David Lucore*)
- 10.C. Downtown social district discussion. (*Commissioner Dan Boone/Commissioner Amber Kovacs*)

11. Mayor and Commissioner Reports/Closing Comments

12. Adjourn

GENERAL MEETING INFORMATION

Town Board:

The Town of Huntersville Mayor and Board of Commissioners are elected for two-year terms. Huntersville operates under the council-manager form of government, which establishes the Town's policies that are carried out by the Town Manager and staff. For more information visit www.huntersville.org.

Meeting Time, Place and Agenda:

All meetings of the Board are open to the public and the public is invited and encouraged to attend. The Board meets in the Town Hall at 6:00 p.m. on the first and third Monday of each month (unless otherwise posted). Agendas are published Thursdays before the meeting on our website. The Board reserves the right to deviate from the agenda.

Public Comment and Public Hearing Policy:

Persons desiring to address the Board during the public comment period or a public hearing shall sign up via the speaker sign-up sheet prior to the beginning of the meeting. Once the meeting has begun, a person may not sign up to speak. Persons who have signed up to speak shall be allowed to speak for up to three (3) minutes. The Mayor shall have the discretion to shorten the allotted speaking time depending on the number persons registered to speak and in consideration of the length of the agenda. (Public Comment and Public Hearing Policy - Adopted April 19th 2021)

Special Accommodations:

Anyone needing special accommodations when attending this meeting and/or if this information is needed in an alternative format please contact the Town Clerk. The Clerk can be reached by phone or fax: 704-875-6541, email: clerk@huntersville.org or at 101 Huntersville-Concord Rd, Huntersville, NC 28078. We request at least 72-hours' notice prior to the meeting to make the appropriate arrangements.

**Town of Huntersville
Town Board
August 7, 2023**

To: Town Board

From: Emily Sloop, Town Attorney

Date: August 7, 2023

Subject: Public Records and Social Media Policy

EXPLAIN REQUEST:

The Board requested a discussion related to the public records and the Town's Social Media Policy for Elected Officials.

ACTION RECOMMENDED:

FINANCIAL IMPLICATIONS:

ATTACHMENTS:

1. Public Records and Social Media Policy Revised 7-28-23



Public Records and Social Media

Topics for Discussion

- Public Records
- Social Media Policy



Public Records

Public Records Defined

N.C.G.S. § 132-1. defines public records as:

"Public record" or "public records" shall mean all documents, papers, letters, maps, books, photographs, films, sound recordings, magnetic or other tapes, electronic data-processing records, artifacts, or other documentary material, **regardless of physical form or characteristics**, made or received pursuant to law or ordinance **in connection with the transaction of public business** by any agency of North Carolina government or its subdivisions. Agency of North Carolina government or its subdivisions shall mean and include **every public office, public officer or official (State or local, elected or appointed), institution, board, commission, bureau, council, department, authority or other unit of government of the State or of any county, unit, special district or other political subdivision of government.**



Limitations

N.C.G.S. § 132-6.2 contains the following limitations:

- Nothing in this section shall be construed to require a public agency to respond to a request for a copy of a public record **by creating or compiling a record that does not exist**...Nothing in this section shall be construed to require a public agency to put into electronic medium a record that is not kept in electronic medium.



Non-Public/Confidential Information

Certain information is non-public or confidential per statute, including:

- Information protected by attorney-client privilege and trial preparation materials
- Tax information, enterprise billing information, electronic payment account numbers
- Proprietary information (trade secrets, design work, computer code)
- Criminal intelligence information, 911 database, sensitive public security information
- Social security numbers and other personally identifying information
- Protected medical information
- Information contained in personnel files



Cost of Production – N.C.G.S § 132-6.2

N.C.G.S. § 132-6.2(b):

Except as otherwise provided by law, no public agency shall charge a fee for an uncertified copy of a public record that exceeds the actual cost to the public agency of making the copy....Notwithstanding the provisions of this subsection, if the request is such as to require extensive use of information technology resources or extensive clerical or supervisory assistance by personnel of the agency involved, or if producing the record in the medium requested results in a greater use of information technology resources than that established by the agency for reproduction of the volume of information requested, then the agency may charge, in addition to the actual cost of duplication, a special service charge, which shall be reasonable and shall be based on the actual cost incurred for such extensive use of information technology resources or the labor costs of the personnel providing the services.



Social Media Policy for Elected and Appointed Officials

Professional and personal conduct standards for social media use:

- Prohibits disclosure of privileged or confidential information.
- Prohibits using social media to violate federal, state, or local laws, including public records and open meetings laws.
- Prohibits using social media to engage in activity constituting conflict of interest.



Social Media Policy for Elected and Appointed Officials

Best Practices and Guidelines:

- Encourages separate personal and professional/official social media accounts.
- Exercise caution when making social media posts.
- Avoid using social media to communicate with Town employees.
- Avoid posts that could be perceived as endorsement by the Town, its employees, constituents, etc.



Social Media Policy for Elected and Appointed Officials

Policy Considerations:

- Social media posts by elected officials are considered public records if they relate to the transaction of Town business.
 - No distinction between posts made on personal vs. professional/official social media pages.
- Public records must be properly archived in accordance with the Records Retention Schedule.
- Assume everything you do on social media is public, including likes, liked pages, comments on other posts, etc.
- Recent increase in the number of public records requests.



Social Media Policy for Elected and Appointed Officials

Additional Policy Considerations:

- First amendment protections against “viewpoint discrimination” apply in government forums.
- Social media pages owned and maintained by governmental units to transact public business have been deemed electronic, government forums when public comments are allowed on the pages.
- First amendment protections do not apply to purely personal social media accounts of elected officials, but issues may arise if personal and official activity are intertwined on a single page or social media account.
- Pages more directly tied to campaign activities than to official business are also distinct.



Social Media Policy for Elected and Appointed Officials

- The Town Board enforces the Social Media Policy.
- Potential policy revisions:
 - Require separate official and personal social media accounts and pages.
 - Prohibit use of official title and contact information on personal social media accounts and pages.



QUESTIONS?



**Town of Huntersville
Town Board
August 7, 2023**

To: Town Board

From: Michael Jaycocks, Director of Parks and Recreation

Date: August 7, 2023

Subject: Ordinance - Temporary Road Closure

EXPLAIN REQUEST:

Adopt Ordinance to temporarily close certain state-maintained roads for the Veterans Day Parade and Event on Saturday, November 11, 2023.

ACTION RECOMMENDED:

Adopt Ordinance to temporarily close certain state-maintained roads for the Veterans Day Parade and Event.

FINANCIAL IMPLICATIONS:

N/A

ATTACHMENTS:

1. Veterans Day Road Closure Request 2023



**AN ORDINANCE TO TEMPORARILY CLOSE CERTAIN STATE-MAINTAINED
ROADS FOR A SPECIAL EVENT ORGANIZED BY
THE TOWN OF HUNTERSVILLE, NC**

WHEREAS, North Carolina General Statute 20-169 authorizes local authorities to regulate by ordinance the use of a highway within their jurisdiction by processions, assemblages or anything that may be construed as a procession or assemblage, and

WHEREAS, the Town of Huntersville will consult with the local NCDOT Division office to verify that a proposed event will not 1) interfere with other planned special events and 2) impact or be impacted by planned maintenance or other activities, and

WHEREAS, the Town of Huntersville will sponsor and hold its annual Veterans' Day celebration on November 11, 2023; and

WHEREAS, this event will require the temporary closing of 1) Old Statesville Rd (NC 115) between Mt. Holly-Huntersville Rd and Sherwood Dr. 2) Gilead Rd/Huntersville-Concord Rd between Sherwood Dr and Main St. 3) Maxwell Ave from Huntersville-Concord Rd to N. Old Statesville Rd (NC 115). 4) Main St between Huntersville-Concord Rd and Bigham St. will be closed from 9 a.m. – 11 a.m. 5) Maxwell Ave and Main St (between Huntersville-Concord Rd and Old Statesville Rd) to vehicular traffic from 9 a.m. – 1:00 p.m. on November 11, 2023. See map attached as reference.

NOW THEREFORE, BE IT RESOLVED AS FOLLOWS:

1. The Board of Commissioners approves and authorizes to temporarily close the above-mentioned town and state-maintained roads for a special event per the attached map.
2. The Board hereby authorizes the Town Manager, acting on advice of counsel, to take any actions necessary to affect the provisions of this Resolution;
3. This Resolution shall be effective as of the date its adoption.

Adopted this 7th day of August 2023.

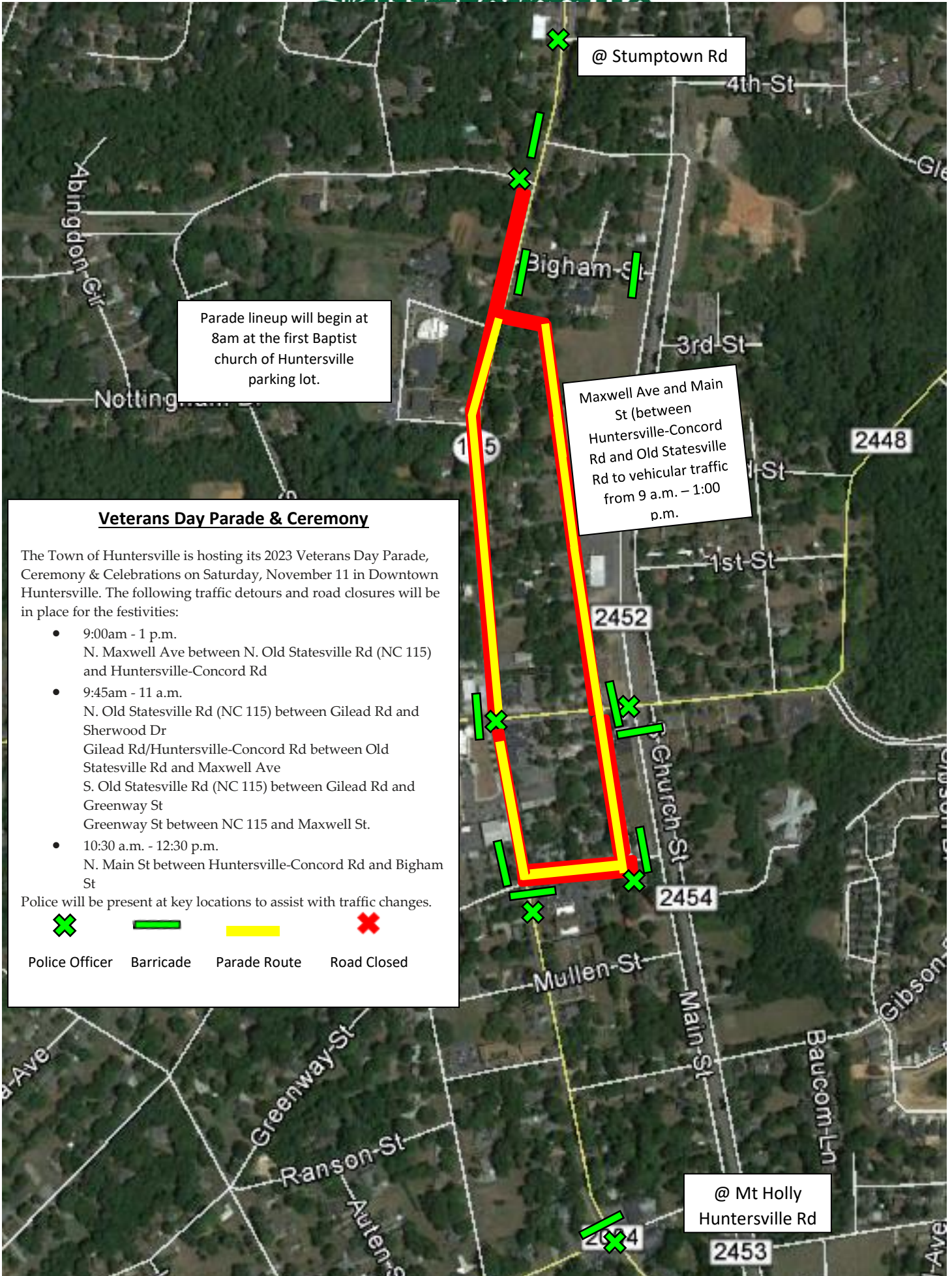
ATTEST:

TOWN OF HUNTERSVILLE

Town Clerk

Town Mayor

Town Attorney



Veterans Day Parade & Ceremony

The Town of Huntersville is hosting its 2023 Veterans Day Parade, Ceremony & Celebrations on Saturday, November 11 in Downtown Huntersville. The following traffic detours and road closures will be in place for the festivities:

- 9:00am - 1 p.m.
N. Maxwell Ave between N. Old Statesville Rd (NC 115) and Huntersville-Concord Rd
- 9:45am - 11 a.m.
N. Old Statesville Rd (NC 115) between Gilead Rd and Sherwood Dr
Gilead Rd/Huntersville-Concord Rd between Old Statesville Rd and Maxwell Ave
S. Old Statesville Rd (NC 115) between Gilead Rd and Greenway St
Greenway St between NC 115 and Maxwell St.
- 10:30 a.m. - 12:30 p.m.
N. Main St between Huntersville-Concord Rd and Bigham St

Police will be present at key locations to assist with traffic changes.



Police Officer

Barricade

Parade Route

Road Closed

@ Stumptown Rd

Parade lineup will begin at 8am at the first Baptist church of Huntersville parking lot.

Maxwell Ave and Main St (between Huntersville-Concord Rd and Old Statesville Rd) to vehicular traffic from 9 a.m. - 1:00 p.m.

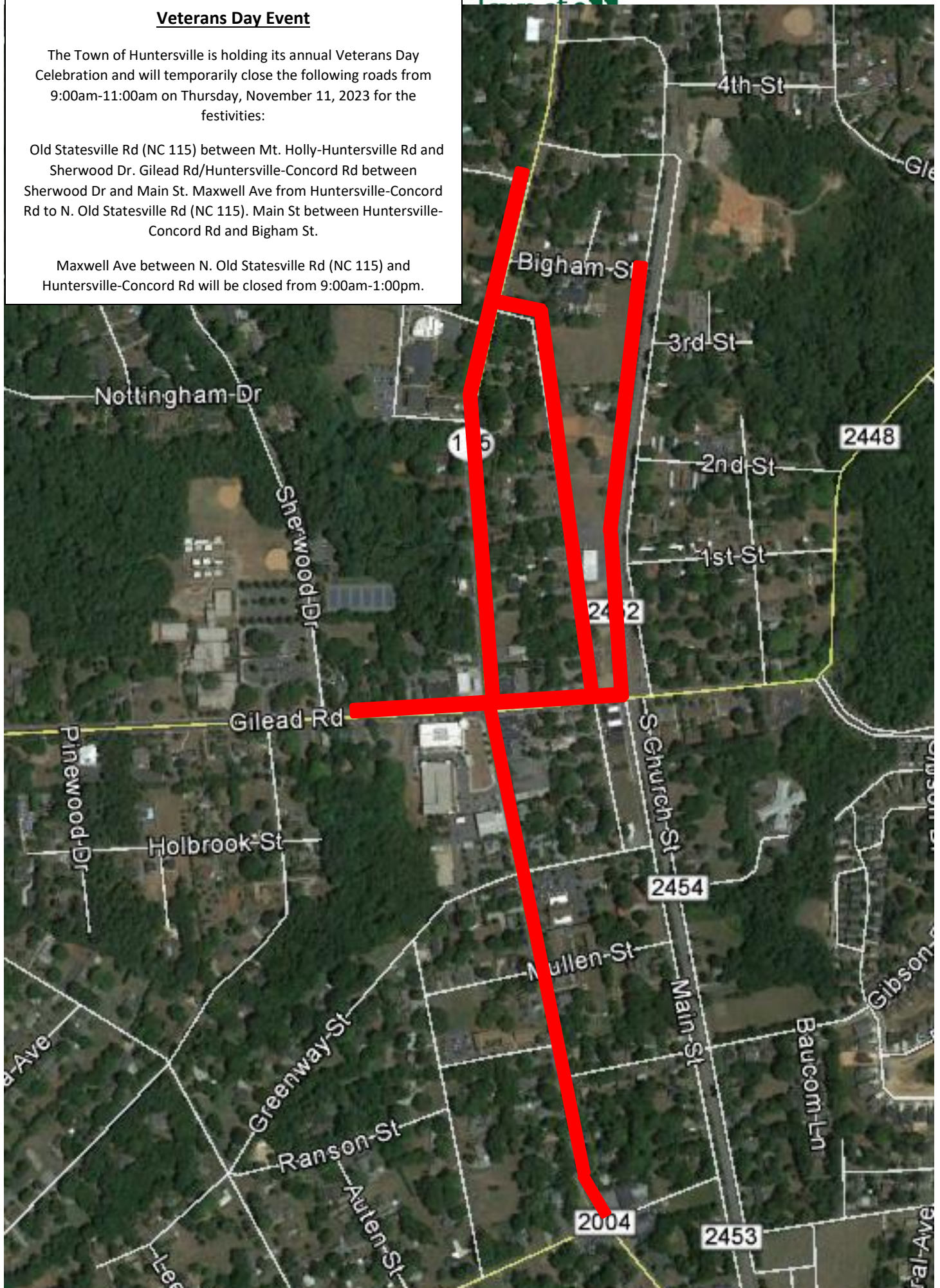
@ Mt Holly
Huntersville Rd

Veterans Day Event

The Town of Huntersville is holding its annual Veterans Day Celebration and will temporarily close the following roads from 9:00am-11:00am on Thursday, November 11, 2023 for the festivities:

Old Statesville Rd (NC 115) between Mt. Holly-Huntersville Rd and Sherwood Dr. Gilead Rd/Huntersville-Concord Rd between Sherwood Dr and Main St. Maxwell Ave from Huntersville-Concord Rd to N. Old Statesville Rd (NC 115). Main St between Huntersville-Concord Rd and Bigham St.

Maxwell Ave between N. Old Statesville Rd (NC 115) and Huntersville-Concord Rd will be closed from 9:00am-1:00pm.



**Town of Huntersville
Town Board
August 7, 2023**

To: Town Board

From: Pattie McGinnis, Finance Director

Date: August 7, 2023

Subject: Tax Collector's Settlement and Order of Collections

EXPLAIN REQUEST:

Approve Tax Collector's Settlement for Fiscal Year 2023 (Tax Year 2022) and adopt Order of Collections for Fiscal Year 2024 (Tax Year 2023).

ACTION RECOMMENDED:

Approve Settlement and adopt Order of Collection.

FINANCIAL IMPLICATIONS:

None

ATTACHMENTS:

1. scan



MECKLENBURG COUNTY

Office of the Tax Collector

July 14, 2023

Anthony Roberts, Huntersville Town Manager
PO Box 664
Huntersville, NC 28070

Re: Tax Collector's Settlement for Fiscal Year 2023 (Tax Year 2022)
Order of Collection for Tax Year 2023

Dear Mr. Roberts:

Please find the enclosed FY 2023 Tax Collector's Settlement. We will work diligently to collect unpaid FY 2023 and other prior year taxes as we move forward with the FY 2024 billing cycle (Tax Year 2023).

According to NCGS 105-373(3), the Tax Collector's Settlement must be entered into the official record of the governing board. Please have this document entered into the record to comply with statute.

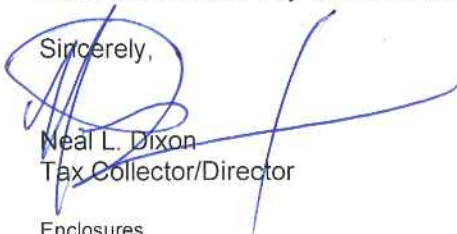
I have also included the Order of Collection for Tax Year 2022 (FY 2024). The order must also be approved by your board after the settlement is received into the record. Please return the signed copy of the Order of Collection to me once executed. A scanned copy can be sent to shalon.page@mecklenburgcountync.gov. A hard copy can be mailed to the following address:

Mecklenburg County Office of the Tax Collector
Attn.: Shalon Page
P.O. Box 31457
Charlotte NC 28231-1457

Your attention to both documents is greatly appreciated.

It was my pleasure to serve you, your board, and your residents again this year. Please do not hesitate to contact me with any feedback about our service during this past year.

Sincerely,


Neal L. Dixon
Tax Collector/Director

Enclosures

CC: Pattie McGinnis, Town of Huntersville Finance Director
Shalon Page, Executive Assistant



MECKLENBURG COUNTY

Office of the Tax Collector

To: Anthony Roberts, Huntersville Town Manager
From: Neal L. Dixon, Director/Tax Collector
Date: July 14, 2023
Subject: Tax Collector's Settlement for Fiscal Year 2023

Pursuant to the provisions of N.C.G.S. 105-373, this memorandum is the Tax Collector's report of settlement to the Huntersville Town Commission for Fiscal Year 2023 (tax year 2022).

The total FY 2023 Real Estate, Personal Property, and Registered Motor Vehicle Tax charged to the Tax Collector for collection was \$26,734,874.15.

<u>Net Levy</u>	<u>Collected</u>	<u>Uncollected</u>	<u>Pct. Collected</u>
\$26,734,874.15	\$26,664,850.46	\$97,077.40	99.74%

At the end of FY 2023 there were 9 tax bills, totaling \$3,118.31, under formal appeal with the Board of Equalization and Review or the Property Tax Commission; consequently, the Tax Collector barred from pursuing collection of these tax bills. In addition, the Tax Collector was barred by the U.S. Bankruptcy Court from collecting 9 real estate, personal property, and registered motor vehicle tax bills totaling \$1,222.81. When this total is removed from the net levy calculation, the collection percentage increases to 99.75%.

Reference is hereby made to reports in the Office of the Tax Collector that list the persons owning real property and personal property whose taxes for the preceding fiscal year remain unpaid and the principal amount owed by each person. These reports are available for inspection and review upon request. The Tax Collector has made diligent efforts to collect the taxes due from the persons listed by utilizing the remedies available to him for collection.

PEOPLE • PRIDE • PROGRESS • PARTNERSHIPS

3205 Freedom Drive, Suite 3000 (28208) • P.O. Box 31457 • Charlotte, North Carolina 28231 • 980-314-4488

Prior Year Collections

During FY 2023, the Tax Collector pursued collection of delinquent prior year taxes.

Real Estate and Personal Property Tax:

<u>Tax Year</u>	<u>Net Levy</u>	<u>Collected in FY 2023</u>	<u>Uncollected</u>	<u>Pct. Collected</u>
2012	\$16,343,051.69	\$637.16	\$11,180.26	99.93%
2013	\$16,512,004.83	\$3,232.80	\$13,739.65	99.92%
2014	\$18,739,426.04	\$2,129.20	\$11,430.39	99.94%
2015	\$19,368,124.32	\$1,416.20	\$13,254.54	99.93%
2016	\$19,886,079.92	\$2,049.06	\$13,990.99	99.93%
2017	\$20,472,885.15	\$2,081.25	\$25,998.59	99.87%
2018	\$21,389,946.92	\$2,594.89	\$18,615.81	99.91%
2019	\$22,976,371.14	\$6,361.59	\$27,687.99	99.88%
2020	\$23,787,193.42	\$13,553.66	\$36,660.48	99.85%
2021	\$25,238,933.03	\$49,195.20	\$50,438.96	99.80%

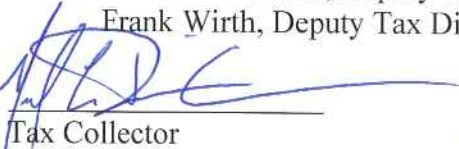
Registered Motor Vehicle Tax:

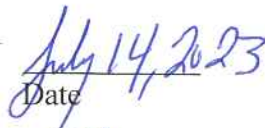
<u>Tax Year</u>	<u>Net Levy</u>	<u>Collected in FY 2023</u>	<u>Uncollected</u>	<u>Pct. Collected</u>
2019	\$0.00	\$0.00	\$0.00	0.00%
2020	\$0.00	\$0.00	\$0.00	0.00%
2021	\$0.00	\$0.00	\$0.00	0.00%

Please contact me at Neal.Dixon@MecklenburgCountyNC.gov or 980-314-4488 if you have any questions or comments regarding this settlement report.

North Carolina General Statute 105-373(3) requires that this settlement be submitted to the governing board. The settlement shall be entered into the minutes of the governing body. Please ensure that this settlement is entered into the minutes of the governing body as required by statute.

cc: Jackie Huffman, Huntersville Deputy Town Manager
Julissa Fernández, Deputy Tax Director
Frank Wirth, Deputy Tax Director


Tax Collector


Date

Sworn to and subscribed before me this 14 day of July, 2023


Notary Public

My commission expires: July 19, 2027
Date



ORDER OF COLLECTION

STATE OF NORTH CAROLINA

TOWN OF HUNTERSVILLE

TO THE TAX COLLECTOR OF THE COUNTY OF MECKLENBURG COUNTY

GENERAL STATUTE 105-321(b)

You are hereby authorized, empowered, and commanded to collect the taxes set forth in the tax records, filed in the Office of the Tax Assessor and in the tax receipts herewith delivered to you, in the amounts and from the taxpayers likewise therein set forth. Such taxes are hereby declared to be a first lien upon all real property of the respective taxpayers in the Town of Huntersville, and this order shall be a full and sufficient authority to direct, require and enable you to levy on and sell any real or personal property of such taxpayers, for and on account thereof, in accordance with law.

Witness my hand and official seal, this _____ day of _____, 2023.

Mayor, Town of Huntersville (SEAL)

Attest:

Clerk to the Board

**Town of Huntersville
Town Board
August 7, 2023**

To: Town Board

From: Tracy Houk, Assistant Director of Parks and Recreation

Date: August 7, 2023

Subject: Budget Amendment - NC Recreation and Park Association Grant

EXPLAIN REQUEST:

The Town of Huntersville received a grant from North Carolina Recreation & Park Association (NCRPA) for \$2,856. Appropriate these funds to NCRPA revenue account (403419.9999.24002) and appropriate the training expense to 406200.0324.24002. This grant will provide for four Parks and Recreation staff employees to complete a Diversity, Equity & Inclusion Certification through UNC Charlotte.

ACTION RECOMMENDED:

Approve Budget Amendment

FINANCIAL IMPLICATIONS:

No net impact to fund balance; offsetting revenue and expense.

ATTACHMENTS:

1. scan

NORTH CAROLINA RECREATION & PARK ASSOCIATION

July 21, 2023

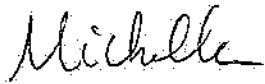
Tracy,

Congratulations! NCRPA is excited to support your project at the \$2,856 level as requested. The check is enclosed.

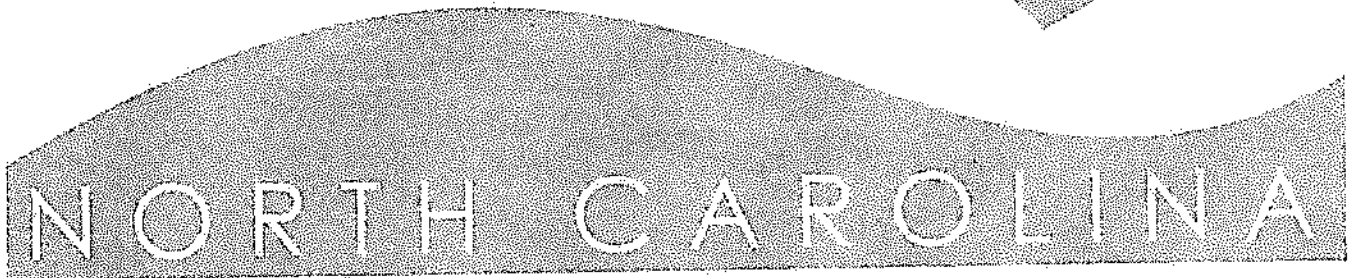
As a reminder, by accepting this grant award, as the grantee you agree to use the funds as proposed. All expenses beyond what is awarded in this grant will be the responsibility of the grantee. Grant work must take place in the state of North Carolina, between June 30th, 2023 - November 30th, 2023. Any unused grant funds are to be returned to the North Carolina Recreation & Park Association by the end of the grant cycle November 30, 2023.

We look forward to seeing the great work you will continue to do in your community.

Sincerely,



Michelle Wells
NCRPA Executive Director



**Town of Huntersville
Town Board
August 7, 2023**

To: Town Board

From: Melinda Bales, Mayor

Date: August 7, 2023

Subject: Award Town Manager Merit/Bonus

EXPLAIN REQUEST:

Consider ratifying previous action of the Town Board taken in Closed Session allowed under the North Carolina Open Meetings Law to award a 2 percent merit increase effective August 1, 2023, and a \$10,000 bonus for the Town Manager based on a performance evaluation.

ACTION RECOMMENDED:

Approve

FINANCIAL IMPLICATIONS:

ATTACHMENTS:

None

**Town of Huntersville
Town Board
August 7, 2023**

To: Town Board

From: David Lucore, Electric System Manager

Date: August 7, 2023

Subject: ElectriCities Contract Labor Award for FY24

EXPLAIN REQUEST:

On behalf of the Town of Huntersville, ElectriCities staff solicited formal bids for Underground and Directional Boring Services for FY24. Contract forces are used to install electric infrastructure for capital projects.

A list of the electric division capital projects approved for FY 24 included as an attachment.

Due to the dollar amount of the project estimates, formal bidding was required. The first formal bid opening occurred on June 26, 2023. NCGS 143-132 requires that three bids be received for a formal bid opening to occur. Only two bids were received, so there was no bid opening. The contract was re-advertised.

Another formal bid opening occurred on July 12, 2023. Again, only two bids were received. However, there is no minimum number of bids required for the second bid opening to occur. Bids were opened publicly and a summary of those bids is listed below:

Bid Summary:

Lamberts Cable Splicing, LLC	\$2,883,353.80
Lee Electrical Construction, LLC	\$5,551,665.25

ACTION RECOMMENDED:

Staff requests the Board of Commissioners to approve the award of the contract to Lamberts Cable Splicing, LLC for a not to exceed amount of \$2,883,353.80 and authorize the Town Manager to execute all documents.

FINANCIAL IMPLICATIONS:

Not to Exceed \$2,883,353.80

ATTACHMENTS:

1. Capital Projects Approved
2. Bid Summary
3. Notice and Instructions to Bidders
4. Contract Documents

TOWN OF HUNTERSVILLE
ELECTRIC DIVISION
CAPITAL PROJECTS APPROVED FOR FY24

RESIDENTIAL:

Mayes Road – 83 Single Family
Caldwell Station Phase 2 – 180 Multi Family
Anchor Mills Townhomes – 361 Multi Family
Spring Grove – 124 Single Family
Hamlet at Huntersville – 200 Single Family, 5 Commercial
Main Street Town Center – 11 Single Family; 190 Multi Family; 2 Commercial

COMMERCIAL/INDUSTRIAL:

Jamesburg Dr – 8 Commercial
Bryton Industrial – 15 Industrial
Hambright Junction – 300 Multi Family
Caldwell Crossing – 130 Senior Apartments

SYSTEM IMPROVEMENTS:

Huntersville East Bulk Feeder
Bryton Bulk Feeder
McCord Road Bulk Feeder
Gilead Road Underground Conversion
Mayes Road Line Extension

BID SUMMARY

AGENT: DAVID LUCORE, ELECTRIC SYSTEMS MANAGER, ELECTRICITIES OF NC, INC.

COMPANY

	Lee Electrical	Lamberts		
Pipe Installation Cost	\$ 2,927,660.00	\$ 1,466,608.00		
Gen. Construction Cost	\$ 651,640.00	\$ 279,987.00		
Open Trench Cost	\$ 776,970.00	\$ 401,812.50		
Boxes & Pads Cost	\$ 320,293.50	\$ 80,203.30		
SL's & Sec. Lights Cost	\$ 200,748.50	\$ 69,687.50		
TX's & Switchgears Cost	\$ 151,689.50	\$ 35,828.75		
Terminations Cost	\$ 66,213.75	\$ 81,326.75		
Wire & Cable Cost	\$ 456,450.00	\$ 467,900.00		
Total Cost	\$ 5,551,665.25	\$ 2,883,353.80		

I attest that these bids were received and have been recorded above accurately according to the bid submissions.

David E. Lucore

7/12/23

Date

UNDERGROUND & DIRECTIONAL BORING SERVICES

NOTICE AND INSTRUCTIONS TO BIDDERS

ElectriCities of NC, Inc.
David E. Lucore, Electric Systems Manager
(704) 659-7375
On Behalf of the
Town of Huntersville, NC

Sealed bids are being sought by ElectriCities of NC, Inc. on behalf of the Town of Huntersville, NC (hereinafter referred to as "Owner") for the furnishing of **Underground and Directional Boring Services** including labor and equipment for construction and maintenance on the Town's 7.2/12.47 kV electric distribution system for Fiscal Year 24. This is a **sealed formal bid** according to NCGS § 143-129.

A bid package may be obtained from the Managing Agent for the Owner by e-mail request to dlucore@electricities.org.

You may mail your bid or hand deliver to: **ElectriCities of NC, Inc., Town of Huntersville, NC, PO Box 664, Huntersville, NC 28070; ATTN: David Lucore with Sealed Bid for Town of Huntersville: Underground and Directional Boring Services, Do Not Open Until 2 PM, July 12, 2023,** indicated on outside of envelope.

Bid(s) must be returned on the attached proposal sheet showing unit prices fully extended and the proposal page completed in its entirety by **Wednesday, July 12, 2023, at 2 PM**. Bidder will be required to comply with all applicable statutes and regulations. Bidder is responsible for the timely delivery of their bid before the deadline. **All bids received after this time will be immediately rejected and returned to the bidder unopened.**

A public bid opening will be held at **2 PM EST on Wednesday, July 12, 2023**, at the Town of Huntersville Town Hall Conference Room, located at 101 Huntersville-Concord Rd, Huntersville, NC 28078. At this time, the bids will be opened and read publicly.

All bids must be valid for the period from July 1, 2023, to June 30, 2024, pending Council approval and award of bid.

ElectriCities of NC, Inc., and the Town of Huntersville, reserve the right to reject any and/or all bids received, and to select the bid which is in the best overall interest of the Town of Huntersville. Awards will be based upon the lowest cost, most responsive bidder.

Incomplete bids or those lacking the required information will be rejected. The Owner reserves the right to waive minor defects and informalities that would not prejudice other bidders, and which speak to the responsiveness of the bid. Mathematical errors may be grounds for removal of bid as set forth in NCGS § 143-129.1.

Contractors shall hold State of North Carolina Contractor's License(s) of the class required to perform the specified work. Contractor's License number shall be included in the proposal to be considered.

Bid Specifications

1. The successful bidder will furnish all labor and equipment which may be necessary to install materials and equipment for the Town of Huntersville's electric distribution system.
2. An estimated quantity of items budgeted for FY24, based on current information, is included. These are estimated quantities and are not guaranteed during the contract period. The schedule and availability of work in FY24 will vary based on many factors including weather, readiness of the project, availability of materials, etc.
3. Contractor will be paid for actual quantities of units installed, in place and as measured and/or verified by ElectriCities of NC, Inc. representatives.
4. ElectriCities will provide plans for each project to the contractor approximately one month before the estimated construction start date. Contractor will produce an estimated cost based on unit prices and ElectriCities will authorize the work to begin with an approved work order issued to the contractor.
5. The Owner will provide all materials for each project. A standard percentage markup will be established for use when the Contractor provides materials when it is mutually agreed to be more efficient and approved by Owner. The total sum of materials provided by the Contractor shall not exceed \$29,999 in cost.
6. The price(s) quoted for each unit item by each bidder shall contain, and shall be deemed to contain in the price, any amounts which are estimated to be payable by the Bidder for any and all taxes imposed by any taxing authority upon the sale, purchase or use of materials, supplies or equipment contained in each project. The bidder shall be solely responsible for the payment of any such taxes.
7. The Owner and Contractor shall mutually agree on an acceptable price for units required but not contained in the proposal by the issuance of a Change Order approved by ElectriCities representatives.
8. The Contractor awarded the contract shall reimburse the Owner the cost for all loss, breakage, or theft of materials once they have taken delivery of them from any warehouse or storage location operated by the Owner.
9. Contractor is responsible for the transportation of materials received from the Owner's warehouse or storage location to each project site.
10. All materials left over or scrapped as part of any project shall remain the property of the Owner and contractor shall transport such items as directed by Owner for reuse or disposal.
11. Each proposal shall be accompanied by a certified check on a bank that is a member of the Federal Deposit Insurance Corporation (FDIC) payable to the order of the Owner, or a Bidder's Bond acceptable by the Owner and running in favor of the Owner, in an amount equal to 5% of the maximum price of the bid.
12. The check or Bidder's Bond shall be returned to contractors whose bid was not accepted and or if the proposal is accepted and a contract is executed, the check or Bidder's Bond shall be returned within thirty (30) days to the bidder; except that each Bidder agrees that provided its proposal was one of the 3 lowest bids, each such proposal shall be firm and binding upon each bidder and each check shall be retained by the Owner for a period not exceeding ninety (90) days from the date of the public bid opening.
13. The successful bidder will be required to enter into a contract with the Owner and furnish Performance and Payment Bonds in the forms attached for the full contract amount to guarantee the full performance of the contract.

CONTRACTOR'S PROPOSAL (Bidder or Contractor)
TO: TOWN OF HUNTERSVILLE, NC (Owner)

LABOR AND EQUIPMENT PROPOSAL for FY24

SECTION 1.

- A. The projects to be worked under this contract will be in and around the Town of Huntersville, NC.
- B. Contractor, hereinafter called the "Bidder" or "Contractor", shall have familiarized himself/herself with all conditions likely to be encountered affecting the cost and schedule of work. The Contractor agrees and warrants that he/she has:
1. Inspected the construction units and proposes a fair and reasonable cost for each unit according to current market rates.
 2. Agreed to provide labor, equipment, transportation, and all other items necessary (other than bulk materials, which will be provided by the Owner) required to construct, repair and/or maintain the Town of Huntersville's electric distribution system in accordance with industry standard practices, federal and state regulations applicable to work of this type, town policies and procedures. Agrees and understands that plans, specifications, and construction standards will be provided by the Owner on a project-by-project basis.
- C. Bidder acknowledges that he/she has carefully examined the contract documents and understands the requirements contained therein and that the documents are appropriate and adequate for contracting with the Owner, and that Bidder has an adequately trained staff of employees who can perform the work on a project-by-project basis in a competent, professional, and workmanlike manner.
- D. Bidder further acknowledges that he/she has or has at their disposal the equipment, machinery, and facilities necessary to perform the work competently.
- E. Bidder declares that this proposal, in all aspects is fair and is provided in good faith without collusion or fraud and that only the person or persons named in this proposal have any interest in this proposal or in the contract to be entered into with the Owner.
- F. Bidder agrees to provide labor and equipment to install units at the prices listed below with one or more crews in complete accordance with the contract documents:

	Unit	UOM	Est. Qty	Unit Price	Total Est. Price
I.	DIRECTIONAL BORING UNITS				
a.	Pipe Installation Units				
1.	(1) 1" - 1 1/2" HDPE	Linear Ft	5000	\$ 10.50	\$ 52,500.00
2.	(1) 2" - 2 1/2" HDPE	Linear Ft	7000	\$ 13.12	\$ 91,840.00
3.	(2) 2" - 2 1/2" HDPE	Linear Ft	400	\$ 21.00	\$ 8,400.00
4.	(3) 2" - 2 1/2" HDPE	Linear Ft	1250	\$ 33.60	\$ 42,000.00
5.	(4) 2" - 2 1/2" HDPE	Linear Ft	1250	\$ 36.25	\$ 45,312.50
6.	(5) 2" - 2 1/2" HDPE	Linear Ft	1250	\$ 42.00	\$ 52,500.00
7.	(1) 2" - 2 1/2" & (1) 1" - 1 1/2" HDPE	Linear Ft	400	\$ 15.75	\$ 6,300.00
8.	(1) 2" - 2 1/2" & (2) 1" - 1 1/2" HDPE	Linear Ft	400	\$ 17.32	\$ 6,928.00
9.	(2) 2" - 2 1/2" & (1) 1" - 1 1/2" HDPE	Linear Ft	1250	\$ 23.10	\$ 28,875.00
10.	(2) 2" - 2 1/2" & (2) 1" - 1 1/2" HDPE	Linear Ft	1250	\$ 26.25	\$ 32,812.50
11.	(3) 2" - 2 1/2" & (1) 1" - 1 1/2" HDPE	Linear Ft	400	\$ 35.70	\$ 14,280.00
12.	(4) 2" - 2 1/2" & (1) 1" - 1 1/2" HDPE	Linear Ft	1250	\$ 42.00	\$ 52,500.00
13.	(5) 2" - 2 1/2" & (1) 1" - 1 1/2" HDPE	Linear Ft	400	\$ 46.20	\$ 18,480.00
14.	(1) 3" HDPE	Linear Ft	2500	\$ 21.00	\$ 52,500.00
15.	(2) 3" HDPE	Linear Ft	500	\$ 27.30	\$ 13,650.00
16.	(3) 3" HDPE	Linear Ft	1500	\$ 37.80	\$ 56,700.00
17.	(4) 3" HDPE	Linear Ft	7500	\$ 33.60	\$ 252,000.00
18.	(1) 3" & (1) 1" - 1 1/2" HDPE	Linear Ft	400	\$ 23.10	\$ 9,240.00
19.	(1) 3" & (2) 1" - 1 1/2" HDPE	Linear Ft	400	\$ 25.20	\$ 10,080.00
20.	(1) 3" & (1) 2" - 2 1/2" & (1) 1" - 1 1/2" HDPE	Linear Ft	400	\$ 29.40	\$ 11,760.00
21.	(1) 3" & (2) 2" - 2 1/2" HDPE	Linear Ft	400	\$ 34.65	\$ 13,860.00
22.	(1) 3" & (3) 2" - 2 1/2" HDPE	Linear Ft	1250	\$ 37.80	\$ 47,250.00

23. (1) 3" & (4) 2" – 2 ½" HDPE	Linear Ft	400	\$ 42.00	\$ 16,800.00
24. (4) 3" & (1) 2" – 2 ½" HDPE	Linear Ft	1250	\$ 37.80	\$ 47,250.00
25. (1) 4" HDPE	Linear Ft	2000	\$ 23.10	\$ 46,200.00
26. (2) 4" HDPE	Linear Ft	900	\$ 35.70	\$ 32,130.00
27. (3) 4" HDPE	Linear Ft	1000	\$ 42.00	\$ 42,000.00
28. (1) 4" & (1) 2" – 2 ½" HDPE	Linear Ft	400	\$ 27.30	\$ 10,920.00
29. (1) 4" & (1) 2" – 2 ½" & (1) 1" – 1 ½" HDPE	Linear Ft	400	\$ 29.40	\$ 11,760.00
30. (1) 4" & (2) 2" – 2 ½" HDPE	Linear Ft	400	\$ 35.70	\$ 14,280.00
31. (1) 6" HDPE	Linear Ft	5000	\$ 33.60	\$ 168,000.00
32. Rock Adder for Directional Bore	Linear Ft	2000	\$78.75	\$ 157,500.00

Pipe Installation Units Total

\$1,466,608.00

b. General Construction Units

33. Asphalt, Cut & Remove 0" – 5" thick	Sq Ft.	2000	\$ 15.75	\$ 31,500.00
34. Asphalt, Cut & Remove 6" - 10" Thick	Sq. Ft.	500	\$ 26.25	\$ 13,125.00
35. Concrete, Cut & Remove 0" – 4" Thick	Sq. Ft.	2000	\$ 15.75	\$ 31,500.00
36. Concrete, Cut & Remove 5" – 8" Thick	Sq. Ft.	500	\$ 31.50	\$ 15,750.00
37. Concrete, Replace 3,000 psi 4" Thick	Sq. Ft.	2000	\$ 15.75	\$ 31,500.00
38. Locates, 12" Core Hole & Restore	Each	200	\$ 157.50	\$ 31,500.00
39. Dig, Barricade & Restore 4' x 4' x 3' Pit	Each	100	\$ 315.00	\$ 31,500.00
40. Locates, 24" Core Hole & Restore	Each	100	\$ 315.00	\$ 31,500.00
41. Locate, Existing Conduits by Excavating, Removal of landscaping, debris & foreign objects	Hour	100	\$ 162.75	\$ 16,275.00
42. Excavating and Relocating Existing Conduits Up to 6"	Hour	100	\$ 144.75	\$ 14,475.00
43. Excavation of existing conduit due to obstructions that would prevent the installation of cable. by normal means	Hour	100	\$162.94	\$ 16,294.00
44. Install pulling string by use of pneumatic tooling, in conduit up to 6"	Hour	100	\$ 150.68	\$ 15,068.00

General Construction Units Total

\$279,987.00

c. Open Trench Units

45. Open Trench 18" W x 36" D	Linear Ft	30000	\$ 4.20	\$ 126,000.00
46. Open Trench 18" W x 48" D	Linear Ft	25000	\$ 4.72	\$ 118,000.00
47. Open Trench 24" W x 60" D	Linear Ft	5000	\$ 5.25	\$ 26,250.00
48. Rock Adder for Open Trench	Linear Ft	500	\$ 157.50	\$ 78,750.00
49. Add 1" – 1 ½" Duct to Trench	Linear Ft	10000	\$ 1.21	\$ 12,100.00
50. Add 2" – 2 ½" Duct to Trench	Linear Ft	25000	\$ 1.21	\$ 30,250.00
51. Add 3" Duct to Trench	Linear Ft	5000	\$ 1.41	\$ 7,050.00
52. Add 4" Duct to Trench	Linear Ft	1500	\$ 1.41	\$ 2,115.00
53. Add 6" Duct to Trench	Linear Ft	750	\$ 1.73	\$ 1,297.50

Open Trench Units Total

\$401,812.50

II. MATERIALS INSTALLATION UNITS

a. Boxes & Pads Units

54. Box, Splice, Streetlight, 10" x 15", w/Conn.	Each	200	\$ 26.25	\$ 5,250.00
55. Enclosure, Fiberglass, 15 kV	Each	50	\$ 48.25	\$ 2,412.50
56. Junction, 15 kV, 200A, 2-Point	Each	50	\$ 267.75	\$13,387.50
57. Junction, 15 kV, 200A, 3-Point	Each	50	\$ 325.50	\$ 16,275.00
58. Junction, 15 kV, 200A, 4-Point	Each	25	\$ 325.50	\$ 8,137.50

59. Junction, 15 kV, 600A, 3-Point	Each	25	\$ 362.50	\$ 9,062.50
60. Pad, Switchgear, 15 kV, PME-9, & ME-11	Each	15	\$ 478.80	\$ 7,182.00
61. Pad, Transformer, 1-Ph	Each	65	\$ 144.37	\$ 9,384.05
62. Pad, Transformer, 3-Ph	Each	25	\$ 334.43	\$ 8,360.75
63. Pedestal, Secondary, UG, 1-Ph	Each	10	\$ 75.15	\$ 751.50

Boxes & Pads Units Total **\$80,203.30**

d. Streetlights & Security Lights Units

64. Fixture, Streetlight, Decorative	Each	100	\$ 78.75	\$ 7,785.00
65. Fixture, Street or Security, Standard, w/arm	Each	50	\$ 81.25	\$ 4,062.50
66. Pole, AL, Decorative, 10' – 16' for SL	Each	100	\$ 157.50	\$ 15,750.00
67. Pole, AL or Fiberglass, Std, 20' 30', for SL	Each	50	\$ 210.00	\$ 10,500.00
68. Foundation, Pole, Direct Bury, for SL	Each	100	\$ 315.00	\$ 31,500.00

Streetlights & Security Lights Total **\$35,828.75**

e. Transformers & Switchgear Units

69. 25 KVA – 100 KVA 1-Ph Install	Each	75	\$ 143.85	\$ 10,788.75
70. 167 KVA 1-Ph Install	Each	10	\$ 236.25	\$ 2,362.50
71. 75 KVA – 500 KVA 3-Ph Install	Each	10	\$ 333.90	\$ 3,339.00
72. 750 KVA & Larger 3-Ph Install	Each	5	\$ 378.00	\$ 1,890.00
73. Grounding ASSY, for Pad-Mtd. Enclosures	Each	120	\$ 62.00	\$ 7,440.00
74. PME-9 Switchgear Install	Each	10	\$ 488.25	\$ 4,882.50
75. PME-11 Switchgear Install	Each	10	\$ 512.60	\$ 5,126.00

Transformers & Switchgears Total **\$35,828.75**

f. Termination Units

76. Adapter, 15 kV, 200A, Reducing	Each	100	\$ 31.50	\$ 3,150.00
77. Bracket, Insulated Standoff, 15 kV	Each	25	\$ 52.30	\$ 1,307.50
78. Bracket, Insulated, Feed-Thru, 15 kV	Each	25	\$ 52.30	\$ 1,307.50
79. Bushing Insert, 15 kV, Loadbreak, 200A	Each	150	\$ 52.30	\$ 7,845.00
80. Bushing Insert, 15 kV, LB, 200A, Feed-Thru	Each	50	\$ 52.30	\$ 2,615.00
81. Cap, Insulated, Protective, 15 kV, 200A	Each	100	\$ 52.30	\$ 5,230.00
82. Cap, Insulated, Protective, 15 kV, 600A	Each	50	\$ 52.30	\$ 2,615.00
83. Elbow, 15 kV, 200A, Loadbreak	Each	100	\$ 120.75	\$ 12,075.00
84. Elbow, 15 kV, 600 A Deadbreak, T-Body	Each	50	\$ 141.75	\$ 7,087.50
85. Elbow, Arrester, 15 kV	Each	35	\$ 79.30	\$ 2,775.50
86. Elbow, Fused, 15 kV	Each	25	\$ 162.75	\$ 4,068.75
87. Riser, House, 200A, Install & Connect	Each	200	\$ 132.00	\$ 26,400.00
88. Wire, Secondary, Any Size	Each	1000	\$ 4.85	\$ 4,850.00

Terminations Total **\$81,325.75**

g. Wire & Cable Units

89. (1) 1/0 Primary, AL, 15 kV, JCN, URD	Linear Ft	50000	\$ 1.41	\$ 70,500.00
90. (3) 1/0 Primary, AL, 15 kV, JCN, URD	Linear Ft	5000	\$ 3.30	\$ 16,500.00
91. 2/0 TPX Aluminum, 600V, UG	Linear Ft	3000	\$ 1.20	\$ 3,600.00
92. #2 STR, Copper, Bare	Linear Ft	10000	\$ 1.05	\$ 10,500.00
93. 350 QPX, Aluminum, 600V, UG	Linear Ft	25000	\$ 1.45	\$ 36,250.00
94. 4/0 TPX, Aluminum, 600V, UG	Linear Ft	20000	\$ 1.25	\$ 25,000.00
95. 4/0 QPX, Aluminum, 600V, UG	Linear Ft	35000	\$ 1.45	\$ 50,750.00
96. #6/3 Streetlight, Aluminum, 600V, UG	Linear Ft	10000	\$ 1.25	\$ 12,500.00
97. (1) 750 MCM Pri., AL, 15 kV, JCN, URD	Linear Ft	10000	\$ 1.73	\$ 17,300.00
98. (3) 750 MCM Pri., AL, 15 kV, JCN, URD	Linear Ft	30000	\$ 7.50	\$ 225,000.00

Wire & Cable Install Total **\$467,900.00**

LABOR AND EQUIPMENT PROPOSAL

SUMMARY

<u>UNITS</u>	<u>SUBTOTAL COST</u>
<u>DIRECTIONAL BORING UNITS</u>	
a. Pipe Installation Units	\$ <u>1,466,608.⁰⁰</u>
b. General Construction Units	\$ <u>279,987.⁰⁰</u>
c. Open Trench Units	\$ <u>401,812.50</u>
<u>MATERIALS INSTALLATION UNITS</u>	
a. Boxes & Pads Units	\$ <u>80,203.30</u>
b. Streetlights & Security Lights Units	\$ <u>69,687.50</u>
c. Transformers & Switchgear Installation Units	\$ <u>35,828.75</u>
d. Terminations Units	\$ <u>81,326.75</u>
e. Wire & Cable Units	\$ <u>467,900.⁰⁰</u>
<u>TOTAL COST</u>	\$ <u>2,883,353.80</u>

SECTION 2.

- a. **Licensing** – Contractor, by submitting a bid, represents that he/she possesses a valid Contractor's License(s) Number(s): W. 35088, that authorizes him/her to perform the work specified in the proposal in the state of North Carolina. The Contractor further agrees to notify the Owner immediately of any change in the status of said License(s).
- b. **Equipment** – All vehicles and equipment used in the performance of this contract shall be in excellent condition and shall be properly maintained to ensure their safety and efficiency and shall present an acceptable image to the public. All vehicles shall be marked with the contractor's name in some fashion to be quickly identified.
- c. **Equipment Staging** – Owner has limited space available at their operations facility and cannot provide room for the staging of Bidder's vehicles and equipment. There may be other Owner sites that accommodate this, however, in the event that suitable space cannot be provided by the Owner, the Bidder agrees to find suitable staging area(s) for all vehicles and equipment at his/her own expense.
- d. **Employee Conduct** – Contractor agrees to provide a staff of professional employees who will:
 1. Always conduct themselves in a professional manner.
 2. Always display the highest regard for safety.
 3. Always be courteous and professional in all dealings with the Owner's staff and the public.
 4. Always display the highest integrity and ethical decision-making skills.
 5. Wear uniforms or clothing that is good repair and condition and is marked with the company name to easily identify them as employees.

4. Always display the highest integrity and ethical decision-making skills.
 5. Wear uniforms or clothing that is good repair and condition and is marked with the company name to easily identify them as employees.
- e. **Materials** – If, during the performance of work under this contract, the contractor needs miscellaneous materials, such as but not limited to, lumber, grass seed, straw, fittings, etc. and it is identified as more efficient and possibly more cost effective for the Contractor to furnish those items, the contractor shall be allowed a standard percentage markup of 10% for the furnishing of those materials with the Owner's or Owner's Representative's approval. Invoices or receipts for all items purchased shall be submitted to Owner before payment will be made. In any case, the total of all miscellaneous items purchased by the contractor shall not exceed \$29,999 during the contract term.
 - f. **Miscellaneous Materials** - The Contractor agrees that when it is necessary to construct units that are not contained in the proposal, the Owner and Contractor shall determine and agree on a fair market rate for each unit. The Contractor shall submit a Change Order to the Owner and the Owner must approve the Change Order before any such item(s) are authorized. Contractor shall use the Change Order form attached hereto as part of this proposal.
 - g. **Estimated Units** - The Contractor, by submitting a bid, agrees and understands that the estimated units listed in the proposal are estimates only and the Owner may specify any number or combination of numbers of units as the Owner deems necessary.
 - h. **Taxes** – The Contractor agrees to provide unit prices include provisions for the payment of all monies which will be payable by the Bidder or the Owner in connection with the construction of the project due to taxes levied by any taxing authority upon the sale, purchase or use of materials, supplies, or equipment to be incorporated in the project as part of such unit(s). The Bidder agrees to pay all such taxes and to furnish to the Owner and all appropriate taxing authorities all required documentation and reports pertaining thereto.
 - i. **Temporary Work** – All temporary work, which the Bidder performs for his convenience in constructing the project shall be installed and removed at his own expense.

NAME OF BIDDER: LAMBERTS CABLE SPLICING, LLC
BY: [Signature] TITLE: President
ADDRESS OF BIDDER: 2521 S. WESLEYAN BLVD. ROCKY MOUNT NC 27803
LICENSE NUMBER(S): U.35088

The Proposal must be signed with the full name of the Bidder. In the case of a partnership, the Proposal must be signed in the firm name by each partner. In the case of a corporation, the Proposal must be signed in the corporate name by a duly authorized officer and the corporate seal affixed and attested by the Secretary of the Corporation. A typewritten copy of all such names and signatures shall be appended.

The Bidder must accompany his bid proposal with an Affidavit of Compliance with N.C. E-Verify Status.

STATE OF NORTH CAROLINA
TOWN OF HUNTERSVILLE
COUNTY OF MECKLENBURG

AFFIDAVIT OF COMPLIANCE WITH
N.C. E-VERIFY STATUS

By executing this affidavit, the undersigned contractor verifies its compliance with N.C.G.S § 64-26, stating affirmatively that the individual, firm or corporation which is engaged in the physical performance of services on behalf of the Town of Huntersville, NC, is duly authorized to use and uses the federal work authorization program commonly known as E-Verify, or any subsequent replacement program, in accordance with the applicable provisions and deadlines established in N.C.G.S. § 64-26.

Furthermore, the undersigned contractor will continue to use the federal work authorization program throughout the contract period and the undersigned contractor will contract for the physical performance of services in satisfaction of such contract only with subcontractors who present an affidavit to the contractor with the information required by N.C.G.S. § 64-26.

Lamberts Cable Splicing Company LLC
Name of Contractor

I hereby declare under penalty of perjury that the foregoing is true and correct.

Executed on June, 14, 2023, in Rocky Mount (city), NC (state).

John Gilbert
Executive Vice President
Signature of Authorized Officer or Agent

John Gilbert
Executive Vice President
Printed Name and Title of Authorized Officer or Agent

STATE OF NORTH CAROLINA
COUNTY OF MECKLENBURG

Sworn to and subscribed before me, this the 14th day of July, 2023.

Notary Public: Lane Warbritton

My Commission Expires: 3-13-2026

LANE WARBRITTON
NOTARY PUBLIC
NASH COUNTY, NC

Document A310™ – 2010

Conforms with The American Institute of Architects AIA Document 310

Bond Number: 95323-TRAV-23-0234

Bid Bond

CONTRACTOR:

(Name, legal status and address)

Lamberts Cable Splicing Company, LLC

1 Cleveland Street, Suite 900

Gordonsville, VA 22942

SURETY:

(Name, legal status and principal place of business)

Travelers Casualty and Surety Company of America

One Tower Square

Hartford, CT 06183-6014

State of Inc: CT

This document has important legal consequences. Consultation with an attorney is encouraged with respect to its completion or modification.

OWNER:

(Name, legal status and address)

ElectricCilles of NC, Inc., on behalf of the Town of Huntersville, NC

PO Box 664

Huntersville, NC 28070

Any singular reference to Contractor, Surety, Owner or other party shall be considered plural where applicable.

BOND AMOUNT: Five Percent of Amount Bid (5%)

PROJECT:

(Name, location or address, and Project number, if any)

Town of Huntersville: Underground and Directional Boring Services

The Contractor and Surety are bound to the Owner in the amount set forth above, for the payment of which the Contractor and Surety bind themselves, their heirs, executors, administrators, successors and assigns, jointly and severally, as provided herein. The conditions of this Bond are such that if the Owner accepts the bid of the Contractor within the time specified in the bid documents, or within such time period as may be agreed to by the Owner and Contractor, and the Contractor either (1) enters into a contract with the Owner in accordance with the terms of such bid, and gives such bond or bonds as may be specified in the bidding or Contract Documents, with a surety admitted in the jurisdiction of the Project and otherwise acceptable to the Owner, for the faithful performance of such Contract and for the prompt payment of labor and material furnished in the prosecution thereof; or (2) pays to the Owner the difference, not to exceed the amount of this Bond, between the amount specified in said bid and such larger amount for which the Owner may in good faith contract with another party to perform the work covered by said bid, then this obligation shall be null and void, otherwise to remain in full force and effect. The Surety hereby waives any notice of an agreement between the Owner and Contractor to extend the time in which the Owner may accept the bid. Waiver of notice by the Surety shall not apply to any extension exceeding sixty (60) days in the aggregate beyond the time for acceptance of bids specified in the bid documents, and the Owner and Contractor shall obtain the Surety's consent for an extension beyond sixty (60) days.

If this Bond is issued in connection with a subcontractor's bid to a Contractor, the term Contractor in this Bond shall be deemed to be Subcontractor and the term Owner shall be deemed to be Contractor.

When this Bond has been furnished to comply with a statutory or other legal requirement in the location of the Project, any provision in this Bond conflicting with said statutory or legal requirement shall be deemed deleted herefrom and provisions conforming to such statutory or other legal requirement shall be deemed incorporated herein. When so furnished, the intent is that this Bond shall be construed as a statutory bond and not as a common law bond.

Signed and sealed this 21st day of June, 2023

DocuSigned by:

melinda perry

(Witness)

Camille Cruz
(Witness) Camille Cruz, Surety Witness

Lamberts Cable Splicing Company, LLC

(Principal)

DocuSigned by:

Teresa Adcock

(Seal)

(Title)

Principal Accounting Of

Travelers Casualty and Surety Company of America

(Surety)

Ana W. Oliveras
Ana W. Oliveras, Attorney-in-Fact

(Seal)

(Title)



Travelers Casualty and Surety Company of America
Travelers Casualty and Surety Company
St. Paul Fire and Marine Insurance Company

POWER OF ATTORNEY

KNOW ALL MEN BY THESE PRESENTS: That Travelers Casualty and Surety Company of America, Travelers Casualty and Surety Company, and St. Paul Fire and Marine Insurance Company are corporations duly organized under the laws of the State of Connecticut (herein collectively called the "Companies"), and that the Companies do hereby make, constitute and appoint Ana W. Oliveras of Palm Beach, Florida, their true and lawful Attorney(s)-in-Fact to sign, execute, seal and acknowledge any and all bonds, recognizances, conditional undertakings and other writings obligatory in the nature thereof on behalf of the Companies in their business of guaranteeing the fidelity of persons, guaranteeing the performance of contracts and executing or guaranteeing bonds and undertakings required or permitted in any actions or proceedings allowed by law.

IN WITNESS WHEREOF, the Companies have caused this instrument to be signed, and their corporate seals to be hereto affixed, this **21st** day of **April**, 2021.



State of Connecticut

City of Hartford ss.

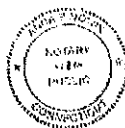
By: *Robert L. Raney*

Robert L. Raney, Senior Vice President

On this the **21st** day of **April**, 2021, before me personally appeared **Robert L. Raney**, who acknowledged himself to be the Senior Vice President of each of the Companies, and that he, as such, being authorized so to do, executed the foregoing instrument for the purposes therein contained by signing on behalf of said Companies by himself as a duly authorized officer.

IN WITNESS WHEREOF, I hereunto set my hand and official seal.

My Commission expires the **30th** day of **June**, 2026



Anna P. Nowik

Anna P. Nowik, Notary Public

This Power of Attorney is granted under and by the authority of the following resolutions adopted by the Boards of Directors of each of the Companies, which resolutions are now in full force and effect, reading as follows:

RESOLVED, that the Chairman, the President, any Vice Chairman, any Executive Vice President, any Senior Vice President, any Vice President, any Second Vice President, the Treasurer, any Assistant Treasurer, the Corporate Secretary or any Assistant Secretary may appoint Attorneys-in-Fact and Agents to act for and on behalf of the Company and may give such appointee such authority as his or her certificate of authority may prescribe to sign with the Company's name and seal with the Company's seal bonds, recognizances, contracts of indemnity, and other writings obligatory in the nature of a bond, recognizance, or conditional undertaking, and any of said officers or the Board of Directors at any time may remove any such appointee and revoke the power given him or her; and it is

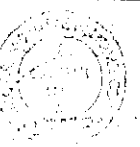
FURTHER RESOLVED, that the Chairman, the President, any Vice Chairman, any Executive Vice President, any Senior Vice President or any Vice President may delegate all or any part of the foregoing authority to one or more officers or employees of this Company, provided that each such delegation is in writing and a copy thereof is filed in the office of the Secretary; and it is

FURTHER RESOLVED, that any bond, recognizance, contract of indemnity, or writing obligatory in the nature of a bond, recognizance, or conditional undertaking shall be valid and binding upon the Company when (a) signed by the President, any Vice Chairman, any Executive Vice President, any Senior Vice President or any Vice President, any Second Vice President, the Treasurer, any Assistant Treasurer, the Corporate Secretary or any Assistant Secretary and duly attested and sealed with the Company's seal by a Secretary or Assistant Secretary; or (b) duly executed (under seal, if required) by one or more Attorneys-in-Fact and Agents pursuant to the power prescribed in his or her certificate or their certificates of authority or by one or more Company officers pursuant to a written delegation of authority; and it is

FURTHER RESOLVED, that the signature of each of the following officers: President, any Executive Vice President, any Senior Vice President, any Vice President, any Assistant Vice President, any Secretary, any Assistant Secretary, and the seal of the Company may be affixed by facsimile to any Power of Attorney or to any certificate relating thereto appointing Resident Vice Presidents, Resident Assistant Secretaries or Attorneys-in-Fact for purposes only of executing and attesting bonds and undertakings and other writings obligatory in the nature thereof, and any such Power of Attorney or certificate bearing such facsimile signature or facsimile seal shall be valid and binding upon the Company and any such power so executed and certified by such facsimile signature and facsimile seal shall be valid and binding on the Company in the future with respect to any bond or understanding to which it is attached.

I, **Kevin E. Hughes**, the undersigned, Assistant Secretary of each of the Companies, do hereby certify that the above and foregoing is a true and correct copy of the Power of Attorney executed by said Companies, which remains in full force and effect.

Dated this 21st day of June, 2023



Kevin E. Hughes

Kevin E. Hughes, Assistant Secretary

To verify the authenticity of this Power of Attorney, please call us at 1-800-421-3880.
 Please refer to the above-named Attorney(s)-in-Fact and the details of the bond to which this Power of Attorney is attached.



101 Huntersville-Concord Road
Huntersville, NC 28078
(704) 875-6541

CONTRACT FOR SERVICES

Firm: Name Lamberts Cable Splicing, LLC

Address: 2521 S. Wesleyan Blvd.

City, State, Zip: Rocky Mount, NC 27803

Project Manager Name: Brad Sigmon

Project Manager email bsigmon@electricities.org

PROJECT:

ADDRESS: Huntersville, NC

Phone (252) 414-1980

This Contract for Services, and all exhibits, (collectively this "Contract") is entered into this 7th day of August 2023, by and between, the Town of Huntersville, a municipal corporation of the State of North Carolina, (the "Town") and Lamberts Cable Splicing, LLC (the "Firm") located at 2521 S. Wesleyan Blvd, Rocky Mount, NC 27803.

For and in consideration of the mutual promises set forth in this Contract, the parties do mutually agree as follows:

1. Scope of Services. The Contractor agrees to perform for the Town the following services according to the following requirements:

The Firm agrees to provide services as needed to complete each project, on a task order basis. Each individual project shall constitute the "Work." The Scope of Services and Pricing Sheet is attached as Exhibit C, which is incorporated herein by reference. A new Scope of Services and Pricing Sheet shall be attached with each new project and task order. The terms of this Contract, with the exception of the Scope of Services and Pricing Sheet, shall apply to each project, unless otherwise agreed. The Firm represents to the Town that the unit billing rates are the Firm's Contracted billing rates. Any meetings not included in the Scope of Services in Exhibit C will be considered "Additional Services." Rates for additional Services will be identified either in writing at Exhibit E or by verbal communication but must be approved in writing by Town before proceeding to perform such Additional Services.

The total sum of all project invoices shall not exceed \$2,883,353.80.

The Firm will be responsible for providing employees to complete the Work in accordance with Town standards. In addition to the indemnification obligations contained in the STANDARD TERMS AND CONDITIONS attached to this Contract, the Firm further agrees to defend, indemnify, and save harmless the Town for claims and liabilities resulting from negligence, errors or omissions of the Firm, including, but not limited to, the employees, technicians or subcontractors.

The Firm agrees to coordinate its Work with the work of any other separate professional services, contractors or with the work of the Town's own forces to avoid delaying or interfering with their work.

The Town reserves the right to terminate this Contract, or an individual project, based on the Firm's breach of this Contract (ex: schedule, responsiveness, quality of work, accuracy of documents etc.) The Town reserves the right to remove any or all work described in Exhibit C Scope of Services and Pricing Sheet at any time and for any reason, and no payment will be made by the Town to the Firm for any work removed.

2. Contract Insurance. Firm shall be required to purchase and maintain during its performance under this Contract insurance coverage as shown on the Insurance Requirements as stated in Exhibit B, which is incorporated herein by reference. With the exception of Worker's Compensation and Professional Liability policies, all insurance purchased shall have a specific endorsement, copy of which shall be provided to the Town, naming the Town as an additional insured and providing that such insurance will not be cancelled without providing thirty (30) days advance written notice to the Town.
3. Standard Terms and Conditions. The Standard Terms and Conditions attached hereto as Exhibit A shall be a part of this Contract and each project. Such Standard Terms and Conditions are hereby incorporated by reference, and all parties agree to be bound thereby.
4. Time for Performance of the Work. The Firm shall begin the as described in the task order or Notice to Proceed for each project from the Town. The Work must be completed as described in the task order or Notice to Proceed.
5. Payment for Services. In consideration of the Work and services as described in the Scope of Services, the Town will pay the Firm, in accordance with the submitted fee schedule attached hereto as Exhibit D, the sum described in each task order and Scope of Services provided, which shall be paid thirty (30) days after receipt of undisputed invoices delivered. The Firm will invoice the Town upon completion of the Work.

In witness thereof, the contracting parties, by their authorized agents, affix their signatures and seals at Huntersville, North Carolina, this _____ day of _____, 20____.

Firm

Town of Huntersville

Name:

Name of Contractor (type or print)

Town Manager

By:

(Signature)

Attest: _____
Town Clerk

Title:

This instrument has been pre-audited in the manner required by the Local Government Budget and Fiscal Control Act

Attest:

(Secretary, if a corporation)

Finance Director

EXHIBIT A
STANDARD TERMS & CONDITIONS

1. **Acceptance.** Contractor's acknowledgment of the terms of this Contract constitutes an agreement to: (i) all terms and conditions set forth or referenced herein, (ii) on any attachments hereto, (iii) any applicable solicitation documentation related to this Contract (including without limitation any request for proposals or invitation for bids or Contractor's response thereto) that deal with the same subject matter as this Contract, and (iv) any other terms and conditions of a written agreement signed by Contractor and the Town that deals with the same subject matter as this Contract (collectively, the "Contract Documents"). The terms and provisions set forth in the Contract Documents shall constitute the entire agreement between Contractor and the Town with respect to the purchase by the Town of the: (i) goods ("Goods") and/or (ii) services provided or work performed ("Services") as described in the Contract Documents. The agreements set forth in the Contract Documents are sometimes referred to herein as the "Contract." In the event of any conflict between any terms and conditions of the Contract Documents, the terms and conditions most favorable to the Town shall control. No additional or supplemental provision or provisions in variance herewith that may appear in Contractor's quotation, acknowledgment, invoice, or in any other communication from Contractor to the Town shall be deemed accepted by or binding on the Town. The Town hereby expressly rejects all such provisions which supplement, modify, or otherwise vary from the terms of the Contract Documents, and such provisions are superseded by the terms and conditions stated in the Contract Documents, unless and until the Town's authorized representatives expressly assent, in writing, to such provisions. Stenographic and clerical errors and omissions by the Town are subject to correction.
2. **Entire Agreement.** These terms and conditions and any other specifications contained in any other documents referenced shall constitute and represent the complete and entire agreement between the Town and Contractor and supersede all previous communications, either written or verbal with respect to the subject matter of this Contract.
3. **Changes, Additions, Deletions.** No changes, additions, deletions, or substitutions of scope of work, specifications, terms and conditions, quantity, unit of issue, delivery date, delivery charges or price will be permitted without the prior written approval from the Town.
4. **Relationship of the Parties.** The Contractor is an independent contractor and not an employee of the Town. The conduct and control of the work will lie solely with the Contractor. The Contract shall not be construed as establishing a joint venture, partnership, or any principal-agent relationship for any purpose between the Contractor and the Town. Employees of the Contractor shall remain subject to the exclusive control and supervision of the Contractor, which is solely responsible for their compensation.
5. **Prices.** If Contractor's price or the regular market price of any of the Goods or Services covered hereunder is lower than the price stated in the Contract Documents on the date of shipment of such Goods or performance of such Services, Contractor agrees to give the Town the benefit of such lower price on any such Goods or Services. In no event shall Contractor's price be higher than the price last quoted or last charged to the Town unless otherwise agreed in writing. No charges for transportation, boxing, crating, etc. are allowable unless such charges are included in the Contract Documents.
6. **Taxes.** Any applicable taxes shall be invoiced as a separate item.
7. **Substitutions.** No substitutions or cancellations shall be permitted without prior written approval from the Town.
8. **Indemnification.** To the greatest extent allowed by North Carolina law, the Contractor shall indemnify and hold harmless the Town, its officers, agents, employees and assigns from and against

all claims, losses, costs, damages, expenses, attorneys' fees ("Claims"). In the event that any portion of the Service performed under the Contract shall be defective in any respect whatsoever, the Contractor shall indemnify and save harmless the Town, its officers, agents, employees, and assigns from all loss or the payment of all sums of money, but only to the extent allowed by law.

9. **Invoices and Payment Terms.** It is understood and agreed that orders will be shipped at the established Contract prices in effect on dates orders are placed. Invoicing that does not comply with this provision will subject the Contract to cancellation. Upon satisfactory delivery of the Goods or satisfactory completion of the Work, all invoices and statements shall reference the Contract number and be submitted to: Town of Huntersville, Accounts Payable, PO Box 664, Huntersville, North Carolina, 28070. Payment terms are Net 30 days after receipt of correct, undisputed invoice or acceptance of Goods or Services, whichever is later.

When the Contract is for construction services, the Contractor will submit monthly Requests for Payment for Work performed, for review. The Request for payment shall be based upon the Contractor's estimate of the percentage of the total Work completed during the period represented on the Request for Payment. The Contractor must certify that the Work represented in the Contractor's Request for Payment has been completed in accordance with the Contract Documents and certify that the Request for Payment is appropriate for payment before the Town shall be obligated to make such payment to the Contractor. If any Request for Payment is disputed by the Town, in whole or in part, the Town shall provide a written explanation for such dispute to Contractor within five days of receipt of the certified Request for Payment and shall pay all undisputed amounts therein.

10. **Anti-Discrimination and Equal Employment.** During the performance of the Contract, Contractor shall comply with all federal and state requirements concerning fair and equal employment and shall not discriminate against or deny the Contract's benefits to any person on the basis of race, religion, color, creed, national origin, age, sex (including sexual orientation, gender identity, and pregnancy), disability or handicapping condition, or genetic information.
11. **Insurance.** The Contractor shall provide the insurance coverages shown on Exhibit B, attached hereto and incorporated herein by reference. The Contractor shall provide the Town with a North Carolina Certificate of Insurance and such endorsements as may be required by the Contract Documents prior to the commencement of any work under the Contract and agrees to maintain such insurance until the completion of the Contract. Such certificates of insurance shall be considered part of the Contract.
12. **Ethics in Public Contracting.** By submitting their prices and acceptance of this Contract, all Contractors certify that their bids are made without collusion or fraud and that they have not offered or received any kickbacks or inducements from any other supplier, manufacturer, or subcontractor in connection with their offer, and that they have not conferred on any public employee having official responsibility for this procurement transaction any payment, loan, subscription, deposit of money, services or anything of more than nominal value, present or promised, unless consideration of substantially equal or greater value was exchanged.
13. **Applicable Laws and Courts.** All Town Contracts for Services shall be governed in all respects by the laws of the State of North Carolina. All matters, whether sounding in contract or tort relating to the validity, construction, interpretation, and enforcement of the Contract, shall be governed in all respects by the laws of the State of North Carolina and venue shall be proper only in a court of competent jurisdiction located in Mecklenburg County, North Carolina. The Contractor represents and warrants that it shall comply with all applicable federal, state, and local laws, regulations, and orders, including, not limited to, licensure requirements.

14. **Codes and Permits.** When applicable, the Contractor shall obtain all required permits, give all required notices, and comply with all laws, ordinances, codes, rules, and regulations bearing on the conduct of the work under this contract. If the Contractor observes that the drawings and specifications are at variance therewith, he shall promptly notify the designer in writing. All work under this contract shall conform to the current North Carolina Building Code and other state and national codes as are applicable. If the Contractor performs any work knowing it to be contrary to such laws, ordinances, codes, rules and regulations, and without such notice to the Owner, he shall bear all cost arising therefrom.
15. **License Requirement.** If applicable, the Contractor must be a licensed General Contractor as required by North Carolina General Statutes Section 87-1 and must have a good ethical and professional standing with the North Carolina General Contractor's Licensing Board. The Contractor will be responsible for providing properly qualified, licensed (if required) personnel to complete the Work in accordance with the standard of care ordinarily used by members of the Contractor's profession practicing under similar circumstances and at the same time in Mecklenburg County.
16. **Strict Compliance.** The Town may at any time insist upon strict compliance with these terms and conditions notwithstanding any previous course of dealing or course of performance between the parties to the contrary.
17. **Assignment.** Contractor may not assign, pledge, or in any manner encumber Contractor's rights under this Contract or delegate the performance of any of its obligations hereunder, without Town's prior, express written consent.
18. **General Provisions.** The Town's remedies as set forth herein are not exclusive. Any delay or omission by the Town in exercising any right hereunder, or any waiver by the Town of any single breach or default hereunder, shall not be deemed to be a waiver of such right or of any other right, breach, or default.
19. **Warranties.** The Contractor warrants it shall adhere to all laws, codes, ordinances, and regulations of the United States, the State of North Carolina, the County of Mecklenburg, and the Town of Huntersville in the performance of the Services outlined in this Contract and any attached specifications. Contractor warrants that any finished work completed hereunder shall also adhere to all laws, codes, ordinances, and regulations of the United States, the State of North Carolina, the County of Mecklenburg, and the Town of Huntersville. Contractor warrants that all Services delivered hereunder will be free from defects in materials and workmanship and will conform strictly to the specifications, drawings, or samples specified or furnished. This warranty shall survive any inspection, delivery, acceptance, or payment by the Town of the Services and shall run to the Town and any user of the Services. Contractor warrants that all Services will be performed in a professional and workman like manner in accordance with best industry practices. This express warranty is in addition to Contractor's implied warranties of merchantability and fitness for a particular purpose which shall not be disclaimed. In addition to any other rights available at law or in equity, the Town shall be entitled to consequential and incidental damages.
20. **Quality and Workmanship.** All work shall be performed to the satisfaction of the Town. The work shall not be considered complete nor applicable payments rendered until the Town is satisfied with the Services provided.
21. **Default.** The Town may terminate the Contract, in whole or in part, immediately and without prior notice upon breach of the Contract by the Contractor. In addition to any other remedies available to the Town in law or equity, the Town may procure upon such terms as the Town shall deem appropriate, Services substantially similar to those so terminated, in which case the Contractor shall

be liable to the Town for any excess costs for such similar supplies or services and any expenses incurred in connection therewith.

22. **Termination for Convenience.** The Town shall have the right, without assigning any reason therefore, to terminate any work under the Contract, in whole or in part, at any time at its complete discretion by providing 10 days' notice in writing from the Town to Contractor. If the Contract is terminated by the Town in accordance with this paragraph, the Contractor will be paid in an amount which bears the same ratio to the total compensation as does the Services actually delivered or performed to the total originally contemplated in the Contract. The Town will not be liable to the Contractor for any costs for materials acquired or contracted for if such costs were incurred prior to the date of this Contract.
23. **Risk of Loss.** Risk of Loss for all supplies, materials, the Work performed, and the Project as it is being constructed, shall be on the Contractor until such time as substantial completion is achieved, and approved by the Town.
24. **No Third-Party Beneficiaries.** There shall be no intended nor incidental third-party beneficiaries of this Contract. Contractor shall include in all contracts, subcontracts, or other agreements relating to the Contract an acknowledgment by the contracting parties that the Contract creates no third-party beneficiaries.
25. **Exclusivity.** Nothing in this Contract shall require the Town to use the Contractor or prohibit the Town from soliciting third parties for the good or services provided in this Contract.
26. **Confidentiality.** The Contractor acknowledges the Town is subject public records law and no term shall be inconsistent with N.C.G.S. §132 et al.
27. **Valid Contract for Services.** In order for a Contract for Services of the Town to be valid, it must be executed by the Town Manager or his or her authorized designee, and must be pre-audited in that manner required by the Local Government Budget and Fiscal Control Act, as the same may be amended.
28. **Verification of Work Authorization.** Contractor shall comply with, and require all contractors and subcontractors to comply with, the requirements of Article 2 of Chapter 64 of the North Carolina General Statutes, "Verification of Work Authorization," sometimes known as E-verify, for all contractors and subcontractors.
29. **Iran Divestment List.** With the execution hereof, Contractor, certifies that they are not on the Iran Final Divestment List created by the N.C. State Treasurer pursuant to N.C.G.S. § 147-86.58, and will not contract with anyone on such List in performance of the work hereunder.
30. **Buyer.** All references to Buyer or Town, throughout these terms and conditions, shall refer to the Town of Huntersville, North Carolina.
31. **Contractor.** All references to Contractor, Seller, or Firm throughout these terms and conditions shall refer to the contractor identified on page 1 of this Contract.
32. **Availability of Funds.** Any and all payments to the Contractor are dependent upon and subject to the availability of funds to the Town for the purpose set forth in this agreement.
33. **Severability.** If any provision of this Contract is found to be invalid or unlawful, then remainder of this Contract shall not be affected thereby, and each remaining provision shall be valid and enforced to the fullest extent permitted by law.
34. **Companies that Boycott Israel.** With the execution hereof, Contractor, certifies that they are not on the Companies that Boycott Israel List created by the N.C. State Treasurer pursuant to N.C.G.S. § 147-86.80, and will not contract with anyone on such List in performance of the work hereunder.
35. **Governmental Immunity.** Nothing contained in this Contract shall constitute a waiver of the Town's governmental immunity or of any limitation on liability or damages created by law.

ADDITIONAL TERMS AND CONDITIONS FOR FEDERAL CONTRACTS

For contracts using federal funds, the following additional terms and conditions shall apply:

1. **Davis-Bacon Act.** For all contracts in excess of \$2,000.00 for construction, alteration, or repair, including painting and decorating, of public buildings or public works, the Contractor shall comply with the Davis-Bacon Act, including payment of no less than the locally prevailing wages as determined by the Secretary of Labor. The contract shall not be valid unless the current prevailing wage as determined by the North Carolina Department of Labor is accepted. The Contractor shall also be prohibited from inducing, by any means, any person employed in the construction, completion, or repair of public work, to give up any part of the compensation to which he or she is otherwise entitled. The Town shall report all suspected or reported violations to the Federal awarding agency.
2. **Contract Work Hours and Safety Standards Act.** For contracts in excess of \$100,000 that involve the employment of mechanics or laborers, each contractor must be required to compute the wages of every mechanic and laborer on the basis of a standard work week of 40 hours. Work in excess of the standard work week is permissible provided that the worker is compensated at a rate of not less than one and a half times the basic rate of pay for all hours worked in excess of 40 hours in the work week. For construction work, no laborer or mechanic must be required to work in surroundings or under working conditions which are unsanitary, hazardous, or dangerous.
3. **Funding Agreements.** If a Federal award meets the definition of "funding agreement" under 37 C.F.R. § 401.2(a) and the Town or Contractor enter into a contract with a small business firm or nonprofit organization regarding the substitution of parties, assignment or performance of experimental, developmental, or research work under that "funding agreement," the recipient or subrecipient must comply with the requirements of 37 C.F.R. Part 401.
4. **Clean Air Act and Federal Water Pollution Control Act.** Contractor shall comply with all applicable standards, orders, or regulations issued pursuant to the Clean Air Act and Federal Water Pollution Control Act as amended for any Contract in excess of \$150,000.00.
5. **Debarment and Suspension.** Contractor acknowledges and warrants that it is not listed on the governmentwide exclusions in the System Award Management (SAM) Exclusions, in accordance with the OMB guidelines at 2 C.F.R. § 180 for "Debarment and Suspension."
6. **Byrd Anti-Lobbying Amendment (31 U.S.C. § 1352).** For an award exceeding \$100,000, Contractors must file the required certification. Each tier certifies to the tier above that it will not and has not used Federal appropriated funds to pay any person or organization for influencing or attempting to influence an officer or employee of any agency, a member of Congress, officer or employee of Congress, or an employee of a member of Congress in connection with obtaining any Federal contract, grant or any other award covered by 31 U.S.C. § 1352. Each tier must also disclose any lobbying with non-Federal funds that takes place in connection with obtaining any Federal award. Such disclosures are forwarded from tier to tier up to the Town.
7. **Prohibition on Certain Telecommunications and Video Surveillance Services or Equipment.** The Contractor warrants that their systems or equipment are not covered under telecommunication equipment as described in Public Law 115-232.
8. **Domestic Preference for Procurements.** As appropriate and to the extent consistent with law, the Contractor will, to the greatest extent practicable under a Federal award, provide a preference for the purchase, acquisition, or use of goods, products, or materials produced in the United States (including

but not limited to iron, aluminum, steel, cement, and other manufactured products), as required under 2 C.F.R. § 200.322.

9. **Procurement of Recovered Material.** The Contractor agrees to comply with section 6002 of the Solid Waste Disposal Act, as amended by the Resource Conservation and Recovery Act. The requirements of Section 6002 include procuring only items designated in guidelines of the Environmental Protection Agency (EPA) at 40 C.F.R. Part 247 that contain the highest percentage of recovered materials practicable, consistent with maintaining a satisfactory level of competition, where the purchase price of the item exceeds \$10,000; procuring solid waste management services in a manner that maximizes energy and resource recovery; and establishing an affirmative procurement program for procurement of recovered materials identified in the EPA guidelines.
10. **Conflict of Interest.** The Contractor agrees to be bound by the Town's Uniform Guidance Conflict of Interest Policy, which is included herein by reference.
11. **Equal Employment Opportunity.** Except as otherwise provided under 41 CFR Part 60, all contracts that meet the definition of "federally assisted construction contract" in 41 CFR Part 60-1.3 include, by reference, the equal opportunity clause provided under 41 CFR 60-1.4(b). The Contractor agrees to abide by 41 CFR 60-1.4(b) during the performance of the contract¹.

¹ 60 CFR Part 60-1.4(b) can be accessed at: [https://www.ecfr.gov/current/title-41/subtitle-B/chapter-60/part-60-1/subpart-A/section-60-1.4#p-60-1.4\(b\)](https://www.ecfr.gov/current/title-41/subtitle-B/chapter-60/part-60-1/subpart-A/section-60-1.4#p-60-1.4(b))

EXHIBIT B
MINIMUM INSURANCE REQUIREMENTS

The Work under this Contract shall not commence until the Contractor has obtained all required insurance and verifying certificates of insurance have been approved in writing by the Town. Except for Worker's Compensation and Professional Liability policies, the Town shall be named as additional insured on all policies. These certificates shall document that coverages afforded under the policies will not be cancelled, reduced in amount or coverages eliminated until at least thirty (30) days after mailing written notice, by certified mail, return receipt requested, to the insured and the Town of such alteration or cancellation. If endorsements are needed to comply with the notification or other requirements of this article copies of the endorsements shall be submitted with the certificates.

a. Worker's Compensation and Employer's Liability

The Contractor shall provide and maintain, until final acceptance, workmen's compensation insurance, as required by law, as well as employer's liability coverage with minimum limits of \$100,000.

b. Comprehensive General Liability Insurance

The Contractor shall provide and maintain, until final acceptance, comprehensive general liability insurance, including coverage for premises operations, independent contractors, completed operations, products and contractual exposures, as shall protect such contractors from claims arising out of any bodily injury, including accidental death, as well as from claims for property damages which may arise from operations under this contract, whether such operations be by the Contractor or by any subcontractor, or by anyone directly or indirectly employed by either of them and the minimum limits of such insurance shall be as follows:

Bodily Injury: \$1,000,000 per occurrence/\$2,000,000 aggregate
Professional Liability: \$1,000,000 per occurrence/\$2,000,000 aggregate
Property Damage: \$1,000,000 per occurrence/\$2,000,000 aggregate

Such coverage for completed operations must be maintained for at least two (2) years following final acceptance of the Work performed under the contract.

c. Deductible

Any deductible, if applicable to loss covered by insurance provided, is to be borne by the Contractor.

d. Other Insurance

The Contractor shall obtain such additional insurance as may be required by the Town or by the General Statutes of North Carolina including motor vehicle insurance, in amounts not less than the statutory limits.

e. Proof of Carriage

The Contractor shall furnish the Town with satisfactory proof of carriage of the insurance required before written approval is granted by the Town.

FORMAL BID PROPOSAL
TOWN OF HUNTERSVILLE, NC
BID MUST BE SUBMITTED BY: JULY 12, 2023 @ 2 PM
UNDERGROUND & DIRECTIONAL BORING UNITS FY24

EXHIBIT C
SCOPE OF SERVICES & PRICING SHEET

COMPANY SUBMITTING BID: Lamberts Cable Splicing Co, LLC
REPRESENTATIVE NAME: Billy Butts
CONTACT NUMBER: (252) 414-1980
E-MAIL ADDRESS: billy.butts@lambertcable.com

I. DIRECTIONAL BORING UNITS		UOM	Qty	Price Each	Total Price
Pipe Installation Units					
1	(1) 1" - 1 1/2" HDPE	Linear Ft	5000	\$ 10.50	\$ 52,500.00
2	(1) 2" - 2 1/2" HDPE	Linear Ft	7000	\$ 13.12	\$ 91,840.00
3	(2) 2" - 2 1/2" HDPE	Linear Ft	400	\$ 21.00	\$ 8,400.00
4	(3) 2" - 2 1/2" HDPE	Linear Ft	1250	\$ 33.60	\$ 42,000.00
5	(4) 2" - 2 1/2" HDPE	Linear Ft	1250	\$ 36.25	\$ 45,312.50
6	(5) 2" - 2 1/2" HDPE	Linear Ft	1250	\$ 42.00	\$ 52,500.00
7	(1) 2" - 2 1/2" & (1) 1" - 1 1/2" HDPE	Linear Ft	400	\$ 15.75	\$ 6,300.00
8	(1) 2" - 2 1/2" & (2) 1" - 1 1/2" HDPE	Linear Ft	400	\$ 17.32	\$ 6,928.00
9	(2) 2" - 2 1/2" & (1) 1" - 1 1/2" HDPE	Linear Ft	1250	\$ 23.10	\$ 28,875.00
10	(2) 2" - 2 1/2" & (2) 1" - 1 1/2" HDPE	Linear Ft	1250	\$ 26.25	\$ 32,812.50
11	(3) 2" - 2 1/2" & (1) 1" - 1 1/2" HDPE	Linear Ft	400	\$ 35.70	\$ 14,280.00
12	(4) 2" - 2 1/2" & (1) 1" - 1 1/2" HDPE	Linear Ft	1250	\$ 42.00	\$ 52,500.00
13	(5) 2" - 2 1/2" & (1) 1" - 1 1/2" HDPE	Linear Ft	400	\$ 46.20	\$ 18,480.00
14	(1) 3" HDPE	Linear Ft	2500	\$ 21.00	\$ 52,500.00
15	(2) 3" HDPE	Linear Ft	500	\$ 27.30	\$ 13,650.00
16	(3) 3" HDPE	Linear Ft	1500	\$ 37.80	\$ 56,700.00
17	(4) 3" HDPE	Linear Ft	7500	\$ 33.60	\$ 252,000.00
18	(1) 3" & (1) 1" - 1 1/2" HDPE	Linear Ft	400	\$ 23.10	\$ 9,240.00
19	(1) 3" & (2) 1" - 1 1/2" HDPE	Linear Ft	400	\$ 25.20	\$ 10,080.00
20	(1) 3" & (1) 2" - 2 1/2" & (1) 1" - 1 1/2" HDPE	Linear Ft	400	\$ 29.40	\$ 11,760.00
21	(1) 3" & (2) 2" - 2 1/2" HDPE	Linear Ft	400	\$ 34.65	\$ 13,860.00
22	(1) 3" & (3) 2" - 2 1/2" HDPE	Linear Ft	1250	\$ 37.80	\$ 47,250.00
23	(1) 3" & (4) 2" - 2 1/2" HDPE	Linear Ft	400	\$ 42.00	\$ 16,800.00
24	(4) 3" & (1) 2" - 2 1/2" HDPE	Linear Ft	1250	\$ 37.80	\$ 47,250.00
25	(1) 4" HDPE	Linear Ft	2000	\$ 23.10	\$ 46,200.00
26	(2) 4" HDPE	Linear Ft	900	\$ 35.70	\$ 32,130.00
27	(3) 4" HDPE	Linear Ft	1000	\$ 42.00	\$ 42,000.00
28	(1) 4" & (1) 2" - 2 1/2" HDPE	Linear Ft	400	\$ 27.30	\$ 10,920.00
29	(1) 4" & (1) 2" - 2 1/2" & (1) 1" - 1 1/2" HDPE	Linear Ft	400	\$ 29.40	\$ 11,760.00
30	(1) 4" & (2) 2" - 2 1/2" HDPE	Linear Ft	400	\$ 35.70	\$ 14,280.00
31	(1) 6" HDPE	Linear Ft	5000	\$ 33.60	\$ 168,000.00
32	Rock Adder for Directional Bore	Linear Ft	2000	\$ 78.75	\$ 157,500.00
Pipe Installation Units Total				\$	\$ 1,466,608.00

II. General Construction Units					UOM	Qty	Price Each	Total Price
33	Asphalt, Cut & Remove 0" – 5" thick				Sq Ft.	2000	\$ 15.75	\$ 31,500.00
34	Asphalt, Cut & Remove 6" - 10" Thick				Sq. Ft.	500	\$ 26.25	\$ 13,125.00
35	Concrete, Cut & Remove 0" – 4" Thick				Sq. Ft.	2000	\$ 15.75	\$ 31,500.00
36	Concrete, Cut & Remove 5" – 8" Thick				Sq. Ft.	500	\$ 31.50	\$ 15,750.00
37	Concrete, Replace 3,000 psi 4" Thick				Sq. Ft.	2000	\$ 15.75	\$ 31,500.00
38	Locates, 12" Core Hole & Restore				Each	200	\$ 157.50	\$ 31,500.00
39	Dig, Barricade & Restore 4' x 4' x 3' Pit				Each	100	\$ 315.00	\$ 31,500.00
40	Locates, 24" Core Hole & Restore				Each	100	\$ 315.00	\$ 31,500.00
41	Locate, Existing Conduits by Excavating, Removal				Hour	100	\$ 162.75	\$ 16,275.00
42	Excavating and Relocating Existing Conduits Up to 6"				Hour	100	\$ 144.75	\$ 14,475.00
43	Excavation of existing conduit due to obstructions that would prevent the installation of cable by normal means				Hour	100	\$ 162.94	\$ 16,294.00
44	Install pulling string by use of pneumatic tooling in conduit up to 6"				Hour	100	\$ 150.68	\$ 15,068.00
					General Construction Units Total			\$ 279,987.00
III. Open Trench Units								
45	Open Trench 18" W x 36" D				Linear Ft	30000	\$ 4.20	\$ 126,000.00
46	Open Trench 18" W x 48" D				Linear Ft	25000	\$ 4.72	\$ 118,000.00
47	Open Trench 24" W x 60" D				Linear Ft	5000	\$ 5.25	\$ 26,250.00
48	Rock Adder for Open Trench				Linear Ft	500	\$ 157.50	\$ 78,750.00
49	Add 1" – 1 ½" Duct to Trench				Linear Ft	10000	\$ 1.21	\$ 12,100.00
50	Add 2" – 2 ½" Duct to Trench				Linear Ft	25000	\$ 1.21	\$ 30,250.00
51	Add 3" Duct to Trench				Linear Ft	5000	\$ 1.41	\$ 7,050.00
52	Add 4" Duct to Trench				Linear Ft	1500	\$ 1.41	\$ 2,115.00
53	Add 6" Duct to Trench				Linear Ft	750	\$ 1.73	\$ 1,297.50
					Open Trench Units Total			\$ 401,812.50
IV. MATERIALS INSTALLATION UNITS								
a. Boxes & Pads Units								
54	Box, Splice, Streetlight, 10" x 15", w/Connectors				Each	200	\$ 26.25	\$ 5,250.00
55	Enclosure, Fiberglass, 15 kV				Each	50	\$ 48.25	\$ 2,412.50
56	Junction, 15 kV, 200A, 2-Point				Each	50	\$ 267.75	\$ 13,387.50
57	Junction, 15 kV, 200A, 3-Point				Each	50	\$ 325.50	\$ 16,275.00
58	Junction, 15 kV, 200A, 4-Point				Each	25	\$ 325.50	\$ 8,137.50
59	Junction, 15 kV, 600A, 3-Point				Each	25	\$ 362.50	\$ 9,062.50
60	Pad, Switchgear, 15 kV, PME-9, & ME-11				Each	15	\$ 478.80	\$ 7,182.00
61	Pad, Transformer, 1-Ph				Each	65	\$ 144.37	\$ 9,384.05
62	Pad, Transformer, 3-Ph				Each	25	\$ 334.43	\$ 8,360.75
63	Pedestal, Secondary, UG, 1-Ph				Each	10	\$ 75.15	\$ 751.50
					Boxes & Pads Units Total			\$ 80,203.30

b. Streetlights & Security Lights Units					
	UOM	Qty	Price Each	Total Price	
64	Fixture, Streetlight, Decorative	Each	100	\$ 78.75	\$ 7,875.00
65	Fixture, Street or Security, Standard, w/arm	Each	50	\$ 81.25	\$ 4,062.50
66	Pole, AL, Decorative, 10' - 16' for Streetlight	Each	100	\$ 157.50	\$ 15,750.00
67	Pole, AL or Fiberglass, Standard, 20' 30', for SL	Each	50	\$ 210.00	\$ 10,500.00
68	Foundation, Pole, Direct Bury, for Streetlight	Each	100	\$ 315.00	\$ 31,500.00
Streetlights & Security Lights Total				\$	\$ 69,687.50
c. Transformers & Switchgear Units					
69	25 KVA - 100 KVA 1-Ph Install and Connect	Each	75	\$ 143.85	\$ 10,788.75
70	167 KVA 1-Ph Install & Connect	Each	10	\$ 236.25	\$ 2,362.50
71	75 KVA - 500 KVA 3-Ph Install & Connect	Each	10	\$ 333.90	\$ 3,339.00
72	750 KVA & Larger 3-Ph Install & Connect	Each	5	\$ 378.00	\$ 1,890.00
73	Grounding Assembly, for Pad-Mtd. Enclosures	Each	120	\$ 62.00	\$ 7,440.00
74	PME-9 Switchgear Install & Connect	Each	10	\$ 488.25	\$ 4,882.50
75	PME-11 Switchgear Install & Connect	Each	10	\$ 512.60	\$ 5,126.00
Transformers & Switchgears Total				\$	\$ 35,828.75
d. Termination Units					
76	Adapter, 15 kV, 200A, Reducing	Each	100	\$ 31.50	\$ 3,150.00
77	Bracket, Insulated Standoff, 15 kV	Each	25	\$ 52.30	\$ 1,307.50
78	Bracket, Insulated Standoff, Feed-Thru, 15 kV	Each	25	\$ 52.30	\$ 1,307.50
79	Bushing Insert, 15 kV, Loadbreak, 200A	Each	150	\$ 52.30	\$ 7,845.00
80	Bushing Insert, 15 kV, LB, 200A, Feed-Thru	Each	50	\$ 52.30	\$ 2,615.00
81	Cap, Insulated, Protective, 15 kV, 200A	Each	100	\$ 52.30	\$ 5,230.00
82	Cap, Insulated, Protective, 15 kV, 600A	Each	50	\$ 52.30	\$ 2,615.00
83	Elbow, 15 kV, 200A, Loadbreak	Each	100	\$ 120.75	\$ 12,075.00
84	Elbow, 15 kV, 600 A Deadbreak, T-Body	Each	50	\$ 141.75	\$ 7,087.50
85	Elbow, Arrester, 15 kV	Each	35	\$ 79.30	\$ 2,775.50
86	Elbow, Fused, 15 kV	Each	25	\$ 162.75	\$ 4,068.75
87	Riser, House, 200A, Install & Connect	Each	200	\$ 132.00	\$ 26,400.00
88	Wire, Secondary, Any Size	Each	1000	\$ 4.85	\$ 4,850.00
Terminations Total				\$	\$ 81,326.75
e. Wire & Cable Units					
89	(1) 1/0 Primary, AL, 15 kV, JCN, URD	Linear Ft	50000	\$ 1.41	\$ 70,500.00
90	(3) 1/0 Primary, AL, 15 kV, JCN, URD	Linear Ft	5000	\$ 3.30	\$ 16,500.00
91	2/0 TPX Aluminum, 600V, UG	Linear Ft	3000	\$ 1.20	\$ 3,600.00
92	#2 STR, Copper, Bare	Linear Ft	10000	\$ 1.05	\$ 10,500.00
93	350 QPX, Aluminum, 600V, UG	Linear Ft	25000	\$ 1.45	\$ 36,250.00
94	4/0 TPX, Aluminum, 600V, UG	Linear Ft	20000	\$ 1.25	\$ 25,000.00
95	4/0 QPX, Aluminum, 600V, UG	Linear Ft	35000	\$ 1.45	\$ 50,750.00
96	#6/3 Streetlight, Aluminum, 600V, UG	Linear Ft	10000	\$ 1.25	\$ 12,500.00
97	(1) 750 MCM Primary, AL, 15 kV, JCN, URD	Linear Ft	10000	\$ 1.73	\$ 17,300.00
98	(3) 750 MCM Primary, AL, 15 kV, JCN, URD	Linear Ft	30000	\$ 7.50	\$ 225,000.00
Wire & Cable Install Total				\$	\$ 467,900.00
TOTAL BID				\$	\$ 2,883,353.80

**Town of Huntersville
Town Board
August 7, 2023**

To: Town Board

From: Barry Graham, Chief of Police

Date: August 7, 2023

Subject: CMPD Dispatch Contract

EXPLAIN REQUEST:

Request action to approve the communications contract between CMPD and HPD for 911 and dispatch services.

ACTION RECOMMENDED:

Approve the Town Manager and the Chief of Police to sign the agreement between Charlotte-Mecklenburg Police Department and the Huntersville Police Department to provide 911 and radio communication services.

FINANCIAL IMPLICATIONS:

\$600,000 for FY24
\$864,372 for FY25

ATTACHMENTS:

1. 2024000021 ACM Packet Comm and Records Management (Town of Huntersville) 7.31.2023 (002)



City of Charlotte
Contract Document Routing Form Submission

This Contract Document Routing Form is required for all contract documents.

Department: <u>Charlotte Mecklenburg Police Department</u>	MUNIS Contract #: <u>2024000021</u>	Document Type: <u>Contract</u>
Vendor Name: <u>Town of Huntersville</u>		Amendment # <u></u>
Contract Name: <u>Communication and Records Management Services</u>		
Total Contract Value: <u>\$864,371.26</u>	Value of Approval: <u>\$864,371.26</u>	
Year of Term: <u>1</u>	Contract Term: <u>3-YR + TWO 3-YR RENEWALS</u>	Routing Date: <u>7/12/2023</u>

Does this document require Pre-Audit per [New Pre-Audit Requirements Memo](#)?
Refer to [Pre-Audit Guide](#) when determining appropriate process.

No Financial Obligation

Provide a brief explanation of the submission, including any special circumstances that apply
***REVENUE CONTRACT: THIS IS A REVENUE CONTRACT WITH THE TOWN OF HUNTERSVILLE TO
PROVIDE COMMUNICATIONS AND RECORDS MANAGEMENT SERVICES FOR AN INITIAL 3-YEAR
TERM.

Primary Contact
Palafox, Euge

Primary Contact Phone:
(704) 336-7690

Routing Contact
Palafox, Euge

Routing Contact Phone:
(704) 336-7690

Required Department Head Approval	
Department Head Signature: <u><i>Johnny Jennings</i></u>	Date Signed: <u>July 21, 2023</u>
Department Head Name: <u>Johnny Jennings</u>	
Additional Department Signature: _____ (if applicable)	
Title: _____ Date: _____	
FOR CONTRACTS WITH A TOTAL VALUE OF \$50,000+: REQUIRED APPROVAL PRIOR TO CITY MANAGER REVIEW	
City Procurement Signature: <u><i>Jennifer Walter</i>, C.P.M.</u>	Date Signed: <u>7/18/2023</u>
Status: <u>Approved</u>	

FINANCIAL SYSTEM CONTRACT CALCULATION ALLOCATION

Change	Description	Amount	Running Total
Enter Change Num...	Select...		\$0.00

Total Amount: \$0.00

Vendor Certification Status

DBE	AC-DBE	MBE	WBE	SBE	MSBE	MWSBE
☐	☐	☐	☐	☐	☐	☐
DBE%	AC-DBE%	MBE%	WBE%	SBE%	MSBE%	MWSBE%
Committed Utilization						
DBE%	AC-DBE%	MBE%	WBE%	SBE%	MSBE%	MWSBE%

Supporting Documentation Checklist

Departments must complete this checklist as part of their Contract/Amendment/Change Order Routing Packet submission, to ensure that all required steps are completed, and all supporting documentation has been provided. Check off each item or indicate "N/A" as applicable.

Have you included the following documents in your completed Routing Packet and uploaded for City Procurement review?

Routing Packet Components	Required Documentation:		
	DEPARTMENT	CITY PROCUREMENT	
	<u>Yes</u>	<u>Yes</u>	Contract, Amendment, or Change Order Signed by Vendor and Risk Management
	<u>N/A</u>	<u>N/A</u>	Certificate(s) of Insurance
	<u>N/A</u>	<u>N/A</u>	Documentation of Inclusion Review (M/W/SBE or DBE/AC-DBE)
	If Applicable Documentation (Write "N/A" if not applicable)		
	DEPARTMENT	CITY PROCUREMENT	
	<u>N/A</u>	<u>N/A</u>	Approved Request for Council Action (RCA)
	<u>N/A</u>	<u>N/A</u>	Approved Waiver Form
	<u>N/A</u>	<u>N/A</u>	Approved Exception Form
<u>N/A</u>	<u>N/A</u>	Innovation & Technology review and approval	

Have you uploaded the following documents in your completed Routing Packet and uploaded for City Procurement review?

Supporting Documentation Components	Required Documentation		
	DEPARTMENT	CITY PROCUREMENT	
	<u>N/A</u>	<u>N/A</u>	Evaluation Summary including pricing evaluation, summary of evaluation proceedings, etc.
	<u>N/A</u>	<u>N/A</u>	Solicitation Document
	<u>N/A</u>	<u>N/A</u>	Copy of Advertisement of Screenshot
	If Applicable Documentation (Write "N/A" if not applicable)		
	DEPARTMENT	CITY PROCUREMENT	
	<u>N/A</u>	<u>N/A</u>	Addenda
	<u>N/A</u>	<u>N/A</u>	Capital Outlay or Approved Change in Capital Outlay (CICO)

Respond to the additional questions below:

Additional Considerations	Additional Considerations		
	DEPARTMENT	CITY PROCUREMENT	
	<u>No</u>	<u>No</u>	Does this project require special financing?
	<u>No</u>	<u>No</u>	Does this include a lease? (City is lessee or lessor of property, equipment, goods, etc.)
	<u>No</u>	<u>No</u>	Will this project be funded in whole or in part with federal funds? (including pass-through grant funds)
	<u>No</u>	<u>No</u>	Did you incorporate Uniform Guidance requirements into your procurement and contract document Per Federal Uniform Guidance Policy (FIN33)
	<u>No</u>	<u>No</u>	Does this project incorporate an electronics receipt or payment component?

	<u>N/A</u>	<u>N/A</u>	If yes above: Has the E-Business Team been engaged in project? Per FIN-9: E-Business Receipts and Payments Policy
	<u>No</u>	<u>No</u>	Has Risk Management reviewed the Insurance coverages during solicitation or contract development?

**STATE OF NORTH CAROLINA
COUNTY OF MECKLENBURG**

**AGREEMENT TO PROVIDE
COMMUNICATION AND
RECORD MANAGEMENT
SERVICES**

This Agreement to Provide Communication and Record Management Services (the "Agreement") is entered into and made effective this _ day of _____, 2023 (the Effective Date) by and between the City of Charlotte, specifically, the Charlotte Mecklenburg Police Department ("CMPD"); and the Town of Huntersville, specifically, the Huntersville Police Department ("HPD").

RECITALS

WHEREAS, the City of Charlotte Police Department and the Mecklenburg County Police Department were consolidated as the CMPD on October 1, 1993 pursuant to Article 20, Chapter 160A of the General Statutes of North Carolina and Chapter 1170, Session Laws of 1969.

WHEREAS, the Town of Huntersville and Chief of the HPD wish to utilize CMPD police services specifically the CMPD communication and record management systems; and

WHEREAS, the City of Charlotte and the CMPD agree to provide communication and record management services as set forth below.

NOW, THEREFORE, for good and valuable consideration, the receipt and sufficiency of which is hereby acknowledged, and in further consideration of the covenants and representations contained herein, the parties agree as follows:

AGREEMENT

1. DESCRIPTION OF SERVICES.

The CMPD will provide communication and record management services, to the HPD. The HPD agrees to pay certain fees and costs associated with the use of said services.

2. TERM.

Unless terminated sooner in accordance with the terms contained herein, this Agreement shall commence on the Effective Date and continue in effect until June 30, 2026. This Agreement shall automatically renew for two (2) additional consecutive three (3) year terms up to 2032, unless either party shall notify the other party, in writing, of its intention not to renew, which notice shall be given at least six months prior to the end of the then current term. Nevertheless, either party may terminate this Agreement by providing one (1) year prior written notice to the other party. Upon the effective date of any termination, HPD shall pay any accrued but unpaid charges under this Agreement to CMPD and thereafter the parties shall have no further obligation to the other. HPD shall retain any equipment owned or leased by it.

3. SERVICES PROVIDED BY CMPD.

3.1 Services

- 3.1.1 HPD will use CMPD Computer Aided Dispatch System and applications including CMPD Knowledge Based Community Oriented Policing System (KBCOPS), I/Netviewer, I/Mobile, and Stop Data.
- 3.1.2 HPD will be required to pay directly to the provider for third party licenses, service and training fees for Verizon, NC DCI, and their connectivity service provider.
- 3.1.3 HPD will be required to maintain secured connectivity with the City of Charlotte network with their chosen service provider in order to receive services.
- 3.1.4 HPD will pay CMPD for Information Technology Services as set forth in Exhibit A.
- 3.1.5 HPD will comply with the Management Control Agreement as set for in Exhibit B.
- 3.1.6 HPD will require all Users abide by City of Charlotte Cyber Security Policy, Section 7, as applicable (Exhibit C), and comply with established CJIS requirements.
- 3.1.7 CMPD will provide train the trainer instruction for the HPD designated personnel on all applicable systems and application changes and updates.
- 3.1.8 CMPD's policies and procedures comply with applicable standards established by the Commission on Accreditation for Law Enforcement

Agencies Inc. (CALEA) related to the administration and operations of the functions of a police communications center.

3.2 Calls for Service to the HPD

- 3.2.1 CMPD will answer all calls from HPD Officers for the purpose of recording their location and contact information.
- 3.2.2 CMPD will respond to and assist HPD Officers when requested.
- 3.2.3 All information will be entered into the CMPD's Computer-Aided Dispatch System (hereinafter referred to as "CAD"). CAD will track each HPD Officer call and time stamp each call.
- 3.2.4 CMPD dispatchers will monitor emergency communications generated by HPD officers and will make proper responses and notifications.
- 3.2.5 HPD will pay for E-911 and dispatch services based on the average call volume. Based on the average call volume from prior years, HPD will pay the amount set forth in Exhibit A for 2023 and 2024 to reach 100% of actual cost. At the end of this period, CMPD will utilize the same formulae and methodology as was used in computing the original charges for these services to compute the charges annually not to exceed 5% total increase.
- 3.2.6 HPD radios must have CMPD radio talk groups approved by the CMPD. HPD shall be responsible for all costs associated with their radios HPD must remain in compliance with the Charlotte-Mecklenburg Radio Communication Council.
- 3.2.7 CMPD Communications will provide DCI support and connectivity for DCI related communications and messaging.

3.3 Telecommunications Circuit and CMPD Network

- 3.3.1 Access to the City of Charlotte network will be via a VPN secure tunnel over the internet. HPD will have access to Report Beam, I/Net Viewer (CAD) product, Mobile (CAD) product, KBCOPS Records Management System, and CMPD Stop Data. KBCOPS would be used to meet Records Management System needs to include full access and usage of all KBCOPS

modules. HPD will provide modems and laptops for the connectivity. CMPD will provide software to install on HPD mobile computers.

- 3.3.2 Access to the City of Charlotte network from HPD desktop computers will be blocked if the City detects a virus attack. Access will be restored after proof is provided by HPD to the City of both virus eradication and virus/security updates have been installed on all HPD computer equipment connected to the City of Charlotte network.

3.4 Upgrades

To maintain the highest level of technical service the CMPD periodically performs upgrades to its hardware and software. CMPD will provide HPD with as much advanced notice as possible when these upgrades will occur. HPD agrees and understands that it must upgrade their equipment as necessary to remain compatible with the CMPD as a condition to receive continued service under this Agreement.

3.5 Training

If requested, and upon reasonable notice, CMPD will provide train the trainer instruction for HPD designated personnel for services associated with this Agreement. The training includes the use of applications made available by the CMPD and the DCI approved certification program.

3.6 Computer Logs

Upon 24-hour notice, CMPD will make relevant computer logs available to HPD for inspection or duplication. The CMPD retains all recorded voice-logged communications for a maximum period of sixty (60) days from the date of occurrence. Upon 24-hour notice, CMPD will provide CD, cassette, or CODEC of requested voice-logged communication recordings to HPD.

3.7 Public Records Request

CMPD will forward all public records requests concerning HPD cases to the Chief of HPD, or designee, for response.

4. OBLIGATIONS OF THE HPD.

4.1 Employee Roster

HPD shall provide the CMPD a current list of employees requiring access to the computer systems at the time of execution of this Agreement. The

HPD shall immediately notify the CMPD when an HPD employee with authorized access to the computer systems has separated from employment. HPD shall immediately notify the CMPD when a new HPD employee requires access to the computer systems. HPD employees using any CMPD system will sign and abide by the CMPD User Agreement.

4.2 On-line and Telecommunication Costs

HPD will be responsible for the purchase and cost associated with additional hardware (routers, firewall, etc.) required to establish the telecommunications circuit with the CMPD. All network and communications software must meet City of Charlotte specifications.

4.3 Purchase and Maintenance of Equipment

HPD will be responsible for placing their 800 MHz radios on the Charlotte-Mecklenburg Radio System. HPD agrees to use laptops in their patrol vehicles to access the CAD system. Laptops purchased or leased by HPD must comply with CMPD Computer Technology Solutions Division (CTS) laptop specifications.

4.4 Additional Data Requests Costs

All requests for additional data, not currently provided, will be reviewed by CMPD Computer Technology Solutions Division (CTS) to determine whether data is available, can be retrieved and a permanent solution can be put into place to provide the data in real time. CTS will notify the requester of the number of billable hours to complete the request for approval to move forward.

4.5 Payment

HPD agrees to pay for services set forth in this Agreement according to the payment schedule set forth in Exhibit A. The payment schedule will be adjusted as provided in section 3.2.5 of this Agreement for any subsequent extensions beyond the initial term.

5. MAINTENANCE RESPONSIBILITY.

5.1 HPD shall be responsible for the maintenance, repair, and upkeep of all communications equipment that is owned, possessed, or used by HPD and its officers, employees, or agents.

5.2 CMPD will provide limited technical support for the duration of the Agreement. The term "limited" shall mean that HPD technical personnel will be called first for technical support. If needed, the CMPD CTS Customer Support Team will work on the problem(s). If CTS can correct the

problem(s) quickly, it will do so. If the problem(s) require action such as dealing with one of HPD's vendors, i.e., the firm that installed HPD's wireless or extended troubleshooting due to something unique to HPD then HPD shall correct the problem(s).

5.3 HPD technical personnel will be called first for technical support. Service requests may be escalated to CMPD CTS Customer Support software issues. CTS Customer Support Team services are available for telephone or email assistance Monday through Friday, 8 a.m. to 5 p.m. HPD officers requiring emergency technical support after hours may contact City of Charlotte's IT support desk.

5.4 HPD will pay for software support services yearly as set forth in Exhibit A.

6. RELATIONSHIP OF PARTIES

Nothing contained in this Agreement shall be construed to make any party to this Agreement an agent of any other party hereto for any purpose whatsoever. None of the parties hereto nor its employees is the representative of any other party for any purpose, and no party hereto has power or authority to act for, bind, or otherwise create or assume any obligation on behalf of any other party. Each party shall be fully and solely responsible for its own acts and omissions and those of its employees, agents, and subcontractors.

7. INDEMNIFICATION.

To the extent permitted by applicable law, each party shall indemnify, defend, and hold harmless any other party hereto, its officers, employees, agents, or subcontractors from and against any and all losses, damages, costs, expenses (including attorney's fees), obligations and other liabilities (including settlement amounts) that arise directly or are attributable to any acts or omissions relating to this Agreement and which are caused solely by such party's officers, employees, agents or subcontractors

8. NOTICES AND PRINCIPAL CONTACTS.

Any notice, consent or other communication required or contemplated by this Agreement shall be in writing, and shall be delivered either in person, by U.S. mail, by electronic mail or by fax to the intended recipient at the address set forth below:

HPD:	CMPD:
Barry Graham	Kellie High-Foster
Chief of Huntersville Police Department	Director, Business Services
Post Office Box 664 Huntersville, NC 28070	601 East Trade Street Charlotte, NC 28202

Notices shall be effective upon the date of receipt by the intended recipient(s). Any party may change its address for notification purposes by giving the other parties hereto written notice of the new address and the date upon which it shall become effective.

9. MISCELLANEOUS.

9.1 Entire Agreement

This Agreement is the entire agreement between the parties with respect to its subject matter and there are no other representations, understandings, or agreements between the parties with respect to such subject matter. This Agreement supersedes all prior agreements, negotiations, representations, and proposals, written or oral, pertaining to the subject matter of this Agreement.

9.2 Amendment

No amendment or change to this Agreement shall be valid unless in writing and signed by all parties to this Agreement.

9.3 Severability

The invalidity of one or more of the phrases, sentences, clauses or sections contained in this Agreement shall not affect the validity of the remaining portions of the Agreement, provided the material purposes of the Agreement can still be determined and implemented. If any provision of this Agreement is held to be unenforceable or invalid for any reason, all parties hereto shall be relieved of all obligations arising under such provisions.

9.4 Waiver

No delay or omission by any party to exercise any right or power under this Agreement shall impair or be construed as a waiver of such right or power. A waiver by any party of any covenant or breach of this Agreement shall not be constituted or operate as a waiver of any succeeding breach of that covenant or of any other covenant. No waiver of any provision of this Agreement shall be effective unless in writing and signed by the parties waiving the rights.

IN WITNESS WHEREOF, and in acknowledgment that the parties hereto have read and understood each and every provision hereof, the parties have caused this Agreement to be executed as of the Effective Date written above.

City of Charlotte, NC

By: _____
City Manager

Town of Huntersville, NC

By: _____
Town Manager

EXHIBIT A
PAYMENT SCHEDULE

	911 Communications Services	Information Technology Services	Total Cost for Services	% Of Actual Cost
2023 CAP	\$ 641,035.70	\$ 223,335.56	\$ 864,371.26	100%
2023 Annual Payment			\$ 600,000.00	69%
2024 Annual Payment			\$ 864,371.26	100%
2025 -2032 Annual Payment	Increase based upon updated Annual Cost Allocation Plan not to exceed 5% in total per year.			
CMPD Computer Technology Services				
Hourly Rate			\$61.67	

EXHIBIT B MANAGEMENT CONTROL AGREEMENT

Pursuant to the CJIS Security Policy Version 5, Sections 3.2.2 and 5.1, it is agreed that with respect to administration of that portion of computer systems and network infrastructure interfacing directly or indirectly with the North Carolina Criminal Justice Information System state network for the interstate exchange of criminal history/criminal justice information, the Huntersville Police Department shall have the authority, via managed control, to set and enforce:

- (1) Priorities.
- (2) Standards for the selection, supervision, and termination of personnel.
- (3) Policy governing operation of justice systems, computers, access devices, circuits, hubs, routers, firewalls, and any other components, including encryption, that comprise and support a telecommunications network and related criminal justice systems to include but not limited to criminal history record/criminal justice information, insofar as the equipment is used to process or transmit criminal justice systems information guaranteeing the priority, integrity, and availability of service needed by the criminal justice community.
- (4) Restriction of unauthorized personnel from access or use of equipment accessing the State network.
- (5) Compliance with all rules and regulations of the Huntersville Police Department Policies and CJIS Security Policy in the operation of all information received.

“Responsibility for management of security control shall remain with the criminal justice agency.”

This agreement covers the overall supervision of Huntersville Police Department systems, applications, equipment, systems design, programming, and operational procedures associated with the development, implementation, and maintenance of any Huntersville Police Department system to include NCIC Programs that may be subsequently designed and/or implemented within the Huntersville Police Department.

Markell Storay, CTO
City of Charlotte

Date

Barry Graham, Chief of Police
Huntersville Police Department

Date

EXHIBIT C
CITY OF CHARLOTTE USER ACCEPTANCE
ACCEPTABLE USE POLICY
CYBER SECURITY MANUAL – Section 7
(ATTACHED)



City of Charlotte

Cyber Security Manual

Prepared by the City of Charlotte Cyber Security Division of Innovation and Technology

Chief Security Officer Approval Date:

5 January 2023

R. Moulton

Randy Moulton

Summary of Changes

Section	Change Description
Overall Document	Editorial changes have been made to either clarify or enhance the intended meaning of certain sections. Throughout the Cyber Security Manual, team names have been updated to reflect current information.
1.4.3	Linked to City's Data Governance Policy
6.3	Linked to City's Data Governance Policy
6.4.3	Changed location of employee generated data from H Drive to OneDrive
6.5	Updated biometric authentication requirements for mobile devices
6.5.2	Clarified responsibility of maintaining a current phone backup
7.6.1	Terminology updated from 2FA to MFA and OneLogin to SSO; updated wording on how the Service Desk verifies an individual's identity
7.6.4	Part of the policy was replaced with a working process
7.7.2	Update to password manager requirement; terminology updated from 2FA to MFA
7.10	Terminology update from 2FA to MFA and OneLogin to SSO. Updated requirement for Telework.
8.8	Wording updated for clarity
8.9	Updated from City Departments to I&T Divisions
8.10	Wording update for clarity
10.2	Added requirements for Business to Business VPN connections.
10.5	Updated the link to new CQ and updated OneLogin to SSO.
12.4.1	Updated terminology from two-factor to multi-factor
Appendix A	Major updates added regarding requirements related to PCI. Entire section should be reviewed by departments that process credit card transactions.
Appendix B	Updated CJIS policy per the latest CJIS policy requirements.

Table of Contents

1.	Introduction	9
1.1.	Purpose	9
1.2.	Scope	9
1.3.	Exemptions or Exceptions	10
1.4.	Roles and Responsibilities.....	10
1.4.1.	Ethics and Information Security	10
1.4.2.	Chief Security Officer (CSO)	10
1.4.3.	Directors	11
1.4.4.	Innovation and Technology (I&T) Leadership Team and IT Managers	12
1.4.5.	Departmental Network and System Administrators	12
1.4.6.	Authorized User Responsibilities	13
2.	Applicable Regulations	14
2.1.	Payment Card Industry Data Security Standard (PCI DSS)	14
2.2.	Criminal Justice Information Service (CJIS).....	14
2.3.	Health Insurance Portability and Accountability Act (HIPAA)	14
2.4.	State of North Carolina Personal Identifiable Information (PII)	15
2.5.	Critical Infrastructure Regulations and Guidance	15
3.	Audit and Accountability	17
3.1.	Audit and Compliance	17
3.1.1.	Additional Audit Purposes.....	17
3.1.2.	Consent to Access For Audit	17
3.2.	Incident Response.....	18
3.2.1.	Reporting Security Violations	19
3.2.2.	Responding to Active Incidents.....	19
3.2.3.	Evidence of Past Incidents.....	20
4.	Education, Training, and Awareness.....	21
4.1.	Formal Training and Awareness Program.....	21
4.2.	Training and Awareness Content	21
5.	Physical Security	22
5.1.	Secure Areas	22
5.2.	Data Centers	22
5.3.	Physical Security for Devices.....	22
5.3.1.	Network Infrastructure	22
5.3.2.	Thin Clients and Personal Computers (PCs)	22
5.3.3.	Laptops and Mobile Devices	23

6.	Asset Management	24
6.1.	Ownership.....	24
6.2.	Inventory.....	24
6.3.	Restricted Data	24
6.4.	Data Handling.....	24
6.4.1.	Storing Documents in a Cloud Environment.....	24
6.4.2.	Handling Data using Portable Storage Devices.....	24
6.4.3.	Handling Employee-Generated Data.....	25
6.4.4.	Logging Network Activity.....	26
6.4.5.	Audit Logs	26
6.5.	Mobile Devices.....	27
6.5.1.	Exception.....	28
6.5.2.	Lost or Stolen devices.....	28
6.5.3.	Disposal of Mobile Phone Devices	28
6.5.4.	Unacceptable Use	29
6.5.5.	Help and Support.....	29
6.5.6.	Bring Your Own Device (BYOD).....	30
6.6.	Software Asset Management.....	30
6.6.1.	Installation Media.....	30
6.6.2.	Software Support and Roadmaps	30
6.6.3.	Software License Entitlements and Agreements	30
7.	Access Control.....	31
7.1.	Expectation of Privacy	31
7.2.	User Acceptance	31
7.3.	Warning Banners	31
7.4.	Acceptable Use.....	31
7.4.1.	Social Media Procedure.....	32
7.4.2.	Procedure for Internet Posts	32
7.4.3.	Email Use	32
7.4.4.	Enforcement and Penalties for Violation.....	33
7.5.	Screen Lockout.....	33
7.5.1.	Predefined Lockout Time Options	34
7.5.2.	Exceptions	35
7.6.	User Access Management	35
7.6.1.	Authentication	35
7.6.2.	Administrator and Non-Administrator Access	36

7.6.3.	Business Requirement for Access	36
7.6.4.	User Identification (User ID).....	37
7.6.5.	Exceptions	37
7.7.	Passwords	37
7.7.1.	Password Construction	37
7.7.2.	Password Storage.....	38
7.7.3.	Password Reuse	38
7.7.4.	Password Sharing and Transfer	39
7.7.5.	Electronic Transmission	39
7.7.6.	Requirements for System Administrators.....	39
7.7.7.	Requirements for Application Developers	40
7.8.	Service Accounts	40
7.9.	Vendor Access.....	41
7.10.	Remote Telework Access	42
7.11.	Access during Foreign Travel.....	42
7.12.	Termination of Employee or Contractor.....	43
8.	Information Systems Acquisition, Development, and Maintenance	44
8.1.	Acquisition	44
8.2.	Development.....	44
8.3.	Production.....	44
8.4.	Patch Management	44
8.5.	Maintenance	45
8.6.	Data Sanitization	45
8.7.	Disposal	45
8.8.	Change Management	45
8.9.	Documentation Management.....	45
8.10.	Back-ups	46
9.	Data and Infrastructure Security	47
9.1.	Network Security.....	47
9.1.1.	Monitoring.....	47
9.1.2.	Network Infrastructure Procedure	47
9.1.3.	Firewall Policies and Installation Procedures.....	49
9.1.4.	Testing	51
9.2.	Wireless Networking and Communication Procedure	51
9.2.1.	Wireless Access Points.....	51
9.2.2.	Wireless Devices	52

9.2.3.	Bluetooth Procedure	52
9.2.4.	Guest Wireless Access.....	53
9.3.	Electronic Commerce	53
9.4.	Vulnerability Management	53
9.4.1.	Assessment	53
9.4.2.	Prioritization	53
9.4.3.	Remediation.....	54
9.5.	Encryption	54
9.6.	Endpoint Protection	55
9.7.	Server Security	55
9.7.1.	Server Security Principles	55
9.7.2.	Ownership and Responsibilities	56
9.7.3.	Management	56
9.7.4.	Server Configuration	57
9.7.5.	Monitoring.....	57
9.7.6.	Compliance.....	58
9.8.	DMZ Procedure	58
9.8.1.	DMZ Equipment Guidelines	58
9.8.2.	Internet-facing Web Servers.....	60
10.	Third-Party/Cloud and Vendor Management	61
10.1.	Formal Agreements	61
10.1.1.	Protection of Information and Resources	61
10.1.2.	Severability, Waiver, Assignment, Liability for Failure to Perform	62
10.2.	Business to Business Virtual Private Network Connections	62
10.3.	City-Owned Equipment.....	64
10.4.	Audit and Review of Third-Party Network Connections	64
10.5.	Cloud Solutions	64
11.	Business Continuity Plan (BCP).....	66
12.	General Information Technology Security	67
12.1.	Incident Response Related.....	67
12.2.	Data Center Guidelines.....	67
12.3.	Secure Area Guidelines	68
12.4.	Virtual Private Networks (VPN)	68
12.4.1.	Client Virtual Private Network Access	68
12.4.2.	Intranet.....	69
12.4.3.	Internet Procedure	69

12.5.	Commonly Used Applications.....	70
12.6.	External Sharing of Information.....	70
12.6.1.	Guidelines.....	70
12.7.	Email Security	70
12.7.1.	Email System Security Guidelines	70
12.7.2.	SMTP Relay	71
12.7.3.	Email Encryption.....	71
12.8.	Virtual Machines on the Workstation.....	71
12.9.	Active Directory	72
12.9.1.	Computer Account Object.....	72
12.10.	Network Printers.....	72
12.10.1.	Networked Printer Security Requirements	72
13.	Key Terms and Definitions	75
	Appendix A PCI Compliance.....	79
	Requirement 1: Firewall and Router Configuration Standards	79
	Requirement 2: Managing Vendor Defaults and Other Security Standards.....	80
	Requirement 3: Protecting Stored Cardholder Data	80
	Requirement 4: Encryption of Transmissions of Cardholder Data	81
	Requirement 5: Protecting Systems Against Malware	83
	Requirement 6: Developing and Maintaining Secure Systems and Applications	83
	Requirement 7: Restricting Access to Cardholder Data.....	84
	Requirement 8: Identification and Authentication	84
	Requirement 9: Restricting Physical Access to Cardholder Data	85
	Requirement 10 and 11: Security Monitoring and Testing	85
	Requirement 12: Information Security for All Personnel.....	88
	Appendix B CJIS Compliance.....	90
	Policy Area 1—Information Exchange Agreements.....	90
	Policy Area 2—Security Awareness Training.....	90
	Policy Area 3 – Incident Response.....	90
	Policy Area 4—Auditing and Accountability	90
	Policy Area 5—Access Control.....	91
	Policy Area 6 – Identification and Authentication	91
	Policy Area 7—Configuration Management.....	91
	Policy Area 8—Media Protection	92
	Policy Area 9—Physical Protection	92
	Policy Area 10—Systems and Communications Protection and Information Integrity	92

Policy Area 11 - Formal Audits.....	93
Policy Area 12—Personnel Security	93
Policy Area 13—Mobile Devices.....	93

1. Introduction

The City of Charlotte Information Security Manual (herein referred to as the “Manual”) documents and implements the policies, procedures, and guidance required to maintain a secure and resilient information technology infrastructure. The procedure in this Manual and their associated standards and guidelines are intended to create a secure and trusted environment, with particular attention to:

- Common approaches to information security risk management;
- Consistent and adequate hardware, software, and data security controls;
- Appropriate uses of resources; and
- Securing the enterprise against internal and external threats.

This Manual creates a unified approach to IT security management across the City of Charlotte departments and information systems to ensure the security of City information. Congress has defined ‘information security’ in FISMA to include: “protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide:

- *Confidentiality*, which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information;
- *Integrity*, which means guarding against improper information or destruction and includes ensuring information nonrepudiation and authenticity; and
- *Availability*, which means ensuring timely and reliable access to and use of information”.¹

1.1. Purpose

The purpose of the Manual is to establish security standards for City of Charlotte information systems to maintain a high level of security of all data and information exchanged, stored, transmitted, and created by the City. All Departments are required to follow the enclosed security procedures and other procedures as defined in this Manual (ADM 16).

This Manual also contains procedures, standards, and guidelines which Departments should use to develop, test, implement, and maintain security plans for their individual technology areas. Each Department is responsible for the execution of training of Department-specific training of procedures, as explicated in this Manual.

1.2. Scope

The procedures in this Manual apply to all Departments, organizations, employees, contractors, and any other City of Charlotte users that operate, manage, or use IT services, equipment, or data to support City of Charlotte business functions per the Information Security Policy (ADM 16).

Additionally, procedures in this Manual apply to all equipment and data used to support City of Charlotte business. However, critical infrastructure networks; including those operated by Charlotte Area Transit System (CATS), Charlotte Douglas International Airport (CLT), Charlotte Water, and Charlotte Department of Transportation (CDOT); will conform to specific guidelines defined in Appendix A.

¹ Federal Information Security Management Act of 2002 (FISMA), 44 U.S.C. § 3541, P.L. 107-296.

The procedures and guidelines in this Manual also apply to the security of IT facilities and off-site data storage; computing, telecommunications, and applications related services purchased from third parties; and, Internet-related applications and connectivity.

Enforcement of the information security manual procedures is enabled by the Information Security Policy ADM 16.

1.3. Exemptions or Exceptions

Any exceptions or exemptions to this procedure must be approved in writing by the Chief Security Officer (“CSO”). In the event an exception or exemption is granted, an alternate procedure must be established that is:

- Appropriate to the technology environment;
- Consistent with the intent of the procedures defined in this Manual; and,
- No less stringent in nature to the procedures defined herein.

Such alternate security procedures must address:

- Appropriate levels of security and integrity for data exchange and business transactions;
- Effective authentication processes and security architecture(s); and
- Compliance, testing, and audit provisions.

Exceptions or exemptions will only be granted in the event that they are deemed necessary to provide enhanced protection to specific assets or following documented procedure would be impractical given operational or procedural considerations. The Department filing the exception must do so by completing a Security Policy Exception form found on the Self-Service Portal.

1.4. Roles and Responsibilities

1.4.1. Ethics and Information Security

The City of Charlotte is committed to a set of information security procedures that protect employees, partners, suppliers, and the City from illegal or damaging actions by individuals or groups, either knowingly or unknowingly. The City of Charlotte will not tolerate any wrongdoing or impropriety at any time. The City will take the appropriate measures to act quickly in correcting the issue if procedures within this Manual are broken.

To cultivate a culture of ethical behavior, managers are encouraged to welcome suggestions and concerns from employees. This will allow employees to feel comfortable discussing any issues and will alert executives to concerns within the work force. Every employee, Manager and Director needs to consistently maintain an ethical stance and support ethical behavior with respect to information systems and data.

1.4.2. Chief Security Officer (CSO)

The Chief Security Officer (CSO) reports to the Chief Information Officer (CIO) within the Innovation and Technology Department. The CSO is responsible for providing recommendations and assistance to the Senior Leadership Team, the I&T Lead Team, and the Technology Management Advisory Team (TMAT) to assure that City of Charlotte Innovation and Technology (I&T) security goals, priorities, and requirements are effectively and efficiently addressed. The CSO will serve on the TMAT to review

investments to the City's enterprise for information security standards and goals. To execute against the objectives outlined, the CSO is charged with the following duties and responsibilities:

- Issuance of I&T security architectural standards, written guidelines, and best practices, which will contribute to a City-wide scalable, interoperable, and secure operating environment.
- Controlling and monitoring access to City of Charlotte computer and network resources, and system and user directories and files; accessing system and users' directories and files in an authorized manner for City of Charlotte business purposes; and the maintenance of system(s) or network(s) for which there is direct administrative responsibility and instances of suspected or actual security incidents.
- Conducting audits of information systems to ensure compliance with information security procedures and best practices.
- Coordinating the implementation of this procedure with City of Charlotte Department Directors.
- Implementing and administering a City-wide Information Security Program to assure that each City information system has a level of security that is commensurate with the risk and magnitude of the harm that could result from the loss, misuse, disclosure, destruction, or modification of the information contained in the system.
- Ensuring that each system has the appropriate and cost effective technical, personnel, administrative, environmental, and telecommunications safeguards.
- Ensuring systems that support critical City functions have a contingency or disaster recovery plan to provide continuity of operation.
- Coordinating with each community of interest and department the administration of a system security program that meets statutory, regulatory, and City requirements as well as the needs of the City and public at large.
- Verifying the Departments are maintaining appropriate records and conducting training as required.
- Updating this Manual on an ongoing basis, as necessary; conducting an annual review of the Information Security Manual.

1.4.3. Directors

Directors play an important role in the security of the City of Charlotte network and systems. In fulfilling their role in support of information security, Directors are charged with the following duties:

- Determining the sensitivity of data created, collected, processed, and stored on City computers and network resources and ensuring that the data is appropriately protected in accordance with [City Data Governance Policy](#).
- Authorizing access to Department data and computer and network resources. Designating the individual(s) who will exercise this responsibility for various systems and networks within their Department.
- Implementing information technology security for their Department in coordination with the CSO.
- Ensuring that mechanisms are in place to obtain acknowledgment from users that they understand and agree to comply with the procedures defined in this Manual.

- Maintaining appropriate records and conducting training as required by this Manual.

1.4.4. Innovation and Technology (I&T) Leadership Team and IT Managers

I&T Leadership Team and IT Managers are responsible for the duties outlined in this Manual.

- Develop, implement, maintain, and test security processes, procedures, and practices to protect and safeguard voice, video, and data computing and telecommunications facilities—including telephones, hardware, software, and personnel—against security breaches.
- Review supplemental I&T security processes, procedures, and practices at least annually and make appropriate updates after any significant change to its business, computing, or telecommunications environment. Practices will include appropriate mechanisms for receiving, documenting, and responding to security issues identified by third parties. Any updates or changes to InfoSec should be coordinated and approved by the CSO.
- Ensure and oversee compliance with this manual.
- Establish its secure business applications within the guidelines of the City of Charlotte's security architecture.
- Ensure Departments select appropriate assurance for specific application or data access, and implement the protections and controls specified by the appropriate assurance levels, as directed by security standards.
- Ensure Departments follow security standards established for securing servers and data associated with the secure application
- Ensure Departments follow security standards established for creating secure sessions for application access.
- Ensure Departments recognize and support the City's standard means of authenticating external parties needing access to sensitive information and applications.
- Participate in focus-group meetings at the discretion of the CSO.
- Ensure staff is appropriately trained in information security procedures, as defined in this Manual.

1.4.5. Departmental Network and System Administrators

In fulfilling their role in support of information security, City Network and System Administrators are charged with the following duties:

- Preparing and maintaining security practices necessary to implement the procedures in this Manual, to include access, system access controls, auditing, physical security, computer viruses, backup, and recovery.
- Guarding against the corruption, compromise, or destruction of City computer and network resources.
- Reporting to the CSO regarding a suspected or recorded incident that may affect the security of City of Charlotte computer and network resources.
- Ensuring that all applicable security patches are applied to systems within 30 days of announcement.

- Apply appropriate security measures when developing transactional Internet-based applications, including but not limited to, electronic commerce (e-commerce).
- All trouble reports received by system administration personnel should be reviewed for symptoms that might indicate intrusive activity. Suspicious symptoms should be reported to the CSO.
- Maintaining a safe security posture by not storing local device authentication credentials locally on a desktop or server and only in CyberArk. See section 7.7.2 for further details.
- Managing all network infrastructure devices, unless exception granted by CSO.

1.4.6. Authorized User Responsibilities

In fulfilling their role in support of information security, authorized users are charged with the following duties:

- Complying with the procedures documented in this Manual, the City policies, as well as state or federal laws applicable to the use of computers and network resources.
- Safeguarding volumes, directories, and files in accordance with rights and permissions granted to them by the Department owning the data.
- Protecting passwords and preventing unauthorized use of their accounts, programs, or data by unauthorized persons.
- Ensuring that only the City network and system administrators and technicians make changes to the users' system configuration that may alter security parameters.
- Applying the adequate and appropriate controls, encryption, and classification levels on City data to ensure protection.
- Using accounts or network access only for the authorized purposes outlined in this Manual.
- Representing themselves in all forms of electronic communication truthfully, in order to avoid a system to assume the network identity or source address of another computer or network resource.
- Respecting the privacy of electronic communications to which they do not have authorization to receive or view.
- Respecting the physical hardware and network configurations of City of Charlotte owned networks by not extending the physical network on which their system resides.
- Users should be trained to report any anomalies in system performance to their system administration staff as well as the CSO or designees.
- Individuals suspicious or aware of any breach of data or network security, or compromise of computer or network resource security safeguards, must immediately report such situations to the Technology Service Desk.

2. Applicable Regulations

Scope: The City of Charlotte must maintain compliance with applicable state and federal laws, regulations, and/or standards. Departments that must be in compliance with applicable state and federal compliance will be allotted a certain amount of time to reach the appropriate level of compliance.

2.1. Payment Card Industry Data Security Standard (PCI DSS)

Where applicable, the City of Charlotte will abide by I&T procedures in accordance with the latest PCI DSS requirements. PCI DSS provides a baseline of technical and operational requirements designed to protect cardholder data. According to the PCI Security Standards Council, the applicability of the PCI DSS is as follows:

“PCI DSS applies to all entities involved in payment card processing – including merchants, processors, acquirers, issuers, and service providers, as well as all other entities that store, process or transmit cardholder data. PCI DSS comprises a minimum set of requirements for protecting cardholder data, and may be enhanced by additional controls and practices to further mitigate risks.” Please see Appendix A for requirements related to PCI DSS.

2.2. Criminal Justice Information Service (CJIS)

Where applicable, the City of Charlotte will abide by I&T procedures in accordance with the latest CJIS Security Policy. According to the CJIS Advisory Procedure Board the scope of the CJIS Security Procedure is as follows:

“At the consent of the advisory process, and taking into consideration federal law and state statutes, the CJIS Security Procedure applies to all entities with access to, or who operate in support of, FBI CJIS Division’s services and information. The CJIS Security Procedure provides minimum security requirements associated with the creation, viewing, modification, transmission, dissemination, storage, or destruction of CJI.

Entities engaged in the interstate exchange of CJI data for noncriminal justice purposes are also governed by the standards and rules promulgated by the Compact Council.”²

Please see Appendix B for requirements related to CJIS.

2.3. Health Insurance Portability and Accountability Act (HIPAA)

Where applicable, the City of Charlotte will abide by I&T procedures in accordance with the latest HIPAA/HiTech Act. According to the HIPAA Act the scope is as follows.

If compliance with security standards is required, there are 18 information security standards in three (3) areas that must be met to ensure compliance with the HIPAA Security Rule.

The three areas are:

1. Administrative Safeguards: Documented policies and procedures for day-to-day operations; managing the conduct of employees with electronic protected health information (EPHI); and managing the selection, development, and use of security controls.

² Criminal Justice Information Services (CJIS) Security Procedure, Version 5.3, 8/04/2014, Criminal Justice Information Services Division, Department of Justice, Federal Bureau of Investigation.

2. **Physical Safeguards:** Security measures meant to protect an organization's electronic information systems, as well as related buildings and equipment, from natural hazards, environmental hazards, and unauthorized intrusion.
3. **Technical Safeguards:** Security measures that specify how to use technology to protect EPHI, particularly controlling access to it.

2.4. State of North Carolina Personal Identifiable Information (PII)

Nothing within this procedure is intended to supersede or replace laws enacted by the State of North Carolina, to include, but not limited to, N.C. Gen. Stat. §14-113.20 and §75-60 to 66 and N.C. Gen. Stat. §132-1.10. Furthermore, any requirements defined within these statutes are considered applicable and are addressed within this security Manual.

2.5. Critical Infrastructure Regulations and Guidance

Critical Infrastructure is one of the more lucrative targets for attackers of government infrastructure. The importance of protecting these environments is paramount as a compromise could impact the livelihood of our citizens. The City of Charlotte must apply a higher degree of security controls to these areas and conduct an increased frequency of audits to ensure protection is maintained. To the extent that any system operated by the City of Charlotte or on behalf of the City of Charlotte are covered by state or federal regulations, those systems must operate in compliance with the applicable regulations in addition to the parameters set forth in this Manual. These systems may include transportation, water, emergency services, and/or Supervisory Control and Data Acquisition (SCADA) systems. Furthermore, owners and operators of such systems will consult with the CSO to apply standards or best practices to these systems, such as those developed by the National Institute for Standards and Technology (NIST) and the National Security Agency (NSA) and Department of Homeland Security. The City of Charlotte conducts operations within the following five critical infrastructures: emergency services, government facilities, information technology, transportation, and water and wastewater sectors. Below is a brief description of the five sectors.

- **Emergency Services Sector:** A system of prevention, preparedness, response, and recovery elements, the Emergency Services Sector represents the nation's first line of defense in the prevention and mitigation of risk from terrorist attacks, man-made incidents, and natural disasters. The Emergency Services Sector also serves as the primary protector for all critical infrastructure sectors. Encompassing a wide range of emergency response functions, the primary mission of Emergency Services Sector is to save lives, protect property and the environment, assist communities impacted by disasters, and aid recovery from emergencies. These functions, the majority of which are performed at the State, local, tribal, and territorial levels, are defined by the following five disciplines: Law Enforcement; Fire and Emergency Services; Emergency Management; Emergency Medical Services; and Public Works. In addition, the sector consists of six specialized capabilities: Hazardous Materials (HAZMAT); Search and Rescue (SAR); Explosive Ordnance Disposal (EOD); Special Weapons and Tactics and Tactical Operations (SWAT); Aviation Units; and Public Safety Answering Points (PSAPs).
- **Government Facilities Sector:** The Government Facilities Sector includes a wide variety of buildings, located in the United States and overseas, that are owned or leased by federal, state, local, and tribal governments. Many government facilities are open to the public for business activities, commercial transactions, or recreational activities while others that are not open to the public contain highly sensitive information, materials, processes, and equipment. These facilities include general-use office buildings and special-use military installations, embassies, courthouses, national laboratories, and structures that may house critical equipment, systems,

networks, and functions. In addition to physical structures, the sector includes cyber elements that contribute to the protection of sector assets (e.g., access control systems and closed-circuit television systems) as well as individuals who perform essential functions or possess tactical, operational, or strategic knowledge.

- **Information Technology Sector:** The Information Technology Sector is central to the nation's security, economy, and public health and safety. Businesses, governments, academia, and private citizens are increasingly dependent upon Information Technology Sector functions. These virtual and distributed functions produce and provide hardware, software, information technology systems and services, and in collaboration with the Communications Sector - the Internet. The sector's complex and dynamic environment makes identifying threats and assessing vulnerabilities difficult and requires that these tasks be addressed in a collaborative and creative fashion.

Information Technology Sector functions are operated by a combination of entities - often owners and operators and their respective associations - that maintain and reconstitute the network, including the Internet. Although information technology infrastructure has a certain level of inherent resilience, its interdependent and interconnected structure presents challenges as well as opportunities for coordinating public and private sector preparedness and protection activities.

- **Transportation Systems Sector:** The Transportation Systems Sector consists of seven key subsectors, or modes. The City of Charlotte operates the following six subsectors:
 - Aviation includes aircraft, air traffic control systems
 - Highway Infrastructure and Motor Carrier
 - Mass Transit and Passenger Rail includes service by buses, rail transit (commuter rail, heavy rail— also known as subways or metros – and light rail, including trolleys and streetcars), long-distance rail, and other, less common types of service (cable cars, inclined planes, funiculars, and automated guideway systems)
 - Pipeline Systems
 - Freight Rail
 - Postal and shipping
- **Water and Wastewater Systems Sector:** The Water Sector's vision is a secure and resilient drinking water and wastewater infrastructure that provides clean and safe water as an integral part of daily life, ensuring the economic vitality of and public confidence in the Nation's drinking water and wastewater services through a layered defense of effective preparedness and security practices in the sector. The sector's goals in support of the vision are to: (1) sustain protection of public health and the environment; (2) recognize and reduce risks in the Water Sector; (3) maintain a resilient infrastructure; and (4) increase communication, outreach, and public confidence.

3. Audit and Accountability

Scope: Appropriate procedures are implemented to ensure compliance with legislative, regulatory, and contractual requirements. This procedure also covers any computer or communications device present on City premises, but which are not directly owned by the City.

3.1. Audit and Compliance

The City of Charlotte conducts information technology audits to ensure compliance and accountability to state, federal, and City requirements. Audits must be performed at a minimum every two (2) years and be conducted by an independent third-party knowledgeable of applicable requirements. PCI audits will be conducted on an annual basis and CJIS audits will be conducted at the discretion of the FBI and North Carolina State Bureau of Investigation (NC SBI).

Audits should be conducted on a regular basis and meet information security and legal requirements. The Information Security team may request to check employee devices periodically. This is important to ensure compliance with this procedure. In the process of performing such reviews, the Information Security team will respect your privacy.

In addition, the CSO may determine that an earlier audit of an agency's information technology processing is warranted. The nature and scope of the audit must be commensurate with the extent of the agency's dependence on secure information technology to accomplish its critical business functions. The CSO will maintain documentation of the audit and the plan(s) for correcting material deficiencies revealed by the audit. To the extent that the audit documentation includes valuable formulate, designs, drawings, computer source codes, object codes, or research data, or that disclosure of the audit documentation would be contrary to the public interest and would irreparably damage vital government functions, such audit documentation is exempt from public disclosure.

Internal audits and records will be documented and maintained.

3.1.1. Additional Audit Purposes

Audits, outside of compliance with legislative, regulatory, and contractual requirements, may also be conducted to:

- Ensure confidentiality, integrity and availability of information and resources,
- Investigate possible security incidents,
- Ensure conformance to corporate security policies,
- Monitor user or system activity where appropriate.

3.1.2. Consent to Access For Audit

Upon the request of the CSO, access will be provided to members of the Information Security staff to the extent necessary to permit the external entity or individual to perform the assessment(s) authorized by this procedure.

This access may include, but is not limited to:

- User level and/or system level access to any computing or communications device.
- Access to information (electronic, hardcopy, etc.) that may be produced, transmitted, or stored on equipment off premises.

- Access to work areas (labs, offices, cubicles, storage areas, etc.).
- Access to interactively monitor and log traffic on third party networks.

3.2. Incident Response

The CSO will establish and chair a Cyber Incident Response Team (CIRT) who will attend regular meetings to discuss security issues affecting corporate systems, determine the occurrence of a cyber security incident, and oversee incident management activities in accordance with the Incident Response Plan. This team will be comprised of the following members:

- CSO
- Incident Response Manager
- Cyber Security Managers and Supervisors
- Cyber Security Engineers
- Cyber Security Analysts
- Enterprise Services Manager
- Data Center Service Manager
- I&T Infrastructure Manager
- I&T Client Services Manager
- Data Services Manager
- Application Services Manager

The CIRT will be responsible for establishing a strict set of procedures to collect information associated with a violation or intrusion, to report the incident to the appropriate law enforcement agency(s), and to take action to correct the situation. Refer to the Incident Response Plan for more information. The CIRT is also responsible for disseminating information to Departments concerning procedures for reporting incidents.

Departments must report all Information Security Incidents to the CIRT. The CSO or designee will then work with the Departments to ensure that evidence is preserved and reported correctly. The CIRT, in conjunction with the Department, will then:

- Respond quickly to ensure that trace and log files are intact and available.
- Make copies of files that the intruder altered or left.
- Ensure that the perpetrator is not directly contacted.
- Identify a primary contact to handle evidence.
- Contact local LEO, NC SBI, FBI, and/or Secret Service, where appropriate.
- Contact the City Attorney's office where appropriate.

When responding to a suspected Information Security Incident, users should:

- Do not stop processing immediately.
- Do not restore files immediately.
- Communicate by telephone, not E-mail.

3.2.1. Reporting Security Violations

It is the responsibility of all City employees, contractors, and other users to report suspected security violations as quickly as possible. Corrective action, depending on the type of breach, can vary. Security breaches may be categorized as follows:

- Physical intrusions
- Electronic intrusions, including networks
- Servers and workstations
- Incidents related to catastrophic disasters
- Breaches as a result of deception or fraud.

The ultimate goal of the CIRT, regardless of the type of incident, is to protect City assets, contain damage, and restore service. These guidelines should be followed:

- Maintain a Log. Documenting the incident is critical, especially in situations that may eventually involve criminal prosecution. The ramifications of security incidents are not always clear at the onset. The Computer Incident Response Form should be used to document the incident details.
- Notification. It is critical to inform the appropriate authorities immediately. All employees or contractors should report any suspected security breach to their manager. The CSO should be notified immediately.
- Release of Information. No information about the incident should be released unless authorized by the CSO or designees.
- Post-Incident Analysis. After all systems are restored to normal operations, a follow-up analysis should be performed. The CIRT should meet and discuss the actions that were taken and the lessons learned. All existing procedures should be evaluated and modified.

Additional requirements pertaining to specific categories of security violations should be addressed as follows:

- For a physical intrusion of secured areas, local law enforcement should be notified. For catastrophic disasters, e.g., fire, bomb threats, floods, or destructive storms, notification procedures must include the local fire department and/or local law enforcement.
- For incidents involving electronic intrusions, other Departments should be notified where appropriate. Any data collected that facilitated detection of the intrusion should be kept until the incident has been investigated and cleared.
- For incidents involving deception and fraud, notification may include the police department, FBI, and/or Secret Service, depending upon the severity of the incident.
- For electronic data violations, normal logging processes should be enabled on all host and server systems. Alarm and alert functions, firewall logs, and other network perimeter access control systems should be enabled. System integrity checks of firewalls and other network perimeter access control systems should be performed on a routine basis.

3.2.2. Responding to Active Incidents

There are two methods for dealing with an active incident:

- Immediately lock the person out of the system and restore the system to a safe state; or, depending on the circumstances,

- Allow the attacker to continue to probe the system while documenting information that will help identify the attacker to the appropriate law enforcement agency(s). The CSO or designees should determine the course of action to follow. The decision should be based on the availability of qualified personnel to monitor and observe the event and the risk to the enterprise.

NOTE: If the hacker is allowed to continue, appropriate qualified personnel should be on-hand to evaluate the level of risk involved.

3.2.3. Evidence of Past Incidents

Many incidents are discovered after the fact, and often there is little evidence available to help identify the source of the attack or how access was gained to the system. The following steps should be taken:

- Generate a System Snapshot. This should include copies of all audit trail information, such as root history files, system log files, etc. It is important to establish a listing of all active network connections.
- Kill all Active Processes. Terminate all processes invoked by the intruder and remove any files or programs that the intruder left on the system. Change passwords for any accounts that were accessed. Document all actions taken.
- Restore the System. Restore the system to a normal stage. Restore any data or files the intruder may have modified. Install patches or fixes to close any security vulnerabilities the intruder may have exploited. All actions taken to restore the system to a normal state should be documented.
- Follow-up. After the investigation, a report describing the incident and actions that were taken should be documented and distributed to the CIRT and the appropriate law enforcement agency(s).

4. Education, Training, and Awareness

Scope: The City of Charlotte maintains a workforce of well-informed I&T users through effective education, training, and awareness activities. Proper and effective training reduces the risks to an information technology system posed by human error. Awareness ensures that suspicious activity is quickly reported to the CSO and potentially malicious activity is identified by users.

4.1. Formal Training and Awareness Program

The CSO is responsible for City-wide security training. I&T and Departmental IT staff are responsible for conducting Department-specific training. Security training and awareness must be covered within 60 days of new employees and contractors receiving an account and must be refreshed on an annual basis. Failure to complete this training within 60 days will result in the user's account becoming disabled. Should a user require elevated permissions, the user will also be required to take an additional training specific to privileged user access prior to receiving their elevated account. Users requiring PCI or CJIS data access are subject to additional training to be administered by the CSO.

Each department is responsible for ensuring their employees complete the security awareness training.

4.2. Training and Awareness Content

The level and detail of training materials will correspond to the individuals' roles and responsibilities but must include:

- Familiarization with the roles and responsibilities associated with InfoSec.
- Review of the procedures established within this Manual.
- The appropriate points of contact in the event of a security incident.
- Training should consist of practical instruction that includes seminars, lectures, demonstrations, case studies, and hands-on practice. Recurring awareness presentations will be delivered in the form of videos, pamphlets, newsletters, posters, e-mail, and City web pages, as appropriate.

5. Physical Security

Scope: The purpose of this procedure is to provide physical security for information systems and related facilities to prevent damage, loss, unauthorized access, or other identified risks from causing harm. Appropriate controls should be in place to protect physical areas and equipment against physical and environmental threats. All City facilities that house computer and network information resources must be protected by physical controls appropriate for the size and complexity of the operations, and the criticality or sensitivity of the information processed on those systems. Directors, the CSO, and I&T staff are responsible for ensuring that cost-effective measures and controls are established and maintained to secure City data, software, and equipment.

5.1. Secure Areas

The processing and storage of sensitive information will be conducted in secure areas. The CSO is responsible for establishing requirements and identifying appropriate security controls to adequately protect facilities containing information systems. Secure areas should be appropriately labeled and clearly marked. The secure areas should have the necessary security controls to prevent unauthorized access. The CSO will maintain a list of all approved secure areas and is responsible for reviewing each area at least annually to ensure established procedures are being followed.

5.2. Data Centers

Physical access to computer operation centers and facilities that contain information servers must be restricted to personnel and approved contractors with a demonstrated need for access.

- Authorized users, visitors, and vendor service personnel must have their access recorded and be escorted. Entrances must be controlled and monitored at all times.
- Auxiliary equipment (generators and air-conditioning units) in support of data operations centers and facilities should be located in areas that will protect them from damage or tampering.
- The CSO or his delegate will approve access to data centers and be responsible for establishing a set of required physical security controls for data centers, and ensuring those security controls are properly implemented. Physical access to data centers and other facilities that house sensitive or customer data (e.g. PCI or CJIS) will be restricted to a “need-to-know” basis.

5.3. Physical Security for Devices

5.3.1. Network Infrastructure

Physical access to network infrastructure components outside of secure areas and data centers should be limited to only those IT personnel and approved contractors with a demonstrated need.

5.3.2. Thin Clients and Personal Computers (PCs)

Thin clients that are hardwired for direct access to hardware or that have control over network or computer operating systems (OS) or hardware must be physically or logically restricted to authorized City personnel. If thin clients or PCs must be left unattended, users either must log off, or have the operating system screen saver and password feature enabled. In addition, users must ensure that the terminal or PC is physically secured to reduce the likelihood of theft.

5.3.3. Laptops and Mobile Devices

Laptops or mobile devices with access to the City network must be physically or logically restricted to authorized City personnel. If laptops or mobile devices must be left unattended, users either must log off, or have the operating system screen saver and password feature enabled. All City laptops and mobile devices will employ City-approved full disk encryption.

Wireless devices that provide direct access to the City network must conform to the Wireless Networking and Communication Procedure. Wireless devices that fail to conform to the Wireless Networking and Communication Procedure must be installed in a manner that prohibits direct access to the City network. Access to the City network through this device must use standard remote access authentication.

6. Asset Management

Scope: The City of Charlotte manages information technology assets to reduce the likelihood of risk occurring through a variety of mechanisms. The City will identify all assets of importance. Assets are defined in six (6) main areas: information, software, physical, services, people, and intangibles (e.g., reputation).

6.1. Ownership

If a City employee, contractor, or vendor has been issued a City of Charlotte device, the City of Charlotte is the owner of all devices and data used for City purposes. If the user is using a personal device (reference 6.6.6. Bring Your Own Device (BYOD)) to access City of Charlotte data, the City of Charlotte is the owner of all data used for city purposes. As the owner of devices and data, the City of Charlotte is responsible for implementing and updating all security controls necessary to protect the devices and the information contained within.

6.2. Inventory

I&T is responsible for ensuring an accurate inventory of all City-owned information system assets is maintained and for auditing records associated with such assets to ensure proper maintenance and accuracy of required information. Asset owners or their designees will maintain and store current records associated with such assets. The asset inventory will include all information necessary in order to recover from a disaster, including type of asset, format, location, backup information, license information, and a business value. Where any portion of the required information can be gathered through automated discovery, ITCSM will configure and support such discovery. The asset owner or designee is responsible for providing and maintaining access for such discovery to occur.

6.3. Restricted Data

Sensitive business data is defined as documents or data whose loss, misuse, or unauthorized access can adversely affect the privacy or welfare of an individual (personally identifiable information, PII), the outcome of a charge/complaint/case, proprietary information, or agency financial operations. For more information on restricted data refer to City procedure, Protection of Restricted Data (ADM 13).and the City's Data [Governance](#) Policy.

Personally Identifiable Information (PII), as defined by the City's Restricted Data Policy, must be encrypted in transit and at rest, and employ DMZ network isolation.

6.4. Data Handling

6.4.1. Storing Documents in a Cloud Environment

The only approved cloud-based storage application is OneDrive. For any additional information on the storage of documents in the cloud, please reference the public records policy (ADM 20).

6.4.2. Handling Data using Portable Storage Devices

This procedure applies to any portable or mobile device capable of being connected to City information technology systems and/or storing information. This includes, but is not limited to, cell phones, USB thumb drives, and SD card readers. Only approved devices, issued by the City with whole drive encryption and passphrase protection may be used to connect to the City resources. Employees are not

authorized to connect electronic storage devices which are not issued by the City or are of unknown origin to City resources.

For City issued USB drives, the City reserves the right to remotely lock or wipe USB drives at their discretion. The City may also seek out drives that provide event logging and geo-tagging to retain information on what computer and where the device is used. Only corporate signed and approved applications may be run from portable drives. The City of Charlotte may also enforce port (e.g., USB port) scanning on all corporate computers whenever a device is connected.

Approved devices should only be used for temporary storage and should never serve as the sole location for City data. In the event a device is lost or stolen, the user is responsible for immediately reporting the incident to the Technology Service Desk along with a detailed inventory of the data on the device. All storage devices issued by the City should be returned upon termination of employment. These devices must be wiped and scanned for viruses before reissuance.

6.4.3. Handling Employee-Generated Data

Access to the data of active employees shall only be granted to other employees when such access is requested by the employee's supervisor or designee and approved by the Department Director, HR, and the CSO.

In accordance with the City's Public Records Policy (ADM 20), for terminated employees, I&T will retain the employee's email and OneDrive files indefinitely. The terminated employee's manager may request access to employee data for a period of 60 days after departure.

When employees are transferred to a different department, that employee's OneDrive will stay with the employee unless the losing Department requests that the employee not retain the data. The exception will be when an employee transfers to a different domain, a new OneDrive will be created, and the gaining department will have to request a transfer of files.

When an employee is terminated, an automatic reply can be configured for email received from external senders by request for 60 days

The City of Charlotte is responsible for establishing a minimum time period for retention of City data. This minimum time period must reflect any applicable laws or regulations. This procedure must be reviewed and approved annually by legal counsel to ensure that there are no issues with any City by-laws or other governing bodies that may require retention of various types of records.

For PCI systems, cardholder data storage will be kept to a minimum and only stored for as long as there is a legitimate business need to retain the data. Data will be retained consistent with the City of Charlotte's business, legal, and regulatory purposes and according to City disposal policies, procedures and processes.

The City will not store sensitive authentication data after authorization, even if it is encrypted. If sensitive authentication data is received, all data will be rendered unrecoverable upon completion of the authorization process.

Data generated as a result of system or component monitoring should be recorded in a log. Events should be dealt with according to the procedures defined for the area in which they occur. These procedures must comply with the directives established in this Manual

6.4.4. Logging Network Activity

The CSO is responsible for logging network activity as necessary to support threat identification and incident response activities.

The City must have a process or system that links a user to the system components the user has accessed, particularly for users with administrative privileges. This system must generate audit logs and provide the ability to trace suspicious activity back to a specific user.

Logging, at a minimum, should include the following information

- Invalid user authentication attempts
- Logon and activities of individuals with root access and network/system administrators
- Unauthorized attempts to access data or transactions
- Security relevant exceptional conditions and changes to identification and authentication mechanisms (i.e., attempts to achieve “root,” “administrator,” “system,” or “super user” privileges, or gain access to system and security files)
- All log data must be maintained for 365 days with a minimum of three months available for immediate review

For each of the above auditable events, the following information, as permitted by the operating system, must be recorded:

- Date and time of the event
- User ID which generated the event
- Type of event
- Success or failure of the event
- Origin of the event (i.e., process, and/or network addresses).
- Name or identity of the affected data, component or resource

6.4.5. Audit Logs

Computer, network, and data transactions must be recorded and routinely reviewed by I&T for inappropriate and illegal activity as determined necessary by the CSO. At the direction of the CSO, the following data may be captured if suspicious or unexplained computer or network activity is occurring:

- Data related to access events between a user and a City computer, network resources, or cardholder data, including date and time, User ID, associated port, network address or communication device, and other information related to connection, disconnection, and traffic traversing the City network.
- Attempted remote instructions or commands, the name of resource(s) accessed, any use of security or encryption services, administrator actions performed, alarms or notices delivered by a computer or network service, and changes in the configuration of the network.
- Any data traversing the City’s network.

NOTE: Only system administrators that have been specifically designated and have written approval by the CSO can capture network traffic.

Audit logging shall be enabled on all systems and should be retained in compliance with the Data Retention Procedure. Audit logs should record access to systems, maintaining a record of access to include unique identifiers, date and time of access, system(s) accessed, failed access attempts, changes to configuration, use of privileges, activation and de-activation of protection systems, and system modifications.

The CSO, or individuals so authorized, will perform audits on a regular basis. The CSO is responsible for presenting audit findings to the appropriate support staff for remediation or justification. Every effort will be made to prevent audits from causing operational failures or disruptions.

The following rules apply to audit logs:

- Audit logs from perimeter access control systems should be reviewed daily.
- Audit logs for servers and hosts on the internal, protected network should be reviewed on a weekly basis.

At a minimum, these retention requirements apply to the following types of information:

- Administrative Correspondence
- Fiscal Correspondence
- General Correspondence
- Casual or Temporary Correspondence
- Essential business information and correspondence, including messages, in accordance with relevant national and local legislation and regulations
- Audit logs
- Operational procedures
- Accounting records
- Database records
- Transaction logs
- Cryptographic keying material (or programs associated with encrypted archives or digital signatures)
- Physical and virtual software media whether internal or vendor developed
- External or internal certificate authority issued certificates and CRL data.

6.5. Mobile Devices

For the purposes of this procedure, mobile devices shall be defined as phones or tablets that run Apple iOS, Windows, or Android operating systems.

I&T Information Security team requires the following security settings on all mobile devices that store any City of Charlotte data. Note that access to the City of Charlotte Exchange email system through any protocol other than using web-based access means the device is storing at least confidential/enterprise data. Only approved mobile applications shall access City email resources and at this time, the only approved mobile email applications are Mail for iOS and Samsung Mail for Android.

Services/applications which retrieve and store City email on cloud services are prohibited. The required security settings are as follows:

- A non-trivial numeric passcode with a minimum required length of four characters. Simple passcodes consisting of consecutive or sequential characters such 0000, 1234, 9876 etc. are strongly discouraged. Passcodes consisting of additional character sets or greater lengths are recommended. Biometrics are acceptable alternative authentication mechanism.
- An inactivity timeout to automatically lock the device after a maximum of 1 minutes
- Enable full device encryption
- Automatic data wiping after eight (8) failed passcode entry attempts
- Enable the ability to remotely wipe data from lost/stolen devices
- Prohibit users from modifying or disabling security safeguards
- Rooting or jail-breaking a mobile device is not allowed
- Geo-fencing will be used to geographically limit access to City resources from nation states or other areas designated as threats by the CSO
- Location-based device tracking may be used to locate City mobile device assets as needed
- Prohibit the installation of applications from unknown sources
- Prevent the copying of City data to unmanaged applications or destinations

These requirements will be enforced by the City approved Mobile Device Management solution.

6.5.1. Exception

- Any device that is not capable of meeting all the requirements is prohibited from being used to retrieve and store any city data. Users can alternatively view their City email on a mobile device through Office 365.
- The CSO may grant exceptions for mobile devices that are unable to meet the aforementioned guidelines.
- The CSO may grant exceptions to this procedure for devices that are owned by the City but used and managed by 3rd party users.

6.5.2. Lost or Stolen devices

- Employees are responsible for the physical security of their mobile device and the device should be kept in their physical presence whenever possible.
- Users are required to immediately report a lost or stolen mobile device incident to the Technology Service Desk so that a remote wipe of the device may be initiated.
- The wiping of a mobile device will result in the loss of **ALL** data on the device, including contacts, pictures, notes, applications, music files, text messages, etc. Mobile device users are responsible for maintaining a current backup of their device(s) so that data may be easily restored in the event of data loss on the device.

6.5.3. Disposal of Mobile Phone Devices

I&T and Resource Management have partnered with outside vendors to securely wipe and recycle unwanted cell phones, tablets and data cards. All personal and corporate information will be removed,

even if the mobile device is broken or the screen is cracked. Once a phone is dropped off or mailed in for recycling, it cannot be returned.

6.5.4. Unacceptable Use

It is the responsibility of any employee of the City of Charlotte who uses a mobile device to access City resources to ensure that all security protocols normally used in the management of data on conventional storage infrastructure are also applied here. It is imperative that any mobile device that is used to conduct City business be utilized appropriately, responsibly and ethically.

City of Charlotte mobile devices **may not** be used:

- For excessive personal use;
- In any capacity while operating City owned equipment (i.e. vehicles, tractors, lawn mowers, gators, forklifts, golf carts, etc.), except where permitted by NC Statute 20-137.4A.(b)
- For commercial activities, such as running any sort of private business, advertising or performing work for personal gain or profit;
- For political activities; such as promoting a political party / movement, or a candidate for political office, or campaigning for or against government decisions;
- To knowingly misrepresent the City of Charlotte;
- To transmit confidential or personal data outside the City of Charlotte unless the data has been encrypted and transmission has been authorized by Chief Security Officer;
- To enter into contractual agreements inappropriately (i.e. without authorization or where another form of agreement is required);
- To view, create, download, host or transmit (other than for properly authorized and lawful purposes) pornographic, offensive or obscene material (i.e. information, images, video clips, audio recordings etc.), which could cause offence to others on the grounds of race, creed, gender identity, sexual orientation, disability, age or political beliefs;
- To retrieve, create, host or transmit material which is defamatory;
- For any activity that would infringe intellectual property rights (e.g. unlicensed installation, distribution or copying of copyrighted material);
- For the installation and use of software or hardware tools which could be used to probe, and/or break the City of Charlotte security controls;
- For creating or transmitting “junk” or “spam” emails. This includes unsolicited commercial emails, chain-letters or advertisements;

6.5.5. Help and Support

- I&T will support its sanctioned hardware and software, but is not accountable for conflicts or problems caused by the use of unsanctioned media, hardware, applications or software.
- I&T, with the exception of connectivity to City of Charlotte email services, will not support personally owned devices.
- City of Charlotte will accept no liability for functionality, serviceability or performance associated with the device or any responsibility with regard to warranty on personal owned devices.

- City of Charlotte accepts no responsibility or liability for the loss of City or personally related data residing on the device.

6.5.6. Bring Your Own Device (BYOD)

All personally-owned mobile devices used to retrieve or store City of Charlotte data must comply with the Mobile Devices procedure. The City retains the right to remove any City data from personally-owned devices at any time.

6.6. Software Asset Management

6.6.1. Installation Media

I&T is responsible for ensuring that enterprise software installed on City assets is properly stored and maintained and does not pose a security risk. Application owners or their designees will store, package and install standard desktop and server software from permissions managed, auditable and virus scanned locations such as a Definitive Media Library (DML), Application Lifecycle Management (ALM) application or from original physical media. I&T will manage, store, and install all enterprise level applications.

6.6.2. Software Support and Roadmaps

I&T is responsible for ensuring that software installed on City assets is properly supported and that security updates are maintained within the vendor guidelines and version roadmaps for each product. Asset owners or their designees will develop and maintain product roadmaps as well as upgrade/migration schedules including end-of-life / end-of-sale (EOL/EOS) dates as applicable to ensure that software remains in a secure and supported state. Technology Management will develop and maintain roadmaps and schedules for all enterprise level applications.

6.6.3. Software License Entitlements and Agreements

I&T is responsible for ensuring that enterprise software installed on City assets is properly licensed and that sufficient license entitlements exist to ensure the software is vendor supported. Asset owners or their designees will maintain license entitlement information including but not limited to contracts, agreements, documentation as well as any required host, seat or user information associated with such licenses as may be required by CSO or vendor audit. Innovation & Technology will maintain all required license information for enterprise level applications.

7. Access Control

Scope: The City tightly controls access to information, information processing facilities, and business processes on the basis of business and security requirements. Access control rules take account of procedures for information dissemination and authorization.

7.1. Expectation of Privacy

Employees do not have a right, nor should they have an expectation, of privacy while using City-owned information systems or devices or personally owned devices for City business at any time. Examples of monitored activities include Internet usage, text messages, email, and voice communications. In addition, all City communication that takes place on these devices are considered property of the City and will be protected and monitored.

7.2. User Acceptance

All City employees, contractors, or other users that are granted access to City information systems and data are required to sign an employee acceptance agreement. This agreement confirms the employees understanding and acceptance of the procedures identified in this manual.

Any employee found to have violated this procedure may be subject to disciplinary action, up to and including termination of employment. Any supplier or vendor found to have violated this procedure may be subject to contract review.

7.3. Warning Banners

Warning statements must be visible to all computer and network users on the limitations and restrictions of authorized and unauthorized activities concerning information resources security. The following warning and disclaimer banners will be displayed during the login process.

- **WARNING.** This is a City of Charlotte computer resource, which may be accessed and used only for official business by authorized personnel. Confidential or protected information may not be disclosed without authorization. Unauthorized access or use of this computer system may subject violators to criminal, civil, and/or administrative action. All information on this computer system may be intercepted, recorded, read, copied, and disclosed by and to authorized personnel for official purposes, including criminal investigations. Access or use of this computer system by any person, whether authorized or unauthorized, constitutes consent to these terms. There is no expectation of privacy for any information transmitted in or through the system.
- **DISCLAIMER OF LIABILITY.** For information available from this computer system, City of Charlotte does not warrant or assume any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed.

7.4. Acceptable Use

The usage of City-owned devices and data is provided to users and must only be utilized for official City business. Each person with access to the City's computing resources is responsible for their own appropriate behavior and by their use agrees to comply with all applicable City, state and federal laws and regulations.

The General Standards for the Acceptable Use of Computer Resources require:

- Responsible behavior with respect to the electronic information environment at all times.

- Behavior consistent with the mission of the City and with authorized activities of the City of Charlotte.
- Compliance with all applicable laws, regulations, and City policies.
- Truthfulness and honesty in personal and computer identification.
- Respect for the rights and property of others, including intellectual property rights.
- Behavior consistent with the privacy and integrity of electronic networks, electronic data and information, and electronic infrastructure and systems.
- Respect for the value and intended use of human and electronic resources.

7.4.1. Social Media Procedure

Employees, contractors, and suppliers may utilize social networking sites and blogs such as Facebook, LinkedIn, Twitter, Pinterest, Instagram, Yahoo! Groups, BlogSpot, MySpace, and Wikipedia. Employees must be mindful to any posts published to these sites. Please refer to the City of Charlotte's [Social Media Policy \(ADM 15\)](#) for further clarification. In particular, Internet posts should not jeopardize the City of Charlotte security by (ADM 15, Page 2):

- Disclosure of confidential information to which an employee has access as part of the employee's role or duties.
- Disclosure of non-public information or legally protected personal information.
- Disclosure of information related to unlawful activities including, but not limited to, the use, sale or distribution of illegal substances.

7.4.2. Procedure for Internet Posts

Employees and contractors are legally and personally responsible for all posts. If a City user posts as an individual and not as a City employee, the user must clearly state within the post that he or she is expressing his or her own personal views and not the views of the City of Charlotte.

7.4.3. Email Use

Use of email by employees of the City is permitted and encouraged where such use supports the goals and objectives of the business. Using a reasonable amount of corporate resources for personal emails is acceptable, but non-work related email shall be saved in a separate folder from work-related email. However, the City reserves the right to monitor cross-domain access for security procedure violations and anomalous activity. Employees or contractors of the City of Charlotte shall have no expectation of privacy in anything they store, send, or receive on the City's email system. The CSO may monitor messages without prior notice. Password protected email attachments are prohibited unless exception for trusted partner is granted by CSO.

Employees who receive malicious emails like phishing attempts or emails that include questionable links or attachments shall forward those messages to bad.mail@charlottenc.gov or click the Phish Alert button. This mailbox will be reviewed by the I&T Information Security team.

In the use of e-mail, employees and contractors **may not**:

- Use personal email accounts (a private, non-City account such as Yahoo, Gmail, etc.) to conduct City business unless City email is unavailable. If City email is unavailable, and an email must be

sent from a personal account, staff's City email account should be copied in the communication. This is in accordance with the City's Public Records Policy (ADM 20).

- Use personal mailbox (.pst) files for storing email outside of the City's email server without permission from the department director and the CSO in accordance with the City's Public Records Policy (ADM 20).
- Use the City communications systems to set up personal businesses, send inappropriate jokes, threats, or chain letters, or for criminal activity.
- The City email system shall not to be used for the creation or distribution of any disruptive or offensive messages, including offensive comments about race, gender identity, hair color, disabilities, age, sexual orientation, pornography, religious beliefs and practices, political beliefs, or national origin.
- Forward City confidential, sensitive, or classified messages to external email accounts or locations.
- Engage in distributing, disseminating or storing images, text or materials that might be considered indecent, pornographic, obscene, harassment, or illegal.
- Engage in distributing, disseminating or storing images, text or materials that might be considered discriminatory, offensive or abusive, in that the context is a personal attack, sexist or racist, or might be considered as harassment.
- Review, downloading or accessing copyrighted information in a way that violates the copyright.
- Use another person's account credentials and login with or without permission via "hacking" into a City accounts.
- Undertake deliberate activities that waste staff effort or networked resources.
- Introduce any form of computer virus or malware into the corporate network.
- Use Outlook rules to forward email to external accounts.
- Configure automatic replies for external addresses

7.4.4. Enforcement and Penalties for Violation

Any user who violates any provision of this procedure or of applicable City, state, or federal laws or regulations may face sanctions up to and including termination and legal action.

Authorized systems administrators may at necessary times suspend access to computing resources immediately for violations of this procedure, pending interim resolution of the situation. For example, by securing a possibly compromised account and/or making the owner of an account aware in person that an activity constitutes a violation. In the case of egregious and continuing violations suspension of access may be extended until final resolution by the appropriate disciplinary body.

7.5. Screen Lockout

A password enabled screen saver helps to protect the information displayed on your screen, stored on your computer's hard drive, and the information that is accessible from your computer when you walk away from the computer. The screen saver locks out an active user after a set amount of time with no activity. By requiring a user to sign in when they return, it minimizes the risk of an unauthorized person using an active session while the authorized user is away.

Users shall lock their desktop computer prior to leaving the computer unattended. All City-owned computers shall be configured to have a password-enabled screen saver. This security lockout feature should automatically initiate after the computer remains idle from user interaction after a predefined time period. The user must then re-enter their password to gain access to the computer. The general best practice for enabling automatic lockout of a screen saver is to set the timeout, so that it can provide adequate security and not interfere with successful City operations.

7.5.1. Predefined Lockout Time Options

Lockout Time	Description	Recommendation
5 minutes	This is the suggested lock out for computers that are located in public areas (E.g. CMGC Front Desk).	Recommended
15 minutes	This is the best practice recommendation for all employee desktops.	Default
60 minutes	This setting should only be used if the computer is located within a secure environment. This is the maximum screen lock out setting allowed for a desktop in Auxiliary Services (E.g. conference rooms, auditorium, police vehicle, crime lab, etc.).	Minimum guideline – This option is not recommended and requires a security policy exception prior to implementation.

No Lockout	This should only be used for single use workstations that do not access private data. (E.g. digital signage, kiosks, etc.).	This option is not recommended and requires a security policy exception prior to implementation.
-------------------	---	--

7.5.2. Exceptions

Exceptions should adhere to the *Exemptions or Exceptions* section in this manual.

Perceived inconvenience is not sufficient grounds for removal or extending the lockout period. I&T Security is able to exempt computers from the lockout guideline only in circumstances where: physical security for the space in which the computer is located is of such high quality as to make access by unauthorized users effectively impossible; or application of the timeout guideline to the particular computer is materially detrimental to work activities and makes work processes effectively impossible. In either of these cases, there must not be a regulatory or compliance requirement for screen lockout. In those cases, exceptions will not be approved.

7.6. User Access Management

The CSO will develop and maintain procedures for managing access controls. This will include procedures for requesting access, granting access, and administering access. The responsibilities for managing access control (access request, access authorization, access administration) must be segmented and no one person or department will be exclusively responsible for multiple roles in managing access control. When granting access to systems, a procedure of the least required access must be followed. Access to records that contain customer information (e.g., PCI or CJIS) will be restricted to a “need to know”.

7.6.1. Authentication

Each individual who is authorized access to City computer and network resources must be authenticated before access will be permitted. All users are required to authenticate their identity at logon time using a password. Authentication may be based solely on passwords, but second layer of authentication may be necessary for access to certain information. In this case, smart cards, tokens, or digital certificates may be used in addition to passwords. Authentication credentials are the responsibility of each user and must not be shared. Access to digital certificates or signatures stored on PC clients must be protected by passwords. If a password is compromised or a card, token, or key is lost or stolen, the compromise and/or loss must be immediately reported to the Department network or system administrator and the Technology Service Desk.

Individuals accessing City computer and network resources that require elevated privileges to perform tasks shall be required to use Multi Factor Authentication (MFA), when available. External vendors are required to use MFA when accessing City computer or network resources to perform any maintenance related task that is required per their executed contracts.

Short Message Service (SMS) text messages should not be used to transmit MFA codes.

The City of Charlotte will maintain a central user registry, through which all authentications will be performed, within the City's Active Directory infrastructure. All cloud services employed by the City shall use the City's Active Directory for authentication via Single Sign-on (SSO) application. Furthermore, all Unix/Linux systems shall also use the City's Active Directory for authentication and adhere to the City's Linux security baseline.

Any password reset for Active Directory credentials performed by the Technology Service Desk must only be performed after the identity of the individual requesting the reset has been verified. Verification of a requester's identity may be performed via the last four digits of the requester's social security number. If the last four digits of the requester's social security number is unavailable, they can be verified by one of the following methods:

1. The Service Desk creates an approval linked to the password reset ticket and an IT Liaison representing the requestor's department approves it within the ticketing system.
2. By the requester successfully answering security questions that have been previously gathered from the user and stored in CyberArk.
3. By having an IT Liaison for their department call the Service Desk, the IT Liaison is verified and confirms the person's password can be reset.

7.6.2. Administrator and Non-Administrator Access

Non-administrator access provides users with the ability to perform tasks, run applications and modify files that only affect that user. Administrator access enables a user to make system-level changes that will affect multiple users. Listed below are the various types of administrator and non-administrator access levels in the City of Charlotte, along with the approval authority for those access levels.

Access Type	Approval Authority
Non-Administrator	
Normal User Access	Delegated
VPN Access	Delegated
Restricted/PCI	CSO
CJIS	Delegated to CMPD
Administrator	
Local Workstation Administrator (Non-restricted, PCI, or CJIS)	CSO
All Other Administrator Access	CSO

7.6.3. Business Requirement for Access

Access to the City network must be based on the employee, contractor, or third party's official duties and responsibilities. Each authorized user and group must be granted the minimum set of rights and permissions necessary to accomplish their assigned departmental tasks. Requests for elevated permissions must be approved in writing by either the supervisor of the user requiring additional permissions or the Department's IT Liaison.

If a City or contractor personnel transfer to another Department or position, their computer and network resource access and access privileges to City data and applications must be reviewed and changed in a timely manner.

7.6.4. User Identification (User ID)

Each individual who is provided authorized access to a City computer or the network is required to use a User Identification (User ID) account that must be unique to the individual and consistently employed throughout the City of Charlotte.

User IDs for all City of Charlotte users will be assigned through interaction between Department IT Liaisons and the Technology Service Desk. Each User ID is the responsibility of the person to whom it is assigned. User IDs may not be shared.

- Users that require elevated privileges on any City of Charlotte systems must use a unique User ID that is distinct from their personal, daily-use user ID. This ID must not be associated with an email access and should only be used when elevated privileges are required for a given task. User ID's requiring elevated privileges will have those privileges assigned via a role defined in the City's Role Based Security procedure.
- User IDs must be disabled immediately for persons who are no longer affiliated with the City of Charlotte, or for persons who have otherwise lost authorization for access to City resources and data.
- User IDs for employees on a leave of absence must be disabled on the first day of leave. The ID should be reinstated upon official notification that the employee has returned from leave.
- User IDs that remain inactive for 60 days must be disabled. User IDs that remain inactive for 180 days must be deleted unless special arrangements have been made.
- User IDs for contractors must have an expiration date that aligns with their contract period of performance. The Department sponsoring the contractor will provide the expiration date. If none is provided, the User ID will be set to expire and be disabled 180 days from the issue date. Any request to extend the expiration date of a contractor account must be submitted prior to the account's existing expiration date. Requests to reactivate and extend the expiration date of a contractor account which has already expired must be approved by Cyber Security.

7.6.5. Exceptions

The Aviation department and I&T Public Safety Communications have internally managed AD environments, which are separate from the City's enterprise AD environment. All controls in this manual related to AD must be applied to these separate AD environments.

7.7. Passwords

The CSO is responsible for establishing requirements for appropriately complex passwords. Required complexity will be determined based on current industry best practices.

7.7.1. Password Construction

At a minimum, all non-privileged user accounts must meet the following password requirements:

- Password must be at least thirteen (13) characters and include at least three of the following types of characters: upper case, lower case, number, and special character.
- New passwords must not have been used in the past 10 passwords.
- Passwords must be changed every 90 days and have a minimum age of two (2) days.

- After 6 unsuccessful attempts your account will be locked out for 2 hours, or until an administrator enables the account.

At a minimum, all privileged user accounts (those granted administrator rights) must meet the following password requirements:

- Password must be at least fourteen (14) characters and include at least three of the following types of characters: upper case, lower case, number, and special character.
- New passwords must not have been used in the past 10 passwords.
- Passwords must be changed every 90 days and have a minimum age of two (2) days.
- After 6 unsuccessful attempts your account will be locked out for up to 2 hours.

At a minimum, all service/application accounts must meet the following password requirements:

- Password must be at least twenty-five (25) characters and include at least three of the following types of characters: upper case, lower case, number, and special character.
- New passwords must not have been used in the past 10 passwords.
- After 8 unsuccessful attempts your account will be locked out for up to 2 hours.

At a minimum, all Local Administrator accounts must meet the following password requirements:

- Password must be at least twenty-five (25) characters and include at least three of the following types of characters: upper case, lower case, number, and special character.

Other regulations or standards may require more stringent password protections for customer information (e.g., PCI or CJIS). The CSO is responsible for implementing the most current password protections for customer data.

7.7.2. Password Storage

- All service, shared, local workstation/server administrator, and privileged account credentials must only be stored in CyberArk.
- Passwords **must not** be stored by unencrypted computer applications such as email. Use of an encrypted password manager application is acceptable, although extreme care must be taken to protect access to the application. Password manager applications must meet the encryption requirements specified in section 9.5 of this Manual and must be protected by MFA. Users should not store Active Directory credentials in their password manager.
- Passwords shall be memorized and never written down or recorded along with corresponding account information or usernames.

7.7.3. Password Reuse

Users must not use the same password for multiple accounts. For example, do not use the password from your Facebook account as the password for your City domain accounts. Also, do not use the same password across multiple City domain accounts.

7.7.4. Password Sharing and Transfer

- Passwords shall not be transferred or shared with others. Do not reveal a password on questionnaires or security forms.
- When it is necessary to disseminate passwords in writing, reasonable measures shall be taken to protect the password from unauthorized access. For example, after memorizing the password, one must destroy the written record.
- The method described in [Sending & Receiving Encrypted Emails with Office 365](#) should be used to send new or temporary passwords.
- All shared and privileged accounts should be stored in CyberArk. Retrieve the password for the account needed via the CyberArk portal. If you do not have access to CyberArk, please request access via a Cherwell ticket with the Technology Service Desk.

7.7.5. Electronic Transmission

Passwords shall not be transferred electronically using insecure methods. Security protocols including IMAPS, SFTP, HTTPS, etc. shall be used.

7.7.6. Requirements for System Administrators

- **Require Passwords for Login** - Systems shall not be configured to allow user login without a password. Exceptions shall be granted for specialized devices such as public access kiosks when these devices are configured with public user accounts that have extremely restricted permissions (e.g. web only) that are separate from administrative accounts.
- **Protect against Password Hacking** - System administrators shall harden their systems to deter password cracking by using reasonable methods to mitigate “brute force” password attacks. For example, some systems will lock an account for a few minutes after several failed login attempts, or detect where the attack is coming from and block further attempts from that location, or at minimum alert an administrator in real-time that an attack is underway so that manual action can be taken.
- **Require TLS Security** – System administrators shall harden their systems which have web management access with TLS 1.2 or greater and use the strongest ciphers possible. All internal management certificates should be signed by the City CA.
- **Logging** - Practical measures shall be put in place to log successful and failed login attempts on critical systems identified. System administrators/owners requiring such logging for their systems should contact the Information Security team.
- **Changing Password after Compromise or Disclosure** - System administrators shall, in a timely manner, reset passwords for user accounts or require users to reset their own passwords in situations where continued use of a password creates risk of unauthorized access to the computing account or resource.
 - Examples of these situations include but are not limited to: disclosure of a password to an unauthorized person; discovery of a password by unauthorized person; system compromise (unauthorized access to a system or account); insecure transmission of a password; replacing the user of an account with another individual requiring access to the same account; password is provided to information technology support staff in order to resolve a technical issue; account password is communicated to a user by the system administrator.

- **Default Passwords** - System administrators shall not use default.
- **Role Base Access** - Applications must provide for some sort of role management, such that one user can take over the functions of another without having to know the other's password.

7.7.7. Requirements for Application Developers

- **Require Secure Transmission** - Application developers shall, whenever possible, develop applications that require secure protocols for authentication.
- **Storing Passwords** - Application developers shall avoid creating applications which store passwords. If password storage cannot be avoided, application developers shall ensure that applications do not store passwords in clear text or an easily decrypted format.
- **Unique User Accounts and Passwords** - Applications shall support unique user accounts and passwords, so that individual users are not required to share a password in order to use the application.
- **Use City username and password whenever possible** - Applications shall, whenever capable, use the City of Charlotte Active Directory username and its associated password for authenticating members of the City of Charlotte community instead of creating another unique ID or username.

7.8. Service Accounts

Service Accounts are a user object that provides authentication for an application or service. This should not be a user's personal account. A service account could also be an account that is used for a scheduled task (sometimes referred to as a batch job account), or an account that is used in a script that is run outside of a specific user's context.

I&T Information Security must approve the creation of service accounts. I&T Data Center Services is responsible for documenting the operational procedures for maintaining service accounts. The Information Security team will review the procedures annually to validate that best practices are followed.

The following requirements at a minimum are as follows:

- Only allow logon types needed, such as Network Logon and Logon as a Service. Explicitly prevent these accounts from logging on interactively, unless required by the service.
- Service accounts should have the least privileges needed for the application to function.
- Restrict the account so that it can only be used to access those specific systems.
- Move all accounts out of the default OU and create specific OUs for each department or role.
- Ensure that service accounts are not human (user) accounts.
- Service accounts must have secure passwords as defined in Section **Error! Reference source not found.**
- Ensure that each service account has the description field populated within Active Directory.
- Service accounts should be explicitly denied access to external resources such as VPN gateways and IIS web servers that support NTLM authentication.
- All service accounts should be stored in our password management software CyberArk.

7.9. Vendor Access

Personnel who provide vendors access to City of Charlotte information systems shall ensure vendor compliance with all applicable City of Charlotte policies, practices, standards, and agreements including, but not limited to: safety policies, privacy policies, security policies, auditing policies, software licensing policies, responsible use policies, and other City of Charlotte information security standard administrative procedures.

Note that this procedure does not apply to contractor personnel. For the purposes of this procedure, contractor personnel are defined as employees of a third party providing services to the City of Charlotte under a contract, who are issued City-owned devices. Access shall be provided to contractor personnel in the same manner as it is provided to City of Charlotte employees. Vendors, on the other hand, only require ad-hoc access to provide specific support needs or short-term implementations.

Vendors who are given access to any non-public City of Charlotte information systems shall have agreements and contracts that define:

- The City of Charlotte information to which the vendor should have access;
- How City of Charlotte information is to be protected by the vendor;
- Acceptable methods for the return, destruction, or disposal of City of Charlotte information in the vendor's possession at the end of the contract;
- That use of City of Charlotte information and information technology resources are only for the purpose of the business agreement. Any other City of Charlotte information acquired by the vendor in the course of the contract cannot be used for the vendors own purposes or divulged to others; and,
- Vendors shall comply with terms of applicable non-disclosure agreements.

The City of Charlotte shall provide an information technology resource Point of Contact (POC) to the vendor. The POC will work with the vendor to make certain the vendor is in compliance with City of Charlotte policies.

Each vendor shall provide the City of Charlotte with a list of all employees assigned to the City of Charlotte contracts. The list shall be updated and provided to the City of Charlotte within 24 hours of staff changes. Failure to notify the City of Charlotte of staff changes may cause the vendor to incur additional liability if information is released.

To maintain account and password security, disclosure of any account information and passwords to anyone other than the account owner is prohibited.

Vendor personnel shall report all security incidents to the City of Charlotte Technology Service Desk and the Information Security Team.

Any vendor access granted to information technology resources will be provided the least security privilege required to accomplish his/her task(s).

Regular work hours and duties will be defined by the POC. Work outside of defined parameters must be pre-approved by the POC, who will make arrangements for necessary facility services and access to secure areas.

The responsibilities and details of any vendor management involvement in City of Charlotte security incident management shall be specified in the contract.

Prior to granting vendor access for software installations and/or upgrades, the process will be reviewed by the appropriate system administrator. After a vendor has installed or upgraded a product, the responsible system administrator will review the system to ensure that it is functioning properly.

The vendor must follow all applicable City of Charlotte change control processes and procedures.

Vendor shall not access any information technology resource remotely via VPN. The information technology resource POC shall gather the list of vendor personnel and systems to which they need access. The information technology resource POC will provide this list to the Information Security team to incorporate them into the BeyondTrust Privileged Remote Access (PRA) solution. The Information Security team will configure and setup the vendor and information technology resource POC to have access to those endpoints through the BeyondTrust portal. Access to this PRA shall require the use of Multi Factor authentication. The information technology resource POC will be responsible for adding/removing personnel from the AD group for the authorized vendors who require access to the resources identified.

It shall be the responsibility of the information technology resource POC to monitor all activity performed by the vendor when accessing City of Charlotte information technology resources.

7.10. Remote Telework Access

Users may access the City of Charlotte network remotely for business purposes; however approved VPN connections must be utilized at all times. The approved method for remote access to the City of Charlotte network is the Palo Alto Global Protect Client using City's standard cloud-based identity provider (IdP). Multi-factor authentication. These methods require credentials and membership in the applicable active directory VPN users groups. In addition, City-managed computers must be used with the VPN system. On the occasion of an Extraordinary Event, a term designating special functions hosted within the City, extreme weather conditions or state of emergencies, access may be restricted to essential personnel in order to maintain operational availability. Any exceptions to the approved method for remote access must be approved by the CSO.

7.11. Access during Foreign Travel

The CSO must establish a foreign travel procedure and process for approving the transport of devices outside of the United States. Access to the City of Charlotte resources while on foreign travel should be kept to an absolute minimum and must be approved by the Cyber Security Manager. The transport of any City information systems, to include laptops and mobile devices, to a foreign country must be approved by the CSO. Access from a given country is not guaranteed.

City employees must:

1. Complete a foreign travel request form located in the Self-Service portal. In the miscellaneous security policy exception request, please provide justification, length and location of travel and extent of remote access needs and what resources will need to be accessed while abroad. This should be submitted three (3) weeks before traveling to a foreign country to receive any special instructions. This will be reviewed by the Cyber Security Manager and/or CSO.
2. While abroad, avoid all unencrypted WIFI access points.
3. Store all City information systems not approved for travel at the employee's respective offices.
4. Never place City information systems in checked luggage or left unattended during travel. If you must leave the computer in the hotel room, the device should be powered off and stored in a safe or locked container if possible.

5. Relinquish City information systems used on travel to the InfoSec team for review prior to reconnecting to the City network or Internet.

7.12. Termination of Employee or Contractor

If a City employee or contractor terminates his or her employment relationship with a Department, all City of Charlotte computer hardware, software, and data must be returned immediately. The direct supervisor is responsible for ensuring that computer hardware, software, and data property assigned to or in custody of the worker is returned. The direct supervisor must ensure that network and system administrators, the Technology Service Desk, and all other appropriate I&T Divisions are promptly notified of terminations, and that all network and system accesses and privileges of the worker are terminated in accordance with Voluntary Separation Policy (HR 20).

- When an employee provides notice of intent to voluntarily separate from the City, any of the employee's accounts that have elevated privileges will be immediately disabled.

If a City employee is involuntarily terminated in accordance with the Pre-Termination Hearing Policy (HR 22) the following procedure will be followed:

1. The direct supervisor will notify the CSO via email and phone upon an approved written 'Notice of Pre-Termination Hearing'
2. Notify the CSO of the date and time when the 'Notice of Pre-Termination Hearing' will be delivered to the employee.
3. After the Termination Hearing the direct supervisor will notify the CSO of the status of the employee.
4. The direct supervisor is responsible for ensuring that a proper succession plan is in place for all employees that have elevated privileges to reduce any operational impact.

8. Information Systems Acquisition, Development, and Maintenance

Scope: The City of Charlotte incorporates information security into all phases of the lifecycle for information systems. Information systems include operating systems, infrastructure, business applications, off-the-shelf products, services, and user-developed applications.

8.1. Acquisition

I&T will engage with the CSO in the acquisition process, with the overall goal to detect and evaluate information security risk, develop a remediation plan with the affected parties for the identified risk, and work with the acquisition team to implement solutions for any identified security risks, prior to allowing connection to City networks.

This procedure applies to all materials acquired by the City that pertain to systems, networks, test equipment, hardware, software and firmware, and/or any other material subject to the authority of the CSO. To prevent security risks to networks, internal systems, and/or confidential/sensitive information from an acquisition of an IT product a risk assessment should be conducted.

8.2. Development

The design, development, and implementation of the information system supporting the business process can be crucial for security. Security requirements should be identified and agreed prior to the development and/or implementation of information systems. All security requirements should be identified at the requirements phase of a project and justified, agreed, and documented as part of the overall business case for an information system.

8.3. Production

I&T will be responsible for maintaining a list of all enterprise production systems and systems owners. Prior to entering into production, a system owner must be designated that has authority over and responsibility for that system. The system owner is responsible for ensuring compliance with all procedures defined within this Manual.

8.4. Patch Management

All City of Charlotte departments should develop, in conjunction with I&T, a patch management process for updating every device connected to a City-owned network to include all enterprise, Public Safety, SCADA, and wireless networks. This includes but is not limited to any network infrastructure owned by the City of Charlotte which may or may not be directly connected to the City enterprise network.

All City computer systems should be running the most recent security patches to ensure that exposure to system flaws and vulnerabilities are minimized. All security revisions and patches released by vendors must be identified as soon as possible. The City requires that all systems accept the latest security patches; there is not the option to opt out of an available and applicable security patch. Administrative owner groups must have processes in place to maintain awareness of the most recent and available patches. All applicable security patches shall be applied to systems within 30 days of announcement. Occasionally, patches are released that address vulnerabilities which are being actively exploited in the wild. Deployment of such patches must be expedited and applied to systems quickly to address the risk. Deployment timing for these patches will be determined by the CSO on a case-by-case basis. Security patches for SCADA and/or operational technology (OT) environments may be extensively vetted for operational risk, but must be applied within 90 days of announcement.

8.5. Maintenance

Regular maintenance of all equipment and software is critical to reducing risk. Maintenance should be conducted on a regular basis to ensure safety, security, and reliability of products and services. Any access required to information systems or City data to perform maintenance must be granted in compliance with the procedures defined within this Manual.

8.6. Data Sanitization

System owners are responsible for sanitizing any hardware component that may retain City data prior to reallocating or disposing of that component. The CSO is responsible for developing and publishing requirements for this sanitization process and identifying tools and processes that adequately prevent the inadvertent disclosure of data or sensitive information. At a minimum, any device containing sensitive information must be sanitized using a process this is equivalent with industry best practices such as NIST SP 800-88.

More information can be found in City procedure, Surplus Computer Disposal Procedure (BSS 10)

8.7. Disposal

Any disposal of media, data, software, or hardware must be conducted in compliance with processes established by the CSO to prevent unauthorized disclosure of sensitive information.

8.8. Change Management

I&T is responsible for the enterprise Change Management process that aligns with and supports the CSO procedure. The I&T Change Management processes will help ensure the security of all City of Charlotte technology dependent systems through appropriate lifecycle management. This includes service design, deployment, upgrades, retirement, and any other activities that may affect the physical or logical architecture of the City of Charlotte enterprise. The only approved tool used to support the Change Management process is the I&T solution. Any other system or tool is considered non-compliant with the established Change Management process.

The Aviation Department has their own change management process for the Aviation and Tenant networks, including weekly CAB meetings which are separate from the City of Charlotte's I&T processes.

The I&T Public Safety Communications team utilizes the Regional Radio Communications Council (RCC) Change Management Process.

8.9. Documentation Management

I&T Divisions are responsible for ensuring that system logs, audit records, incident reports, and information technology-related accreditations or certificates are maintained in a consistent and structured manner. In maintaining these documents, the I&T Divisions are also responsible for compliance with any established City procedures with respect to the time limitations and methods of storage.

Files should be maintained as necessary for operational purposes (e.g., audits and incident response) as well as for the purpose of compliance with any applicable laws or regulations. The CSO must ensure this information is maintained securely and steps are taken to protect personal information from unauthorized access, modification or disclosure. Any documents containing personally identifiable information (PII) must be destroyed or have the PII removed when no longer required.

8.10. Back-ups

Back-ups and recovery testing of critical business information should be conducted regularly to ensure critical information is available and has the appropriate protection. The CSO is responsible for establishing requirements for the types of information that must be backed up, the frequency of those backups, and the transport and storage of backups. I&T will maintain control over the storage, internal or external distribution and accessibility of all media.

Requirements:

- All City information servers must be backed up.
- All City information server backups should include the server Operating System and data necessary to recover the complete system in the event of a disaster. This is commonly referred to as bare-metal recovery.
- All City backups should be replicated to the City's designated off-site recovery facility to provide site redundancy. The recovery facility should be supported by badge access controls, surveillance cameras, dual power grids, UPS and generators. A review of the back-up location's security will be performed annually.
- All City information server backups which use network attach storage (NAS) or file shares (SMB) must leverage file retention locks to prevent unauthorized modification of backups once written. In addition, any file shares used for backups should have distinct and independent paths and permission from other environments and backup repositories. Permissions to read and modify backups on file shares should be limited to administrators only.
- Critical systems refer to servers and their associated applications which are essential for, but not limited to, business operations.
- Critical system backups should employ multi-factor authentication due to the sensitive and confidential nature of data being stored in backups.
- Routine restoration and recovery should be performed to ensure the useability of the backups to recover servers. Critical system backups should be tested bi-annually.
- The City will maintain a log of all media and conduct media inventories at least annually.

9. Data and Infrastructure Security

Scope: The Data and Infrastructure Security Procedure establishes a computer and network security procedure that assures: confidentiality of data that is exempt by City code and State or Federal laws from disclosure to unauthorized individuals; integrity of public and protected data from unauthorized, unanticipated, or unintentional destruction, modification, or access; and, availability of data and computer network resources to authorized users to meet business requirements and maintain the full faith and confidence of constituents.

9.1. Network Security

The CSO is responsible for monitoring and mitigating risks to City networks and information systems to protect against internal and external threats.

9.1.1. Monitoring

The CSO is responsible for establishing and maintaining the technical capability to monitor and mitigate network traffic, e-mail, activities on information systems, and user behavior for the purpose of detecting and identifying potentially malicious activity. At a minimum, all inbound and outbound network traffic shall be monitored using industry standard tools for devices such as firewalls, intrusion detection systems, and email filtering. To the extent feasible, the CSO will monitor all internal network traffic for malicious activity.

In order to ensure compliance with City policies, the City also reserves the right to use monitoring software in order to check upon the use and content of emails. Such monitoring will be employed in accordance with approved procedures. In addition, the CSO reserves the right to monitor connections between City networks and any partner or third-party networks for security procedure violations and anomalous activities.

9.1.2. Network Infrastructure Procedure

The term “managed network device” refers to City owned and managed routers, switches, VPN appliances, optical network system, wireless controllers, and wireless access points whether managed by I&T or departmental resources. Please refer to the Wireless Networking and VPN procedure for further details on wireless infrastructure. The CSO is responsible for ensuring the security of all managed network devices which includes the City Enterprise, Public Safety, Transportation, SCADA and other De-militarized Zone (DMZ) networks.

All managed network devices should be secured in an area where physical access (power, console port, uplink port) is limited to authorized device administrators and where access to the equipment can be monitored. The use of badge readers and video surveillance shall be used in data centers where managed network devices are installed.

In addition, managed network device software should be updated to the latest stable and secure code on a regular basis.

The management for City or department network operations is responsible to the CSO for:

- Determining installation location of all managed network devices.
- Maintaining a directory of standard system software for all managed network devices.
- Determining the network device and role associations to comply with role-based security.

- Establishing a review board and maintaining the process for evaluating network device administrators for role-based security.
- Maintaining a hardened device template based on NSA and other best practice security recommendations. This template should be reviewed with security annually to ensure compliance.

I&T or department network engineers, administrators and technicians are responsible to the CSO for:

- Maintaining the physical security of all managed network devices once the installation has been completed.
- Installing and maintaining the latest standard system software on all managed network devices to include bootcode firmware and operating system.
- Installing and maintaining the current hardened device template on all managed network devices.
- Maintaining the most accurate information on all managed network devices in a central management system at minimum to include:
 - Make and model
 - Physical location
 - Point of contact and contact information
 - Serial number
 - Purpose of device
- Ensuring all managed network devices are accessible via SSH using centralized authentication and authorization at all times.
- Ensure SSH retries are set to three times to prevent brute-force login attempts.
- Ensuring artificial network processes or anti-timeout mechanisms are not to be used to keep managed network device connections open.
- Ensuring administrative passwords are not stored in SSH client configurations.
- Ensuring all local managed network device accounts are stored individually in CyberArk and passwords are changed every 90 days.
- Ensuring all managed network device configurations backed up to a central repository for daily audit.
- Ensuring daily audit reports are monitored, evaluated and corrected for deviations in the hardened device template and errors.
- Ensuring all switches are audited for unused ports, and those unused ports are shutdown.
- Ensuring that all unmanaged or rogue network devices, such as non-City owned SOHO hubs, switches or routers, or unauthorized wireless access points, are reported to the CSO and confiscated immediately.
- Ensuring network devices require strong authentication for dynamic routing protocols as well as Simple Network Management Protocol (SNMP). Password hashing for authentication strings must be enabled when supported.
- Ensuring proper network device segmentation:

- User Network – The user network should be separate from all other networks. This network segment will also include City-approved wireless access points (not wireless bridges). No static IPs are allowed in this network segment. All user network ports should employ layer-2 segmentation to prevent user devices from communicating with devices on the same layer-2 network.
- Printer Network – A printer network should be separate from all other networks with access control lists preventing printers from communicating with any device other than approved City print servers. No static IPs are allowed in this network segment. All printer network ports shall employ layer-2 segmentation to prevent printers from communicating with devices on the same layer-2 network.
- Voice Network – A voice network should be separate from all other networks with access control lists preventing VoIP phones from communicating with any device other than approved VoIP servers. No static IPs are allowed in this network segment.
- Security Network – A security network should be separate from all other networks with limited access to the Enterprise network. This network segment is used for appliances which fit none of the above categorizations. Some examples include: Veeder Root tank monitoring, UPS management, or IP Cameras. Limited use of static IPs are allowed in this network segment with the Information Security team approval. All security network ports will employ layer-2 segmentation to prevent security devices from communicating with devices on the same layer-2 network. Also, the Information Security team reserves all 10.x.69.x networks for their appropriate security networks as needed.
- Additional segmentation – Additional segmentation should be done in datacenters for organization and security. For example, DNS/DHCP/AD/Storage servers should be segmented to a separate network from other servers. In some cases, certain servers may need to be segmented into firewall DMZs. As need InfoSec personnel may require QoS priority above other traffic to rapidly respond to security incidents. Please coordinate with the Information Security team for additional segmentation direction.

Each managed network device must implement the following warning banner for display at the time a user logs on:

***** Warning! Warning! Warning! *****

This system is restricted to CITY of CHARLOTTE Intranet administrators and users for business purposes only. Unauthorized access is unlawful and violators will be prosecuted. This service may be monitored for administrative and security reasons. By proceeding, you consent to this monitoring.

***** Warning! Warning! Warning! *****

9.1.3. Firewall Policies and Installation Procedures

General Overview

A firewall procedure dictates how firewalls should handle network traffic for specific IP addresses and address ranges, protocols, applications, and content types (e.g., active content); the documentation requirements for approval and the approval process which are adherent to the City's Information Security Policy. Also, the procedure will set forth the expectations for completion of firewall rule requests.

The Cyber Security Manager in conjunction with the CSO is responsible for establishing and maintaining City Firewall policies. The Cyber Security – Defense team will implement approved firewall changes at the direction of the Cyber Security Manager. The CSO must approve all firewall design and configuration requirements associated with third party networks or services.

Documentation Requirements

Documentation is required for approving firewall rule requests. This documentation should generally come from the vendor of the software or device which is used in the communications. If vendor documentation does not exist, the requestor should schedule a meeting with the Cyber Security team to assist in the creation of this documentation. This documentation should include application and infrastructure architecture designs for reviewing the proposed request.

Any document that contains details on the positioning or configurations of City firewalls must be redacted and not be disseminated without prior approval from the CSO. Firewalls and security devices will not be named with a standard naming convention, instead using an obfuscation naming convention. The obfuscated names will be maintained by Cyber Security staff and may be made available on a need to know basis.

Approval Process

Firewall procedures should be whitelist-based, dropping all inbound and outbound traffic, with security exceptions made for approved traffic. Firewall security exceptions are made through the Cyber Security Services section of the self-service portal and are thoroughly evaluated by the Cyber Security team. In certain cases, additional documentation and discussion may be required. Approved firewall security exceptions will be implemented within 24-48 hours during the approved installation windows. All threat and application firewall database updates will occur weekly. If approved and based on urgent business or security need, firewall security exceptions may be completed outside of these windows. Typically, these are done in conjunction with a scheduled change control. Firewall security exceptions should be requested **in advance** of any project or departmental deadline to ensure a thorough security risk evaluation is conducted.

Projects

All project-related firewall requests should be submitted in a revision-tracked, consolidated and single project documentation format which articulates many of the commonly asked questions such as source IP, destination IP and destination port. Enough time should be allotted during the planning phase of the project to account for all required communication rules so that minimal changes are required leading up to project deadlines. If changes are required in post-planning phases of the project, this document may be updated and those updates should be highlighted for easy discernment.

This firewall project documentation should include the following:

1. Table of Contents
2. Revision history
3. Statement of Confidentiality

4. Host Group Definition section grouped by function (Name, IP Address, Description)
5. Port Definition section (Protocol, Ports, Purpose)
6. Application Communications section sectioned by function (Source, Destination, Port, Purpose)
7. Document password protection

All projects shall be coordinated with the Cyber Security management to ensure appropriate time and resources are allocated for the security risk evaluation and implementation.

Zones

Firewalls are commonly delimited by a trusted and untrusted zone. The security evaluation process which each firewall request undergoes is a careful review of how the proposed firewall rule might impact the security posture of the firewall's protected infrastructure or trusted zone. A comprehensive business justification is required for each firewall request. Depending on the detail received for the business justification, firewall requests may require additional investigation to determine the full extent of the proposal. After the security evaluation is completed, the request is either approved for installation or rejected due to security risk.

Expiration

Approved firewall rules are not infinite. At regular intervals, firewall audits are done to verify if installed rules are still required. If a firewall rule is installed but not used for a period of six months, those rules will be evaluated for removal.

Host-based Firewalls

All City workstations and servers must have a functional host-based firewall installed; the management and deployment of that capability will reside with the CSO. Certain standards and regulations, such as PCI and CJIS, may require additional firewall protections for customer data. The CSO is responsible for fulfilling all regulatory obligations as they pertain to firewall implementation.

9.1.4. Testing

Cyber Security systems and plans should be regularly tested to avoid exploitation of critical information or data. Testing of Cyber Security systems will also help prevent unknown programming vulnerabilities.

9.2. Wireless Networking and Communication Procedure

9.2.1. Wireless Access Points

The CSO is responsible for monitoring and securing Wireless Access Points. The connection of any wireless access point to the City network without written approval by the CSO is prohibited. I&T Network Operations is responsible for maintaining an inventory of all authorized Wireless Access Points in use including documented business justification. Network Operations must also perform quarterly auditing, testing, or scanning for rogue wireless access points. Scanning or testing methods must be sufficient to detect and identify authorized and unauthorized Wireless Access Points. I&T is responsible for ensuring that default passwords are changed, and appropriate encryption is implemented on all wireless access points. Audit logs should be protected from modification by unauthorized users and system administrators. As deemed necessary by the CSO, access points may be subject to periodic penetration tests and audits. In addition, the following procedures should be followed in regard to wireless communications:

- The Service Set Identification (SSID) shall be configured so that it does not contain any identifying information.
- All enterprise and guest wireless SSIDs should be hidden and not broadcasted.
- All SSID's and their security parameters to be approved by the CSO.
- Defensive mechanisms such as rogue AP detection, black holing, handshake validation and rate limiting should be deployed to protect the City's infrastructure and users from attack.
- Encryption for wireless networks shall be AES-CCMP WPAv2 or greater.
- IEEE 802.1X - EAP PEAP authentication shall be used for all enterprise wireless networks. Guest networks may be created with pre-shared authentication if approved by the CSO.
- All wireless pre-shared authentication keys will be changed every six months.
- All rogue wireless access points in City facilities should be investigated to determine if the uplink is the City Enterprise network and if so, reported to the CSO and confiscated immediately.
- All wireless access points will be centrally managed and audited.
- All wireless controller and management configuration should generate and publish security compliance reports.
- All wireless zones should be protected with a network ACL which prevents inter-zone communications. Also, client isolation should be deployed.
- All wireless access points must be physically secured to prevent tampering or theft.

9.2.2. Wireless Devices

This procedure pertains to all wireless data communication devices, e.g., personal computers, tablets, mobile phones, etc., connected to any City network. This procedure prohibits access to City networks via unsecured wireless communication devices. All wireless connections to the City network must be authenticated and encrypted.

Devices connected to the internal network shall never connect to a separate network via a wireless connection. No Wireless device shall be installed on City equipment without prior approval by the CSO. All wireless Network Interface Cards (e.g., PC cards) used in corporate laptop or desktop computers must be registered with Shared Services - Technology Management (I&T). Any loss of City-owned wireless devices or personal devices that are used for City business should be reported immediately to the Technology Service Desk.

9.2.3. Bluetooth Procedure

Hands-free enabling devices, such as the Bluetooth, may be issued to authorized City personnel. The following are guiding principles for the use of Bluetooth services:

- Employees should ensure that Bluetooth pairing does not take place in public area to prevent incidental pairing with other devices.
- All Bluetooth devices shall employ "Security Mode 3", which encrypts traffic in both directions, between your Bluetooth Device and its paired equipment.
- If possible, default PIN numbers should be changed immediately. Use a minimum PIN length of eight (8).

- Switch Bluetooth devices into non-discoverable mode.
- Bluetooth mode must be turned off when not in use.

9.2.4. Guest Wireless Access

The use of city-owned Guest Wireless is a way to provide Internet access to non-City employees for business-related functions as opposed to Public Wireless networks which are for citizen personal usage. City employees should only connect to Enterprise Wireless. Guest Wireless networks will be subject to further scrutiny since the computers and devices connecting to these networks are unmanaged, their users are unknown, and the users are using the City's Internet connection. Thus, Guest Wireless security involves taking steps to remove client access in order to prevent illegal, suspicious, or unauthorized access.

9.3. Electronic Commerce

The CSO is responsible for ensuring that all payment card processing and storage occurs inside a secure computing environment, which is segmented from the rest of the network with additional safeguards and monitoring applied to ensure due diligence in protecting customer data. The CSO is responsible for ensuring all legal and regulatory requirements are met for e-commerce applications.

9.4. Vulnerability Management

The CSO is responsible for establishing and maintaining the City's vulnerability management process by assessing City information systems for vulnerabilities, prioritizing discovered vulnerabilities, and directing remediation of vulnerabilities as a part of the overall risk management function.

9.4.1. Assessment

Awareness of the latest information system vulnerabilities will be maintained through regular monitoring of information security publications, news media, vendor disclosures, and vendor patch publications. On a recurring basis, as determined by the CSO, the City's networks will be assessed to determine if information systems with a vulnerable configuration are present. Assessments may be performed through vulnerability scans, penetration tests, asset audits, or other methods deemed appropriate by the CSO. A Vulnerability Report will be produced detailing the results of assessments.

9.4.2. Prioritization

On a recurring basis, as determined by the CSO, the CIRT will convene to operate the vulnerability management program and invite system administrators and information owners when vulnerabilities affecting their systems or information are scheduled to be discussed. The CIRT, chaired by the CSO, will review the latest vulnerability reports and determine the level of risk of the vulnerabilities discovered on the City's information systems, taking into account the affected asset's priority and threats faced by the City. Based on the risk level determined by the CIRT, the vulnerabilities will be prioritized and the CIRT will determine appropriate remediation measures for the vulnerabilities. The CIRT will produce Remediation Advisories detailing the remediation measures that should be implemented and the order in which they should be prioritized.

Vulnerabilities are classified into the following groups:

- Critical – A vulnerability, which, if exploited would allow malicious native-code to execute, potentially without a user being aware.

- High – A vulnerability, which, if exploited would compromise data security, potentially allowing access to confidential data, or could compromise processing resources in a user's computer.
- Medium – A vulnerability that is limited to a significant degree by factors such as default configuration, auditing, or is difficult to exploit.
- Low – A vulnerabilities that typically has very little impact on an organization's business. Exploitation of such vulnerabilities usually requires local or physical system access.

Once vulnerabilities are discovered, confirmed to exist, and rated for their impact and likelihood in the City's environment, the Information Security team will notify the asset owners via an official means. This could include an official report out meeting, vendor disclosure, patch release notifications, or other means.

9.4.3. Remediation

Remediation advisories, as produced by the CIRT, will be distributed to information system administrators to direct remediation steps for their respective systems. Prior to applying remediation measures, system administrators will perform an appropriate level of testing to ensure systems operate as expected after remediation measures are applied and that remediation measures do not induce unanticipated system degradation. System administrators will conform to the City's configuration control policy when applying remediation measures. Once remediation measures are applied, applicable information systems will be rescanned to ensure targeted vulnerabilities have been successfully remediated.

Remediation timelines for vulnerabilities are based on the severity of impact and likelihood of occurrence. The asset owners shall remediate the vulnerability according to the following timeframe:

- Critical – 7 days
- High – 30 days
- Medium – 60 days
- Low – 180 days

Vulnerabilities that are not able to be remediated in the required timeframe shall be brought to the attention of the Information Security team. A new remediation plan must be submitted detailing reasons why the deadline was missed, steps taken to remediate the vulnerabilities, dates and milestones to track remediation and verification of fixes prior to implementation in production.

Any vulnerability identified that is either not able to be remediated or the asset owners are accepting the risk of the vulnerability, must be submitted as an exception to the information security team for documentation and approval.

9.5. Encryption

This procedure applies to the use of any encryption algorithm being used to protect sensitive or confidential data at rest or in transit. Encryption is necessary for records and files containing information that, (1) is declared confidential by North Carolina Revised Statutes or is otherwise exempt from inspection, and (2) is protected from disclosure or inspection by Federal laws or codes, and that will be stored in non-secure locations or transmitted over open City networks and the Internet.

Encryption helps to maintain the confidentiality of City information. When implementing encryption, the required level of protection should be identified, taking into account the type, strength, and quality of the

encryption algorithm required. Any transmission of sensitive City information should be performed utilizing an industry standard level of encryption. The CSO is responsible for establishing guidelines on the use of cryptographic keys and certificates to protect City information. At a minimum, these guidelines shall include the following:

- The preferred encryption algorithm is AES 256 bit
 - If a device is not capable of AES 256 bit, AES 128 bit may be used with CSO approval
- The use of proprietary encryption algorithms is prohibited.
- The export of encryption technologies is restricted by the U.S. Government.
- Algorithms must comply with federal and state regulations.
- Effective key management practices shall be implemented such that only trusted keys and/or certificates are accepted.
- Digital Certificates may only be issued by City-approved certificate authorities. Access to digital certificates stored on computer systems must be protected by passwords and passphrases.
- Customer information that is transmitted over a wireless network must be encrypted.

9.6. Endpoint Protection

Protections against malicious code, such as endpoint protection and other controls shall be implemented on all City devices. Only approved endpoint security software may be installed on City systems. All users should be aware of the types of malicious code or logic that could compromise a computer or system. The following are general guidelines for endpoint protection:

- The City will use SentinelOne Agent as the standard endpoint protection solution for the City.
- Business continuity plans should include remediation necessary for recovering from malicious code attacks, including all necessary data and software back-up and recovery arrangements
- All incoming mail and files received from external networks must be scanned for viruses as they are received.
- Endpoint protection software shall be installed on servers and kept on the latest version in order to limit the spread of viruses within the City network.

9.7. Server Security

The purpose of this procedure is to standardize the base configuration of internal server equipment owned or leased by the City, with the overall goal of minimizing unauthorized access to proprietary information and technology. Approved server configuration guides must be established and maintained, based on business needs and periodically reviewed. Departments should monitor configuration compliance and implement an Exception Procedure specific to their environment. Configuration changes must be performed in compliance with City change management policies.

This procedure applies to server equipment owned or leased by the City of Charlotte, and to servers registered under any corporate internal network domain.

9.7.1. Server Security Principles

- **Simplicity:** Security mechanisms should be as simple as possible. Complexity is at the root of many security issues.

- **Layered Defense:** Security mechanisms should be layered so that compromise of a single defensive measure is not sufficient to compromise the host or network.
- **Psychological Acceptance:** Staff should understand the necessity of security. Security mechanisms should be sensible and give staff the usability they require to perform their duties. If they find security mechanisms too cumbersome, they may devise ways to work around or compromise them. Security should not be weakened so it is understandable and acceptable; rather the objective is to educate staff and design procedures that are usable and effective.
- **Least Privilege:** Each process, user or task should be granted only the minimum required rights to perform its job so that if compromised, the scope of the damage is constrained to the limited resources that were granted.
- **Effort Factor:** There should be an understanding of what it would take to break a system's security defenses. The amount of effort necessary should exceed the value that would be gained from a successful compromise.

9.7.2. Ownership and Responsibilities

All internal servers must be managed in accordance with processes approved by the CSO. Approved server configuration guides must be established and maintained, based on business needs and periodically reviewed. Departments should monitor configuration compliance and implement an Exception Procedure specific to their environment. Each Department must establish a process for changing the configuration guides, which includes review and approval by the CSO in accordance with the Change Management Procedure.

Servers must be registered within the City-wide corporate management system. At a minimum, the following information is required to positively identify the point of contact:

- Server contact(s) and location and a backup contact
- Hardware and operating system/version
- Main functions and applications, if applicable.

Information in the City-wide corporate management system must be kept up-to-date. Any configuration changes for production servers must follow the appropriate change management procedures.

9.7.3. Management

Effective management practices are essential to operating and maintaining a secure server. Security practices include the identification of an organization's information system assets and the development, documentation, and implementation of policies, standards, procedures, and guidelines that ensure confidentiality, integrity, and availability of information system resources. Implementation of the following practices is part of a robust security procedure;

- **Change Management:** Controlling modification to a system's design, software, hardware and firmware helps to protect against the introduction of improper modifications.
- **Standardized Configurations and Builds:** Provides consistency with information security procedures as well as providing support benefits.
- **Business Continuity Planning (BCP):** Allows the City to maintain operations in the event of a disruption. For more information refer to the Business Continuity Planning section (ADM 12).

- **Server Backup:** Maintains the integrity of the data on a server and provides the ability to restore in the case of a malicious or unintentional act or a hardware or software failure. There are also legal and financial reasons for maintaining a good backup procedure.

9.7.4. **Server Configuration**

- Operating System configuration should be in accordance with approved I&T guidelines.
- Servers must be registered within the City-wide corporate management system.
- Remove all services, applications and network protocols (e.g., IPv4, IPv6) that are not required and disable any unnecessary components that cannot be removed. If possible, start with a minimal OS installation and then add, remove or disable applications, services and protocols as necessary.
- Remove or disable unneeded or non-interactive server accounts. For Unix systems, disable the login shell (e.g., /bin/false) for non-interactive system accounts and disable remote root login.
- A patching process should be created, documented and implemented. Vulnerabilities should be mitigated temporarily if possible and permanent security fixes (patches or upgrades) should be applied as soon as practical.
- Secure protocols that provide encryption of usernames, passwords, and data (e.g., SSH, HTTPS) must be used. Do not use unencrypted protocols (e.g., telnet, FTP, HTTP).
- Servers should be physically located in an access-controlled environment. Servers are specifically prohibited from operating from uncontrolled cubicle areas.
- Configure Network Time Protocol (NTP) synchronization. As some authentication protocols will not function if the time difference with the authenticating server is significant, Network Operations will ensure:
 - All critical system clocks are synchronized, consistent and have the correct time. Accurate time stamps are necessary for accurate logging.
 - Time data is protected.
 - Time settings are received from an industry-accepted time source.
 - Changes to time settings are logged, monitored, and reviewed.
- Disable Server Message Block version 1 (SMB1) in all SMB or Samba servers and clients.
- SSH global client configuration on servers should be set to deny the creation of tunnels.

9.7.5. **Monitoring**

- All security-related events on critical or sensitive systems will be logged and audit trails saved as follows:
 - All security related logs will be kept online for a minimum of 90 days and offline for 1 year.
- Security-related events will be reported to the Information Security team, who will review logs and report incidents to IT management. Corrective measures will be prescribed as needed. Security-related events include, but are not limited to:
 - Port-scan attacks

- Evidence of unauthorized access to administrator accounts
- Anomalous occurrences that are not related to specific applications on the host.

9.7.6. Compliance

Audits will be performed on a regular basis by authorized individuals designated by the CSO

Audits will be managed by the internal audit group or the CSO, in accordance with the Audit and Compliance Procedure. The CSO will filter findings not related to a specific operational group and then present the findings to the appropriate support staff for remediation or justification.

Every effort will be made to prevent audits from causing operational failures or disruptions.

9.8. DMZ Procedure

Network and Host Internet devices residing in the DMZ of a network are particularly vulnerable to attack, lack adequate security mechanisms for production use, and contain network connectivity or devices outside of the City of Charlotte control. Accordingly, it is critical to define standards designed to minimize the City's potential exposure from the loss of sensitive or confidential data, or intellectual property, etc.

Equipment and applications within the scope of this procedure must adhere to processes approved by the CSO for DMZ systems, applications, and network management. Adherence to these requirements will minimize the potential risk to public image caused by unauthorized use of corporate resources, and the loss of sensitive or confidential data and intellectual property.

The following guidelines must be met:

- DMZ configurations must include the use of firewall zones and network segmentation.
- Changes to the connectivity and/or purpose of existing DMZ areas and establishment of new DMZ areas must be approved by the CSO and coordinated with the Cyber Security Manager.
- The CSO and/or Cyber Security Manager reserve the right to interrupt connections if a security concern exists. Traffic from DMZ areas to the production network should be limited to an absolute minimum.

9.8.1. DMZ Equipment Guidelines

Equipment should be maintained to ensure its continued availability and integrity. Privileges should be allocated to users on a need-to-use basis and on an event-by-event basis in line with the access control procedure. All new DMZ equipment must present a business justification approved by an area manager, prior to submission to the CSO for approval.

For compliance verification purposes and at the discretion of the CSO, I&T will periodically audit DMZ equipment in accordance with the Audit and Accountability Procedure.

- Any use of the DMZ on the internal network must be approved by the CSO.
- Any equipment added to DMZ networks must be coordinated with the Cyber Security team to ensure the device is contained in the appropriate DMZ.
- DMZ equipment should be in a physically separate room from any internal networks. If this is not possible, the equipment must be in a locked rack with limited access.

- I&T must maintain a list of who has physical and network access to the equipment.
- DMZ equipment must not be connected to the production networks, either directly or via a wireless connection.
- Security of the equipment deployed by external service providers must be clarified in the contract with the service provider and security contacts, and escalation procedures documented. Contracting departments are responsible for third party compliance with this procedure.
- Operating systems of all hosts internal to the DMZ Lab running Internet Services must be configured to the secure host installation and configuration standards.
- Services and applications not serving business requirements must be disabled.
- Confidential information is prohibited on equipment where non-City personnel have physical access.
- Hardware, operating systems, services, and applications must be approved by the CSO, or designees, as part of the pre-deployment review phase.
- Operating system configuration must be done according to the secure host and router installation and configuration standards.
- Services and applications not serving business requirements must be disabled.
- Trust relationships between systems may only be introduced according to business requirements, must be documented, and must be approved by the CSO.
- Insecure services or protocols must be replaced with more secure equivalents whenever such exist.
- Remote administration must be performed over secure channels, such as encrypted network connections using the highest available level of encryption for SSH or IPSEC, or console access independent from the DMZ networks. Where a methodology for secure channel connections is not available, one-time passwords must be used for all access levels.
- Network interfaces must have appropriate Domain Name Server records (minimum of A and PTR records).
- Password must be maintained in the City's CyberArk password vault
- Changes to existing equipment or deployment of new equipment must follow change management processes/procedures.
- All host content updates must occur over secure channels.

All equipment must be documented and registered in the City Asset Management program, and include the following information:

- Host contacts and location
- Hardware and operating system/version
- Main functions and applications.

9.8.2. Internet-facing Web Servers

All City-owned Internet-facing web sites should be reviewed and approved by Information Security before they are placed online whether they exist in the cloud, or in any third-party host environment. The following security controls should be applied to internet-facing web services as necessary:

- Secured by the F5 Web Application Firewall or via an approved cloud-based Web Application Firewall
- Secured with TLS 1.2 and ECDHE ciphers.
- Application/OS vulnerability scanning
- PCI vulnerability scanning
- All internet-facing services (websites, APIs, etc) will require penetration testing and remediation prior to production go-live. Remediation may result in design changes.
- Will be placed in DMZs with restricted network access.

10. Third-Party/Cloud and Vendor Management

Scope: The City will establish a third party/cloud and vendor management and security procedure. This procedure ensures that the use of third parties/cloud and vendors will not cause undue harm to the City's operations or systems. Any increased risk of using an external party for any services should be avoided. The processing and dissemination of information by an external party should have the appropriate security controls implemented.

The CSO is responsible for ensuring that appropriate security controls are implemented to protect the integrity and privacy of City assets stored on third-party or vendor networks. The City should verify that a third-party service provider is validated in PCI if the service provider handles payment card information. At no time should the City rely on access/authorization control mechanisms at the Third Party's site to protect or prohibit access to City confidential information.

The City of Charlotte will not be responsible for ensuring the protection of third-party information. The third party shall be entirely responsible for providing the appropriate security measures to ensure protection of their private internal network and information.

10.1. Formal Agreements

This procedure applies to the following formal agreements:

- Third party network connection agreement
- Network connection procedure
- Third party connection request
- Information Requirements Document
- Non-Disclosure Agreement
- Equipment Loan Agreement (when applicable)

Contact the I&T Information Security team for more details about the above documents and their use.

Each agreement represents a formal commitment between the signatories concerning the subject matter of the agreement and replaces any prior oral or written communications between the parties. There are no conditions, understandings, agreements, representations, or warranties, expressed or implied, which are not specified herein. These agreements may only be modified by a written document executed by the parties hereto. Any disputes arising out of or in connection with these agreements shall be governed by North Carolina law without regard to choice of law provisions.

Each party will be responsible for all costs incurred by that party under each agreement, including, without limitation, costs for phone charges, telecommunications equipment, and personnel for maintaining the network connection.

10.1.1. Protection of Information and Resources

The CSO is responsible for ensuring appropriate security controls for the protection of information and resources are in place, such as the application of encryption for the transmission of data. The protection of information and resources helps to ensure business continuity and minimize risk to the City. Requirements for confidentiality or non-disclosure agreements reflecting the City's needs for the protection of information should be identified and regularly reviewed. Listed below are guidelines suggested for the protection of information:

- Define information for protection (e.g., confidential information).
- Bound the duration of an agreement, including cases where confidentiality might need to be maintained indefinitely.
- Required actions when an agreement is terminated.
- Responsibilities and actions of signatories to avoid unauthorized information disclosure, (e.g., classification labels).
- Ownership of information, trade secrets and intellectual property, and how this relates to the protection of confidential information.
- Permitted use of confidential information, and rights of the signatory to use information;
- Right to audit and monitor activities that involve confidential information.
- Process for notification and reporting of unauthorized disclosure or confidential information breaches.
- Terms for information to be returned or destroyed at agreement cessation.
- Expected actions to be taken in case of a breach of this agreement.

10.1.2. Severability, Waiver, Assignment, Liability for Failure to Perform

If for any reason a court of competent jurisdiction finds any provision or portion of this Agreement to be unenforceable, that provision of the Agreement will be enforced to the maximum extent permissible so as to affect the intent of the parties, and the remainder of this Agreement will continue in full force and effect.

The failure of any party to enforce any of the provisions of this Agreement will not be construed to be a waiver of the right of such party thereafter to enforce such provisions.

Neither party may assign this Agreement, in whole or in part, without the other party's prior written consent. Any attempt to do so will be null and of no effect. Subject to the foregoing, this Agreement is for the benefit of and will be binding upon the parties' respective successors and permitted assigns.

Neither party will be liable for the failure, disruption, or delay in meeting obligations stated in this Agreement if they occur as the result of an "act of God" or a cause beyond either party's reasonable control, including but not limited to any mechanical, electronic, or communications failure.

10.2. Business to Business Virtual Private Network Connections

A business to business connection occurs when third party organizations connect to City networks for the purpose of conducting business transactions. This procedure applies to all connections between third parties that require access to non-public resources, regardless of whether a circuit is used for the connection.

Connections from third parties should be subjected to an information risk analysis. The City should ensure that the third party maintains sufficient service capability together with workable plans designed to ensure that agreed service continuity levels are maintained following major service failures or disaster.

The City should pursue appropriate due diligence in service provider research and selection, contractual assurances regarding security responsibilities, controls, and reporting, nondisclosure agreements regarding the institution's systems and data, independent review of the service provider's security though

appropriate audits and tests, and coordination of incident response procedures and contractual notification requirements. Special controls should be established to safeguard the confidentiality and integrity of data passing over public networks or over wireless networks, and to protect the connected systems and application. The CSO is responsible for conducting a periodic review of controls and integrity procedures to ensure that they will not be compromised by the changes.

All new connection requests involving third parties require a signed Third Party Connection Agreement. This agreement must be signed by the Director of the Department as well as a representative from the third party who is legally empowered to sign on their behalf. The signed document is to be kept on file with both the relevant extranet team and the CSO. Documents pertaining to connections into corporate labs are to be kept on file with the responsible manager and the CSO.

NOTE: B2B VPN tunnels have limitations regarding network capacity. While there are several advantages to the usage of these connections, the business should determine the level of criticality of their application before seeking to this type of connectivity. In some cases, dedicated circuits are apropos for business to business connectivity because of increased network traffic required or stability requirements. Since B2B VPN tunnels rely on the Internet, which is outside the control of the City, they are considered best-effort connections.

The following guidelines apply to business-to-business connections:

- All connectivity established must be based on the least-access principle.
- B2B VPN tunnels use is to be controlled using either a shared secret or certificate authentication.
- In no case will the City rely upon third parties to protect corporate networks or resources.
- Security of third-party connections will be maintained by a firewall rule base on the Partner's routers to which the third-party sites are connected.
- The firewall rule base will restrict access to pre-defined hosts within the network. The ACLs will be established and managed by the Cyber Security Manager in conjunction with the CSO. Third party network access points will be established in locations where minimal cost is incurred.
- All access changes must be accompanied by a valid business justification and are subject to security review. Any changes must follow the Change Management Procedure.
- When access is no longer required, Departments must notify the CSO, which will then terminate the access. This may mean a modification of existing permissions up to terminating the circuit, as appropriate.
- Third parties may only use approved network connections for the specific business purposes defined by the CSO.
- All third-party network connections will be reviewed on a quarterly basis and information regarding specific third party network connections will be updated as necessary. Third party network connections no longer in use will be terminated immediately.

To maintain the network's security with a third-party connection, the following standards must be in place:

- Secure Shell (SSH) version 2 access from the Internet will be provided to the third-party gateway machine (SSH version 1 and Telnet access will not be granted), where the connection will be authenticated. Once the connection is authenticated, SSH sessions to internal hosts will be limited to necessary services only.

- Services provided over third-party network connections should be limited only to those services needed, and only to those devices (hosts, routers, etc.) needed. The default procedure position is to deny all access and then only allow those specific services that are needed and approved by the CSO.
- In no case shall a third-party network connection to the City production network be used as the Internet connection for the third party.

Any existing third-party network connections that do not meet all of the guidelines and requirements defined in this procedure will be re-engineered as needed at the discretion of the CSO.

10.3. City-Owned Equipment

The City of Charlotte maintains the decision to loan, or not to loan, any third-party equipment or software for use on City premises. This equipment will be used solely by third parties on City premises and for the purposes defined in this Agreement. Any changes to the configuration must follow the Exception Procedure and be granted approval in writing by the CSO. Third parties will not change or delete any passwords set on City equipment without prior approval of the CSO. All such equipment will be documented. Access to network devices, such as routers and switches, will only be provided to City support personnel. All City-owned equipment located at Third Party sites must be used only for business purposes. Any misuse of access or tampering with City-owned hardware or software, except as authorized in writing by the CSO or designees, may result in termination of the connection agreement with the Third Party.

10.4. Audit and Review of Third-Party Network Connections

Third party network connections will be monitored by the CSO and/or authorized designees. Automated tools will be used wherever possible to accomplish the auditing tasks. Monthly reports should be generated showing the specific login entries and the appropriate contact information. Associated managers will receive a copy of the monthly reports showing all of the accounts pertaining to their respective area. Copies of the reports will also be mailed to the Department

Nightly audits will be performed on all City-owned/-maintained third party router/network device configurations and the output will be mailed to the appropriate CSO designees. Any unauthorized changes will be investigated immediately.

10.5. Cloud Solutions

Cloud-based Software as a Service (SaaS) solutions are applications hosted by cloud service providers (CSP) delivered to customers via the internet. SaaS solutions may be utilized to provide services to the City of Charlotte as authorized by the CSO.

). Any SaaS solution used by the City must federate authentication with the City's standard cloud-based identity provider (IdP).

If a business requirement for a SaaS solution exists, the Department sponsoring the solution must initiate a review of the proposed solution with the CSO. Prior to this review, the Department must work with the CSP to verify that the solution meets the SaaS Security Requirements and fill out the [Cloud Security Questionnaire](#). This document will be the Department and CSP's primary means of documenting and communicating the factors that affect the risk associated with the use of the SaaS solution. Once the Cloud Security Questionnaire has been completed, it should be submitted to the CSO via the Cloud Security Review form on the Cherwell self-service portal. Technology Investment Process (TIP)

submissions that include a cloud component will not be approved prior to a full review of the associated Cloud Security Questionnaire.

Once the Cloud Security Questionnaire has been reviewed, it will receive one of the following designations.

APPROVED	This solution meets the security requirements of the City. You will receive an APPROVED email notification. You may move forward with TIP approval and implementation.
CONDITIONALLY APPROVED	This solution, as proposed, does not fully meet the security requirements of the City. Specific requirements must be addressed prior to implementation. These requirements will be detailed in the CONDITIONALLY APPROVED email notification. Examples of these requirements include: purchasing a different licensing tier for security features, vendor implementing SSO, and vendor conducting a penetration test. When the specific requirements are met by the vendor, you may move forward with TIP approval and implementation.
DISAPPROVED	This solution, as proposed, does not meet the security requirements of the City. There are specific security requirements that the vendor does not meet in this solution. This solution is not approved. The reasons for disapproval will be detailed in the DISAPPROVED email notification. If the solution changes in the future and meets the security requirements, you can resubmit the Cloud Security Questionnaire for review.
DISAPPROVED AND UNAUTHORIZED	This solution is not secure and/or operates in risky geo-locations. The solution is not approved and will not be reconsidered for approval in the future. You are not authorized to procure this solution.

11. Business Continuity Plan (BCP)

Scope: The City will develop a business continuity plan to ensure all plans are consistent, address information security requirements, and identify priorities for testing and maintenance.

The business continuity plan should encompass procedures in the event of:

- Equipment failure
- Human error
- Natural disaster
- Social or political unrest
- Sabotage
- Malicious attacks
- Disruption of power or application failures

A variety of techniques should be used in order to provide assurance that the plan will operate as intended. The CSO will be charged with responsibility of reviewing each of the Department's updated business plans and assisting with testing of the business continuity plan. The CSO will leverage the IT teams to ensure security and resiliency in the event of an event that could disrupt business continuity. The business continuity plan (BCP) should be regularly tested.

12.General Information Technology Security

12.1. Incident Response Related

Security-related events must be logged, and audit trails saved to approved logs. Security-related events include, but are not limited to:

- User login failures
- Failure to obtain administrator access
- Access procedure violations
- The CSO will address non-compliance waiver requests on a case-by-case basis.

12.2. Data Center Guidelines

The following guidelines for physical security of data centers should be followed whenever possible.

- Datacenters must be located above flood level, and the roof must be anchored to the walls.
- If credit card information is processed in a datacenter, cameras must be installed to monitor all entrances and exits to the datacenter. Video must be retained for 90 days.
- No windows should be located in the main area of the Datacenter, and no bathrooms or sump pumps may be located in the datacenter or in an adjoining room.
- There should be no potential access to the Datacenter from the ceiling, and the doors must be metal-cored and fire-resistant.
- Door hinges should be concealed, whenever possible, and doors must be fire-rated for a minimum of two hours.
- There must be adequate smoke detectors in place.
- Power cables and outlets should be checked routinely to avoid overload.
- All floor and ceiling penetrations (cable conduits, etc.) must be sealed.
- Fire alarms must be interlocked with fresh air supply sources (air conditioners, etc.) to prevent feeding the flames in the event of a fire.
- Procedures for dealing with fires must be clearly displayed.
- Magnetic media must be stored in locked fire safes.
- High-volume printers must be located in separate rooms.
- Onsite tape libraries must be located outside the main computer room.
- Datacenters should not be located beneath overhead water pipes.
- There must be drip trays under air conditioners.
- Datacenters must have adequate power capacity, and sufficiently powered standby generators must be in place.
- Procedures must be defined for routine battery care and maintenance.
- Voltage, amperage, frequency, and spikes must be routinely monitored.

- Temperature monitors must be in place.
- Cables should be laid neatly in conduit or cable trays.
- Maximum use should be made of fiber-optic lines

12.3. Secure Area Guidelines

At a minimum, these shall include:

- Restricting access to areas where sensitive information is processed or stored;
- Establishing appropriate entry authentication controls (e.g., access card and PIN numbers)
- Logging of the date and time of entry and departure of visitors;
- Supervision of all visitors in secure areas;
- Restricting visitor access to specific, authorized purposes;
- Providing all visitors with instructions and security requirements and emergency procedures;
- Requiring the visible display of identification badges for all authorized personnel and visitors;
- Notification procedures in the event unauthorized personnel are identified within a secure area;
- Regularly reviewing of access rights;
- Limiting the storage of bulk supplies or hazardous materials within secure areas;
- Appropriately placing health and safety systems within secure areas; and,
- Mandating compliance with appropriate health, safety, and security codes and regulations.

12.4. Virtual Private Networks (VPN)

The establishment of Virtual Private Network (VPN) sessions over the Internet or the addition of clients or server networks to an existing VPN requires written/digital approval. A review of the security procedures in use on each client system or server at each site to be connected to the VPN must be performed before operation will be authorized by the CSO.

Approved City employees, contractors, and authorized third parties may utilize the benefits of VPNs, which are considered a "user managed" service. A "user managed" service indicates that the user is responsible for selecting an Internet Service Provider (ISP), coordinating installation, installing any required software, and paying associated fees. It is the responsibility of employees with VPN privileges to ensure that unauthorized users are prohibited access to City internal networks.

12.4.1. Client Virtual Private Network Access

Authorized City employees and third parties may use remote connections to gain access to the City network through a virtual private network (VPN). Personnel granted remote access privileges must remain constantly aware that remote connections between their location and the City are literal extensions of the City's network, and that they provide a potential path to the City's most sensitive information. Individuals using VPN connections must take every reasonable measure to protect the City's information assets.

Personnel with VPN privileges are responsible for ensuring that unauthorized users are not allowed access to any device connected to the City network via VPN. I&T is responsible to the CSO for maintaining procedures for VPN access that ensure the following minimum standards are met:

- Only CSO-approved VPN clients may be used.
- All VPN users must be enrolled in Multi factor authentication. Multifactor authentication is required for remote access into the City's network.
- When actively connected to the production network, VPNs will force all traffic to and from the computer over the VPN tunnel; all other traffic will be dropped.
- A VPN account with no activity for a period of six months will expire and no longer function. The user must follow the standard procedure for requesting a new VPN account.
- All computers connected to internal networks via VPN or any other technology must use the most up-to-date endpoint protection (antivirus) software in accordance with the Endpoint Protection Procedure.
- Customer information, particularly cardholder data that is transmitted over wireless or open networks must be encrypted.
- Dual (split) tunneling is NOT permitted; only one network connection is allowed. All traffic including internet must be routed through the VPN tunnel.
- VPN gateways will be set up and managed by the Information Security team.
- Pings or other artificial network processes are not to be used to keep the connection open.
- The VPN concentrator is limited to an absolute connection time of 144 hours.
- Users of computers that are not City-owned equipment must use the Web VPN portal.
- Placing VPN capability on the firewall and the remote gateway protects information from disclosure between the gateways.

12.4.2. Intranet

For any City systems hosting critical applications or providing access to protected and confidential information, firewalls must be used to provide strong access control and support for auditing and logging. These controls must be used to segment the Intranet to support the access procedures developed by the designated owners of information.

Intranet servers are for serving internal City information to City of Charlotte Departments only. City of Charlotte sponsored internal information services that are subject to restrictions by City code or State or Federal law will not be hosted on any Intranet server unless the system access controls and physical security features as prescribed by this procedure are implemented. If the hosted information will traverse any public network, it must be encrypted. IT prescribes the procedures for Intranet servers and information services. All information posted on the Intranet must be properly coordinated and approved prior to posting.

12.4.3. Internet Procedure

All users who require access to the Internet through City of Charlotte computer and network resources must do so by using City-provided Internet Service Provider applications, Internet Gateway(s), and Firewall(s). All other forms of Internet access, (i.e., client or server modems) while connected to the City of Charlotte City computer, network, and telecommunications infrastructure are prohibited.

All inbound/outbound Internet services must be processed by a firewall. If a new service is requested, that service will not be made available until approved by the CSO.

Users' service requirements should be classified in a way that identifies their criticality to the business and documented in contracts or service level agreements.

12.5. Commonly Used Applications

Commonly used applications should be made available on a centralized City server. Individuals who require access to an application that is not currently available must contact the CSO. The CSO is responsible for establishing a process to test and approve access to the application.

12.6. External Sharing of Information

The City of Charlotte will establish a procedure to ensure that the exchange of information (data, software, or hardware) with external entities is secure. Information exchange may occur through the use of a number of different types of communication facilities, including electronic mail, voice, facsimile, and video. The City of Charlotte employees and contractors will follow the outlined procedures and use the appropriate controls for the formal exchange of information.

12.6.1. Guidelines

The following guidelines are for all City employees, contractors and other users to abide by:

- All information exchange facilities should comply with relevant legal requirements.
- City personnel should not have confidential conversations in public places or open offices and meeting places with non-sound proofed walls.
- Employees, contractors and other users must not compromise the organization through defamation, harassment, impersonation, or unauthorized purchases.
- In order to protect the confidentiality, integrity, and availability of information, all employees, contractors and other users must employ cryptographic techniques when appropriate.
- Procedures must be designed to protect exchanged information from interception, copying, modification, misrouting, and destruction.
- Procedures must be in place to detect and protect against malicious code that may be transmitted through the use of electronic communications.
- Procedures must be in place for protecting communicated sensitive electronic information that is in the form of an attachment.
- Retention and disposal guidelines must be adhered to for all business correspondence, including messages, in accordance with relevant national and local legislation and regulations.
- All City employees, contractors, and other users should be reminded not to register personal demographic data, such as e-mail address or other personally identifiable information, in any software to avoid collection for unauthorized use.

12.7. Email Security

12.7.1. Email System Security Guidelines

The following guidelines are for email system administrators:

- Auto-forwards to external accounts are prohibited.
- Automatic Replies will be restricted to internal addresses only.
- Exchange will be configured to not return a Non-Deliverable Receipt to external senders.
- All incoming external emails will be appended to include “[EXT]” in the header and add the below message to the email body:
 - EXTERNAL EMAIL: This email originated from the Internet. Do not click any images, links or open any attachments unless you recognize and trust the sender and know the content is safe. Please click the Phish Alert button to forward the email to bad.mail@ci.charlotte.nc.us

12.7.2. SMTP Relay

Simple Mail Transfer Protocol (SMTP) relay allows City of Charlotte users to programmatically send mail from their applications to their target users without having to run their own email server. Common uses range from servers that may generate high volumes of mail to low volume printers, scanners and multifunction devices. This can be used to send mail to both City and non-City email addresses. This service is insulated from spammers by maintaining a table of IP addresses allowed to relay.

Transport of email through City of Charlotte’s infrastructure via unauthenticated SMTP relay shall be prohibited to non-City email addresses. Transport of email via unauthenticated SMTP relay to City of Charlotte email addresses shall be allowed as requested.

A SMTP relay shall be audited on a recurring basis, at least once annually, to ensure decommissioned PCs, servers, printers, multifunction devices, etc., have been removed from the table of allowed unauthenticated sources.

12.7.3. Email Encryption

Any email containing sensitive data should be encrypted using the method described in [Sending & Receiving Encrypted Emails with Office 365](#). Office 365 can be used to encrypt emails to both internal employees, and external email addresses. It is discouraged to send PII in email, even when encryption has been used. Departments are encouraged to use alternative approved methods of sharing PII data.

Sensitive data may include:

- First time or temporary passwords
- Information not subject to public record
- Diagrams or information about City infrastructure
- PII only when no other approved option exists

For more information on sensitive data please refer to City Procedure, Protection of Restricted Data (ADM 13).

12.8. Virtual Machines on the Workstation

Virtual machines allow City of Charlotte users to host secondary operating systems on their workstation in a convenient way. Virtual machines may be used for software development and application testing. The following guidelines must be followed when deploying virtual machines on a workstation.

- Virtual machines that communicate over the network (internet access, file shares, etc) must be in bridged mode. NAT mode is not allowed. Due to port security in place it is likely that when you create your first virtual machines you will need to submit a security policy exception request to allow for additional MAC's on your network port.
- All virtual machines should be on the City's Active Directory domain and utilize the standard endpoint protection.
- Virtual machines on workstations should not host network services on the enterprise network (web servers, databases, DHCP, etc.).
- If you have a need to host server services (i.e. IIS, SQL, etc.) for testing within a virtual machine, then those services must be configured to listen on localhost or a host-only network. For example, you may run a web server on 127.0.0.1 for development purposes.

12.9. Active Directory

Active Directory (AD) allows the City of Charlotte to store User and Computer account objects. These account objects are utilized to allow authentication and control access in a networked domain environment.

12.9.1. Computer Account Object

Computer Account Objects are created in AD once the Computer is joined to a domain in the Forest. Unused computer account objects should be deleted from AD to avoid inaccurate reporting, group policy slowness, software patching issues, and syncing.

- Computer Account Objects will be disabled in AD after 90 days of inactivity.
- Computer Account Objects will be deleted from AD after 180 days of inactivity.

12.10. Network Printers

This Standard describes the baseline technical security standards required for Networked Printers connected to the City network.

Definitions

Networked Printer – Networked Printers include, but are not limited to: printers, multi-function devices (MFDs), copiers, scanners, or similar devices.

12.10.1. Networked Printer Security Requirements

This Standard applies to all Networked Printers connected to the City network, whether or not they are acquired and managed at the department level.

Update firmware with related critical security fixes within 90 days of vendor release date.

Many Networked Printers have embedded firmware that is exploitable out of the box. Note: some models (e.g. HP) have separate network interface card (NIC) firmware and print functionality (e.g. PostScript) firmware. In these cases, security fixes for both should be updated.

Enable encryption of internal storage device (hard drive) where supported.

Many Networked Printers with hard drives have full disk encryption features. In these cases, encryption should be enabled to prevent unauthorized access to data on the hard drives. If a Networked Printer does not support encryption, disable caching and refrain from using the device to print, scan, or email Restricted Data, as defined in the Protection of Restricted Data policy (ADM 13).

Set Passwords.

Quite often, each management interface has a separate password. Make sure that each management interface has a password set, even those that are disabled, because the next firmware upgrade may re-enable them. Additionally, if a management interface or other printer function comes with a default password, that should be changed to a unique password.

Disable unused management interfaces.

Networked Printers may support a number of different configuration options including built-in web servers, file transfer protocol (FTP), telnet, and simple network management protocol (SNMP). Typically, the built-in web server is used for management. The following options must be disabled and modified as indicated:

- FTP must be disabled when not in use.
- Telnet must be disabled
- SNMP, both the public and private “community strings” must be changed from the vendor default values.

Manage Networked Printers using secure protocols.

Transaction layer security (TLS) or equivalent protocols must be used for securely connecting to and managing Networked Printers over the network.

Disable unused printing interfaces.

Networked Printers may support many different protocols for sending print jobs to them. The most secure printing protocol supported by client machines must be used. The following protocols must be configured as shown below:

- Disable IPX/SPX
- Disable Appletalk
- Disable DLC/LLC
- Disable RHPP
- Disable web printing because it may allow firmware uploads
- Disable SMBv1
 - Set the Client auth level to NTLMv2

Disable the following network discovery protocols:

- Disable Bonjour
- Disable WSD
- Disable NBT

- Disable SSDP

Configure a Networked Printer's email service properly or disable it altogether.

If the device is able to send or receive email, configure the email service properly to prevent denial of service (DOS) attacks to the mail system and unauthorized access to data stored, processed or transmitted by the Networked Printer. Example scenarios may include, but not be limited to:

- Notifications to technicians about supply levels
- Copies of printed and/or scanned documents

13.Key Terms and Definitions

Term	Definition
Authentication	The process of determining the identity of a user, process, or entity attempting to access a system (e.g., password, PIN, or token).
Component Failure	Failure due to design flaws or hardware/software faults that can lead to denial of service or security compromises through the malfunction of a system component.
Computer Virus Attacks	Attacks using viral code that reproduces itself by modifying other programs, spreading across multiple programs, data files, or devices on a system or through multiple systems in a network that may result in the destruction of data or the erosion of system performance.
Computing Devices	For purposes of this procedure, “computing device” means a device, usually programmable, that can store, retrieve, and process data. Computing devices can include, but are not limited to, desktops, laptops, mainframes, routers, PDAs, tablet computers, multifunction printers and smartphones.
Department	The individual Departments within the City.
DMZ	De-militarized Zone. A network segment isolated from the corporate production network.
Encryption	The transformation of data into an unreadable form that can only be deciphered with a secret key.
Endpoint Protection Software	Software designed to detect, identify, defend against, and, in some cases, rid viruses from a system.
Firewall	A computerized barrier placed between two or more network segments used to restrict or closely scrutinize network traffic.
Fraud	Attempts to masquerade as a legitimate user to steal services or information, or to initiate transactions that result in financial loss or embarrassment to the organization.
FTPS – File Transfer Protocol Secure	An extension to the commonly used File Transfer Protocol (FTP) that adds support for the Transport Layer Security (TLS) cryptographic protocols
HTTPS - Hypertext Transfer Protocol Secure	HTTPS creates a secure channel over an insecure network. This ensures reasonable protection from eavesdroppers and man-in-the-middle attacks,

	provided that adequate cipher suites are used and that the server certificate is verified and trusted.
Information Browsing	Unauthorized viewing of sensitive information by intruders or legitimate users.
Information Integrity	Unauthorized deletion, modification, or disclosure of information.
IMAPS - Internet Message Access Protocol Secure	Internet protocol that allows an e-mail client to access e-mail on a remote mail server. IMAP over TLS (IMAPS) is assigned port number 993.
Internet Protocol address (IP address)	A numerical label assigned to each device (e.g., computer, printer, multifunction device) participating in a computer network
Jailbreaking	Jailbreaking your device means installing a small program that removes restrictions in the default software. A jailbroken device can run apps and extensions (themes and tweaks) not approved by Apple.
Malicious Code	General term referring to worms, viruses, or other programs designed to be destructive, to compromise security, or to impede normal operations. Malicious code can be delivered via multiple channels such as email, spam, unsolicited commercial bulk email, and media.
Misuse	The use of information assets by either internal or external users for other than authorized purposes.
Penetration attack	Attacks by unauthorized persons or systems that may result in denial of service or significant increases in incident handling costs.
PIN (Personal Identification Number)	A number used as a password by a computer user.
Rooting	Rooting is the process of allowing users of smartphones, Tablet and other devices running the Android mobile operating system to attain privileged control within Android's sub-system.
Sanitized Data	Information that has been obscured or altered in such a way as to prevent unauthorized use or disclosure.

Security	The ability to protect the integrity, availability, and confidentiality of information held by the City and to protect information technology assets from unauthorized use or modification and from accidental or intentional damage or destruction.
Server	A computer that provides services to other computers over a network. For example, a computer housing files accessed by multiple users from multiple locations over a network is referred to as a file server. In other words, a Server is defined as an internal City Server. Desktop machines and Lab equipment are not relevant to the scope of this procedure.
SMTP (Simple Mail Transfer Protocol)	An Internet standard for email transmission.
Token	A small device containing an embedded microprocessor that stores information for authentication to a server or system. Unique data specific to that user is imbedded in the token.
Unauthorized Alteration	Additions and/or changes to infrastructure components that are not authorized.
Virus	A program that can “infect” another software program by modifying it to include a copy of itself. A program need not cause malicious damage to be a virus; the act of “infecting” other programs is central to the definition.
Worm	A program that spreads copies of itself throughout a network. A worm typically becomes a security problem when it spreads and disrupts the network by overloading it.

Appendix A PCI Compliance

The following is a list of procedures for applicable departments. The PCI DSS Requirements outlined in Appendix A are to be applied in addition to the requirements stated in the main body of this security manual. In cases of overlapping standards, the standard that offers the most protection for the network and Card Data Environment (CDE) should be applied.

Requirement 1: Firewall and Router Configuration Standards

The City must maintain a formal process for approving and testing all network connections, and changes to the firewall and router configuration must be in place for every change made to systems within the scope of the cardholder data environment (CDE). The CSO is charged with the following tasks:

- Managing the City's logical network.
- Performing a formal review of all City firewall and router configurations at least every six months.
- Network connections and router configurations must be approved and tested. All connections must be diagrammed, and the diagram should be verified quarterly.
- Personal firewall software is required on all portable devices that connect to the Internet when outside the Charlotte network.
-
- Inbound and outbound traffic must be restricted to only traffic necessary for the CDE. All other traffic must be denied. Unauthorized outbound traffic from the CDE to the Internet is prohibited.
- Audits of City information systems must be done to ensure compliance with information security procedures and best practices.
- Approved VLAN must be used for systems that are part of the CDE. The VLAN will be agreed upon by the requesting department and the [change management process](#).
- Configuration files are secured from unauthorized access and kept consistent with active network configurations.
- Anti-spoofing measures must be implemented to detect and block forged source IP addresses from entering the trusted network

Changes to the configuration of firewalls, routers, servers, or workstations in the CDE must be documented to include the following:

- The impact of the change, so all affected parties will be able to plan appropriately for any processing changes.
- All authorized parties must approve the change.
- Functionality testing must be performed and documented to verify the change does not adversely impact the security of the system.
- Back out procedures must be well documented to restore the system to its previous state in the event the change is unsuccessful.

Upon completion of a significant change, all relevant PCI DSS requirements must be implemented on the new or changed systems and networks and documented accordingly.

Requirement 2: Managing Vendor Defaults and Other Security Standards

- All vendor-supplied defaults (passwords, encryption keys, etc) must be changed and all unnecessary default accounts must be removed or disabled before a system can be installed on the network.
- For wireless environments connected to the CDE or transmitting cardholder data, wireless vendor defaults must be changed at installation, including default wireless encryption keys, passwords, and SNMP community strings.
- Systems should be configured with industry accepted hardening in mind. Systems should only run the processes necessary for that system.
- To prevent functions that require different security levels from co-existing on the same server, only one primary function per server will be implemented.
- Only necessary services, protocols and daemons required for the functionality of the system will be enabled. All unnecessary system functionality will be disabled.
- Where insecure services, daemons or protocols are required, additional security must be implemented and documented. Business justification must be documented.
- Security policies and daily operational procedures for managing vendor defaults and other security parameters must be documented, in use and known to all involved.
- System security parameters must be set appropriately and configured in such a way that they address security settings and parameters that have known security implications for each type of system in use.
- All non-console administrative access must be encrypted using strong cryptography.

Requirement 3: Protecting Stored Cardholder Data

- Cardholder data retention is limited to that required for legal, regulatory, and/or business requirements. On a quarterly basis stored data not deleted during the retention period will be identified and remediated.
- Secret and private cryptographic keys used to encrypt/decrypt data must be in accordance with the latest PCI DSS standards.
- Cardholder data retention is limited to that required for legal, regulatory, and/or business requirements. On a quarterly basis stored data not deleted during the retention period will be identified and remediated.
- Secret and private cryptographic keys used to encrypt/decrypt data must be in accordance with the latest PCI DSS standards.
- Sensitive authentication data must not be retained after authorization, even if encrypted. All sensitive authentication data received must be rendered unrecoverable upon completion of the authorization process
- The card verification code cannot be retained upon completion of the authorization process.
- The City of Charlotte will ensure media is destroyed when it is no longer needed for business or legal reasons as follows:
 - Hardcopy Materials will be cross-cut shredded, incinerated, or pulped so that cardholder data cannot be reconstructed. Storage containers used for information to be destroyed

will be secured. For example, verify "to-be-shredded" containers have locks preventing access to the contents. It is the responsibility of the CSO to ensure documents are securely disposed of and are not thrown in the trash or put in recycling bins.

- **Electronic Media:** The CSO will render cardholder data stored on electronic media unrecoverable so the data cannot be reconstructed. Removable media must be stored in a secure location until it has been destroyed. It is the responsibility of CSO to ensure secure disposal is implemented and effective.
- **On-Line Electronic Data:** Once stored data exceeds the retention period, the CSO will ensure it is deleted via an automated process. Electronically stored cardholder data must be deleted by a certified application or a management-approved secure deletion process that deletes data beyond recovery.
- **Back-Up/Removable Media:** The CSO will ensure cardholder data is destroyed beyond recovery by using a wipe program to delete files.
- The CSO will verify the sanitation process renders data unrecoverable in accordance with industry-accepted standards for secure deletion or otherwise physically destroying the media.

Requirement 4: Encryption of Transmissions of Cardholder Data

- Industry best practices will be used to implement strong cryptography and security protocols for data transmitted over any wireless network. • Industry best practices will be used to implement strong cryptography and security protocols for data transmitted over any wireless network.
- The City will maintain strong cryptography and security protocols (e.g., SSL/TLS, IPSEC, SSH, etc.) to safeguard sensitive cardholder data anywhere such data is stored, received or transmitted over open, public networks.
- Unprotected PANs (Primary Account Numbers) will never be sent by end-user messaging technologies (e.g., e-mail, instant messaging, chat, etc.). If the PAN must be sent, the City will ensure the PAN has been rendered unreadable or secured with strong cryptography.

Cryptographic Keys Protection and Management

The City of Charlotte will protect keys used for encryption of cardholder data by, 1) securely storing encryption keys in the fewest possible locations and forms and 2) limiting access to the fewest number of custodians possible. Keys are to be stored in encrypted format, and key-encryption keys must be stored separately from data-encryption keys. The CSO will implement and document all key-management processes and procedures for the cryptographic keys.

Any cryptographic key solution used in the CDE must meet the following requirements:

- Generate strong keys.
- Distribute keys securely, meaning keys are not distributed in the clear and are only distributed to the proper custodians.
- Store keys securely, meaning keys are not stored in the clear. They must be encrypted with a key-encryption key.
- Cryptographic keys must be changed when they reach the end of their cryptoperiod (as defined by the associated application vendor or key owner and based on industry best practices).
- When the integrity of a key has been weakened or when keys are suspected of being compromised, a defined process must exist to retire and replace those keys.

- If manual clear-text cryptographic key management operations are used, these operations must be managed using split knowledge and dual control of keys.
- The encryption solution must not allow for or accept substitution of keys coming from unauthorized sources or unexpected processes.
- Cryptographic key custodians must formally acknowledge they understand and accept their key-custodian responsibilities, and this must be formally documented.
- Encryption protocols that use only secure configurations and do not support insecure versions or configurations will be used.

Authentication/Access Management

- Multi factor authentication is required to secure all individual non-console administrative access and for all remote access to the cardholder environment.
- Access to databases containing cardholder data is restricted. Direct user access or queries to databases must be restricted to database administrators. Where authentication mechanisms such as physical or logical tokens, smart cards, certificates etc. are used, these mechanisms must be assigned to an individual account and not shared and must be secured enough to ensure only the intended account can use that mechanism to gain access.
- The City must ensure proper user identification and authentication management for users and administrators of CDE systems. To ensure user additions, revocations, and modifications are performed in a secure manner, all additions, deletions, and modifications of user IDs and passwords will be managed and controlled by the I&T under the authority of the CIO.
 - Devices that capture payment card data via direct physical interaction with the card must be protected from tampering and substitution.
 - Each department must maintain a list of all devices and personnel authorized to use the devices. This list should include the make and model of each device, the location of the device and the device serial number or other method of unique identification.
 - I&T must verify user identity before performing password resets or modifications to any user account.
 - Device surfaces must be periodically inspected to detect tampering or substitution by checking the serial number or other device characteristics to verify it has not been swapped with a fraudulent device.
 - The CSO must provide training for personnel to be aware of attempted tampering or replacement of devices. This training should include:
 - Verifying the identity of any third-party persons claiming to be repair or maintenance personnel, prior to granting them access to modify or troubleshoot devices.
 - Devices should not be installed, replace or returned without verification.
 - Awareness of suspicious behavior.
 - Reporting suspicious behavior and indications of device tampering or substitution to appropriate personnel.
- All access control systems must automatically disable any user accounts inactive for 90 days or more. In the event this is not feasible, the Data Center Services must perform a quarterly audit to

disable user accounts that have been inactive for 90 days or more. Data Center Services will maintain a record of the quarterly system audits.

- Cryptography must be strong enough to render all authentication credentials unreadable during storage and transmission.
- IDs used by third parties to remotely access, support or maintain system components will be enabled only during the time period it is needed, monitored while it is in use and disabled when it is not being used.

Requirement 5: Protecting Systems Against Malware

- Endpoint protection software, such as Antivirus, that can detect and remove malicious software will be deployed on all systems commonly affected by malicious software (particularly personal computers and servers) and will remain actively running. The Antivirus program(s) must be capable of detecting, removing, and protecting against all known types of malicious software, including viruses, Trojans, worms, spyware, adware, and rootkits.
- For systems not commonly affected by malicious software, periodic evaluations must be performed to identify and evaluate evolving malware threats in order to confirm that such systems continue to not require anti-virus software.
- The Antivirus software must be configured to automatically update the software and definitions, and it must perform periodic scans of the entire system. The CSO must ensure all Antivirus mechanisms are current and perform periodic scans and active or real-time scans. OR performing continuous behavioral analysis of systems or processes and always generating audit logs.
- The Antivirus software must be able to monitor for removable electronic media and perform automatic scans of when the media is inserted, connected, or logically mounted. Performs continuous behavioral analysis of systems or processes when the media is inserted, connected, or logically mounted.
- Audit logs provide the ability to monitor virus activity and Antivirus reactions. Thus, it is imperative to configure the Antivirus software to generate audit logs and to manage these logs in accordance with PCI DSS Requirement 10.7. Any exceptions to this policy must be approved by the CSO.
- The CSO must ensure Antivirus mechanisms are actively running and cannot be disabled or altered by users, unless specifically authorized by the CSO on a case-by-case basis and for a limited time period.
- Antivirus solutions may be temporarily disabled only if there is legitimate technical need, as authorized by the CSO on a case-by-case basis. Additional security measures may also need to be implemented for the period of time during which Antivirus protection is not active.

Requirement 6: Developing and Maintaining Secure Systems and Applications

- Reputable outside sources will be used to stay up to date with the latest vulnerability information and systems will be installed with the latest security patches.
- Software development procedures will be based on industry best practices including code reviews, coding techniques, change control processes, separation of duties, and environments.

Requirement 7: Restricting Access to Cardholder Data

All system components within the cardholder environment must use an automated access control system based on a user's need to know and must be configured to support the following:

- Group definitions based on job classifications and function must be used to establish privileges by user class; however, each user must have a unique user name and password. Group, shared, or generic accounts or passwords are not allowed.
- All access control systems must enforce a default “deny-all” setting.
- All users must be assigned a unique ID before being allowed access to system components or to the CDE.
- In addition to assigning a unique ID, users will be identified using one of the following methods:
 - A password
 - A token device or smart card
 - A biometric (e.g. fingerprint, retina scan)
- Access to system components and cardholder data must be limited to only those individuals whose job requires such access. Assignment of privileges is based on individual's job classification and function (role-based access control [RBAC]) and must be applied to all users with access to the CDE. Limiting access to those with a legitimate business reason for the access helps to prevent mishandling of cardholder data.
- However, in order to limit access to CHD to those individuals who need such access, it is first necessary to define access needs for each role, the systems/devices/data each role needs access to, and the level of privilege each role needs to effectively perform assigned tasks. Once roles and corresponding access needs are defined, individuals can be granted access accordingly. The CSO will ensure user access rights are defined by role, and access to privileged user IDs are restricted to the least privilege necessary to perform job responsibilities.
- There must be documented approval by authorized parties, in writing or electronically, for all access to the CDE. This documentation must specify the required minimum privileges necessary to complete the user's job function. All technology use must be authenticated with a unique user ID and password or other authentication item (e.g., a token, smart card, biometric) for each user.
- Vendors with remote access into systems will only be provided access when needed, and access will immediately be terminated after use.
- All access by application and System accounts and related access privileges must be reviewed periodically at least every 6 months. The review must identify if the applications and system access remain appropriate for the function being performed.
- During review if any inappropriate access is identified it must be addressed immediately. After the review Management acknowledges that access remains appropriate.

Requirement 8: Identification and Authentication

- All users accessing PCI systems or cardholder data will be assigned a unique ID and will be required to follow the mentioned password requirements. Users will be locked out for 30 minutes or until reactivation after 6 unsuccessful login attempts. Idle session of more than 15 minutes will require re-authentication to re-activate terminal session. Inactive accounts will be removed or disabled within 90 days.

- All passwords must be a minimum length of 12 characters (or IF the system does not support 12 characters, a minimum length of eight characters). Contain both numeric and alphabetic characters. Individuals are not allowed to submit a new password/passphrase that is the same as any of the last four passwords/passphrases used.
- Multi-factor authentication is to be incorporated for all non-console access into the CDE environment with admin privileges and for all remote network access regardless of privileges.
- Passwords and authentication mechanisms are to be assigned to one individual account and no shared accounts are allowed.

Requirement 9: Restricting Physical Access to Cardholder Data

- Physical access to sensitive areas will be monitored and reviewed with video cameras or access control mechanisms. The data collected will be stored for at least three months unless otherwise restricted by law.
- Physical access to sensitive areas within the CDE is controlled through access based on individual job function. Access and all mechanisms such as keys, access cards are returned and revoked immediately upon termination.
- Physical access to publicly accessible network jacks, wireless access points, handheld devices, and network/communication hardware is to be restricted.
- Onsite personnel and visitors should be easily distinguishable from one another. Visitors with access to cardholder data processing or storage are to be authorized and escorted at all times. A visitor log will be maintained for at least three months. Visitor badges are to be surrendered or deactivated before visitor leaves the facility or at the date of the expiration.
- All media is to be physically secured and classified. Management approval is required before moving media via a secure delivery method. When no longer needed, media is to be destroyed in a manner such that no physical or digital information is recoverable or reconstructable.
- Devices that capture payment card data via direct physical interaction will be protected from tampering by being periodically inspected. A list of devices is also to be maintained and kept up to date.
- All personnel at point-of-sale locations are to be trained for awareness of tampering or replacement attempts. Any Suspicion of temperingtampering must be reported to immediate supervisor.

Track and Monitor Access to Network Resources and Cardholder Data

- Critical system clocks will use a time synchronization technology and receive time only from designated central time servers. The central time servers will keep accurate time with each other if more than one is used and will only receive time signals from external sources
- The following will be reviewed daily: security events, all system logs, and all system component logs. This can be a manual or automated process. Anomalies will be investigated per the incident response procedures. Audit logs will be maintained for at least one year and immediately available for a minimum of three months.

Requirement 10 and 11: Security Monitoring and Testing

Secure Audit Trails

Audit trails must be secure such that they cannot be altered.

The City of Charlotte must ensure the following practices are followed:

1. Audit trails will be accessible only to those whose job function requires such accessibility.
2. Protect audit trail files from unauthorized modification.
3. Backup audit trail files to a centralized log server or to media that is difficult to alter.
4. Write logs for external-facing technologies to a secure, centralized internal log server or media device.
5. Use file-integrity monitoring (FIM) or change-detection software on logs to ensure existing log data cannot be changed without generating alerts (although new data being added should not cause an alert).

File-integrity-monitoring systems check for changes to critical files and notify personnel when such changes are noted. File-integrity monitoring software must be configured to run at least weekly and should send alerts when any unauthorized modifications are made to critical system files, or configuration or content files.

For log files that change frequently, monitor items such as log file deletion, file sizes that suddenly grow or shrink significantly, or any other indicators that a malicious individual has tampered with the log file.

Daily Log Review

Checking logs daily minimizes the time and exposure of a potential breach. The log-review process does not have to be manual; log harvesting, parsing, and alerting tools can be used. The CSO, their designee or an approved monitoring tool will perform a daily review of logs and security events for all system components that store, process, or transmit CHD.

Daily log reviews must include all security events, all critical system components, all system components that store, process, or transmit CHD, and all servers and system components that perform security functions such as intrusion-detection systems (IDS) and authentication, authorization, and accounting protocol (AAA) servers (e.g., RADIUS).

Log reviews of other system components should be performed periodically based on The City's policies and risk management strategy. Exceptions and anomalies identified during the review process should be investigated and addressed. If exceptions and anomalies are not investigated, The City may be unaware of unauthorized and potentially malicious activities that are occurring within the network.

Vulnerability Assessments

Vulnerability scans will be performed on the internal and external network. These scans will be performed quarterly and after any significant change in the network (including new system component installations, changes to network topology, firewall rule modifications, or product upgrades). For PCI compliance, four passing quarterly scans must occur each year. A passing scan indicates no "High" vulnerabilities are present within the CDE's network. High risk vulnerabilities must be mitigated within 30 days and rescans must be performed to verify resolution. A vulnerability report will be produced detailing the results of assessments.

Vulnerability Risk Rankings

Risk rankings should be based on industry best practices. It is imperative that the City maintain a process for identifying security vulnerabilities and assigning risk rankings to aid in mitigating risks and resolving vulnerabilities.

The purpose of establishing risk rankings is to define the process used to rank vulnerabilities detected during quarterly internal vulnerability scans to meet the following Payment Card Industry Data Security Standard (PCI DSS) requirements as follows:

Run internal and external network vulnerability scans at least quarterly and after any significant change in the network.

Address vulnerabilities and perform rescans to verify all “high” vulnerabilities (as defined in this document), have been resolved according to the resolution timeline below. Vulnerability scans must be performed by a qualified internal resource or a qualified external third party.

Maintain a process that identifies and assigns a risk ranking to newly discovered security vulnerabilities.

Conduct internal vulnerability scans for all systems determined to be in scope for PCI DSS compliance, referred to as the CDE.

Once an internal vulnerability scan has been conducted, the CSO will identify vulnerabilities to the CDE.

All vulnerabilities and misconfigurations must be assigned a severity level. The designation of each severity level must allow an easy comparison between the levels. Common tools used to categorize and rank vulnerabilities and determine scan compliance are as follows:

The Common Vulnerability Scoring System (CVSS) version 3.1 Base Scoreⁱ

The National Vulnerability Database (NVD).ⁱⁱ

The risk a vulnerability poses must be evaluated and ranked according to the following criteria:

Severity Level	Description	Time to Resolve
High	CVSS Base Score of 7.0 – 10.0	30 days or less
Medium	CVSS Base Score of 4.0 – 6.9	31-60 days
Low	CVSS Base Score of 0.0 – 3.9	TBD

Vulnerability severity levels may be adjusted, based upon the risk each poses to the organization, but each must be documented and approved by the CSO.

Once weaknesses are identified, the CSO will correct the high-severity items and repeat the scan to verify that all high-severity vulnerabilities have been corrected.

Classifying the risks (for example, as “high,” “medium,” or “low”) will allow the City to identify and address high-priority risk items more quickly and reduce the likelihood that vulnerabilities posing the greatest risk will be exploited.

Internal vulnerability scans must be performed by a qualified internal resource or a qualified external third party. Organizational independence of the tester must exist (e.g., a firewall administrator cannot be responsible for scanning the firewall).

For external vulnerability scans, an Approved Scanning Vendor (ASV) approved by the Payment Card Industry Security Standards Council (PCI SSC) must perform quarterly external vulnerability scans of the City’s CDE.

Penetration Testing

Internal and external penetration testing will be conducted at least annually and after any infrastructure or application upgrade or modification. The determination of what constitutes a significant upgrade or modification is highly dependent on the configuration of a given environment. If an upgrade or modification could allow access to cardholder data or affect the security of the CDE, then it could be considered significant. Findings will be reviewed and corrected. Testing will be repeated to verify corrections.

The penetration testing methodology must:

- Be based on industry-accepted penetration testing approaches (for example, NIST SP 800-115).
- Include coverage for the entire CDE perimeter and critical systems.
- Include testing from both inside and outside the network.
- Include testing to validate any segmentation and scope-reduction controls.
- Define application-layer penetration tests that include, at a minimum, vulnerabilities outlined according to PCI Requirements 6.5.1 – 6.5.10.
- Define network-layer penetration tests to include components supporting network functions and operating systems.
- Include review and consideration of threats and vulnerabilities experienced in the last 12 months.
- Specify retention of penetration testing results and remediation activity results.
- Penetration testing activities must cover all in-scope environments, including those hosted or managed by service providers.

Requirement 12: Information Security for All Personnel

- A risk assessment will be conducted annually and after significant changes in the environment. The assessment will identify critical assets, threats and vulnerabilities. The process will be conducted by the CSO with a resulting formal analysis document
- Authorized parties will be allowed to use only company approved critical technologies. A list of technologies and their locations/users should be kept. Using remote technology to copy, move, or store locally card holder data is prohibited unless authorized for business purposes.
- Security Awareness training will be provided to employees upon hire and at least annually thereafter
- In addition to the security awareness training, those whose job responsibilities include access to PCI data and technologies are required to take PCI awareness training and will annually agree to having read and understood the Information Security Manual
- All service providers but have a written agreement outlining responsibility for the security of card holder data. A list of service providers is to be maintained and the providers will be monitored at least annually for PCI DSS compliance.

Service Providers

- The city will maintain a list of service providers which includes a description of the service they provide as well as the PCI DSS requirements they manage and those managed by the City. The

list will be maintained by the CSO, and the providers will be monitored at least annually for PCI DSS compliance.

- All service providers have a written agreement outlining their responsibility for the security of card holder data they possess, store or transmit on behalf of the city.
- Service providers must be thoroughly vetted including a risk analysis prior to establishing a formal relationship. The city will perform their due diligence and maintain a set process for engaging all service provider prior to the engagement.

Appendix B CJIS Compliance

The following is a list of procedures for applicable departments. These are to be followed in congruency with the latest CJIS Security Policy. The essential premise of the CJIS Security Policy is to provide the appropriate controls to protect CJI, from creation through dissemination; whether at rest or in transit. Always refer to the latest CJIS Security Policy for the most up to date and detailed requirements.

Link to current policy: https://www.fbi.gov/file-repository/cjis_security_policy_v5-9-1_20221001.pdf/view

Policy Area 1—Information Exchange Agreements

- The requirements set here apply to all handling, processing, storing, or communication of Criminal Justice Information.

Policy Area 2—Security Awareness Training

- Basic security awareness training shall be required within six months of initial assignment, and biennially thereafter, for all personnel who have access to CJI to include all personnel who have unescorted access to a physically secure location.

Policy Area 3 – Incident Response

- To ensure protection of CJI, the city shall: establish operational incident handling procedures that include adequate preparation, detection, analysis, containment, recovery, and user response activities; track, document, and report incidents to appropriate agency officials and/or authorities.

Policy Area 4—Auditing and Accountability

- The City's information system shall generate audit records for defined events. The City's information system shall produce, at the application and/or operating system level, audit records containing sufficient information to establish what events occurred, the sources of the events, and the outcomes of the events. The list of events are as followed:
 - Successful and unsuccessful system log-on attempts.
 - Successful and unsuccessful attempts to use:
 - access permission on a user account, file, directory or other system resource;
 - create permission on a user account, file, directory or other system resource;
 - write permission on a user account, file, directory or other system resource;
 - delete permission on a user account, file, directory or other system resource;
 - change permission on a user account, file, directory or other system resource.
 - Successful and unsuccessful attempts to change account passwords.
 - Successful and unsuccessful actions by privileged accounts.
 - Successful and unsuccessful attempts for users to:
 - access the audit log file;

- modify the audit log file;
- destroy the audit log file.

Policy Area 5—Access Control

- The City shall manage information system accounts, including establishing, activating, modifying, reviewing, disabling, and removing accounts. The City shall validate information system accounts at least annually and shall document the validation process. The validation and documentation of accounts can be delegated to local agencies.
- Access control mechanisms to enable access to CJI shall be restricted by object (e.g., data set, volumes, files, records) including the ability to read, write, or delete the objects. Access controls shall be in place and operational for all IT systems to:
 - Prevent multiple concurrent active sessions for one user identification, for those applications accessing CJI, unless the City grants authority based upon operational business needs. The City shall document the parameters of the operational business needs for multiple concurrent active sessions.
 - Ensure that only authorized personnel can add, change, or remove component devices, dial-up connections, and remove or alter programs.
- A personally owned information system shall not be authorized to access, process, store or transmit CJI unless the City has established and documented the specific terms and conditions for personally owned information system usage. When personally owned mobile devices (i.e. bring your own device [BYOD]) are authorized, they shall be controlled in accordance with the requirements in CJIS Security Policy Area 13: Mobile Devices. This control does not apply to the use of personally owned information systems to access the City's information systems and information that are intended for public access (e.g., the City's public website that contains purely public information).

Policy Area 6 – Identification and Authentication

- Each person who is authorized to store, process, and/or transmit CJI shall be uniquely identified. A unique identification shall also be required for all persons who administer and maintain the system(s) that access CJI or networks leveraged for CJI transit. The unique identification can take the form of a full name, badge number, serial number, or other unique alphanumeric identifier. The City shall require users to identify themselves uniquely before the user is allowed to perform any actions on the system. Agencies shall ensure that all user IDs belong to currently authorized users. Identification data shall be kept current by adding new users and disabling and/or deleting former users.

Policy Area 7—Configuration Management

- The City shall ensure that a complete topological drawing depicting the interconnectivity of the City network, to criminal justice information, systems and services is maintained in a current status.
 - The network topological drawing shall include the following:
 - All communications paths, circuits, and other components used for the interconnection, beginning with the city-owned system(s) and traversing through all interconnected systems to the city end-point.

- The logical location of all components (e.g., firewalls, routers, switches, hubs, servers, encryption devices, and computer workstations). Individual workstations (clients) do not have to be shown; the number of clients is sufficient.
 - “For Official Use Only” (FOUO) markings.
 - The city name and date (day, month, and year) drawing was created or updated.
- The system configuration documentation often contains sensitive details (e.g. descriptions of applications, processes, procedures, data structures, authorization processes, data flow, etc.). The City shall protect the system documentation from unauthorized access consistent with the provisions described in CJIS Security Policy Section 5.5 Access Control.

Policy Area 8—Media Protection

- The City shall protect and control digital and physical media during transport outside of controlled areas and restrict the activities associated with transport of such media to authorized personnel.
- Controls shall be in place to protect digital media containing CJI while in transport (physically moved from one location to another) to help prevent compromise of the data. Encryption, as defined in CJIS Security Policy Section 5.10.1.2, is the optimal control during transport; however, if encryption of the data isn’t possible then the City shall institute physical controls to ensure the security of the data.
- The City shall sanitize, that is, overwrite at least three times or degauss digital media prior to disposal or release for reuse by unauthorized individuals. Inoperable digital media shall be destroyed (cut up, shredded, etc.). The City shall maintain written documentation of the steps taken to sanitize or destroy electronic media. The City shall ensure the sanitization or destruction is witnessed or carried out by authorized personnel.
- Physical media shall be securely disposed of when no longer required, using formal procedures. Formal procedures for the secure disposal or destruction of physical media shall minimize the risk of sensitive information compromise by unauthorized individuals. Physical media shall be destroyed by shredding or incineration. The City shall ensure the disposal or destruction is witnessed or carried out by authorized personnel.

Policy Area 9—Physical Protection

- The City shall authorize and control information system-related items entering and exiting the physically secure location.

Policy Area 10—Systems and Communications Protection and Information Integrity

- When CJI is at rest (i.e. stored digitally) outside the boundary of the physically secure location, the data shall be protected via cryptographic mechanisms (encryption).
- The metadata derived from CJI shall not be used by any cloud service provider for any purposes. The cloud service provider shall be prohibited from scanning any email or data files for the purpose of building analytics, data mining, advertising, or improving the services provided.
- CJI transmitted via a single or multi-function device over a standard telephone line is exempt from encryption requirements. CJI transmitted external to a physically secure location using a

facsimile server, application or service which implements email-like technology, shall meet the encryption requirements for CJI in transit as defined in CJIS Security Policy Section 5.10.

Policy Area 11 - Formal Audits

- Formal audits are conducted to ensure compliance with applicable statutes, regulations, and policies.
- All agencies having access to CJI shall permit an inspection team to conduct an appropriate inquiry and audit of any alleged security violations. The inspection team shall be appointed by the APB and shall include at least one representative of the CJIS Division. All results of the inquiry and audit shall be reported to the APB with appropriate recommendations

Policy Area 12—Personnel Security

- The City shall employ formal sanctions for personnel failing to comply with established information security policies and procedures

Policy Area 13—Mobile Devices

- Mobile devices accessing CJI outside the US have all controls in place prior to and after deployment outside the US
- If a Mobile Device Management application is used for devices that process, store or transmit CJI data, the following controls shall be put in place:
 - Ensure that CJI is only transferred between CJI authorized applications and storage areas of the device.
 - MDM with centralized administration configured and implemented to perform at least the:
 - Remote locking of device
 - Remote wiping of device
 - Setting and locking device configuration
 - Detection of “rooted” and “jailbroken” devices
 - Enforcement of folder or disk level encryption
 - Application of mandatory policy settings on the device
 - Detection of unauthorized configurations
 - Detection of unauthorized software or applications
 - Ability to determine the location of city-controlled devices
 - Prevention of unpatched devices from accessing CJI or CJI systems
 - Automatic device wiping after a specified number of failed access attempts
- Wireless devices at a minimum must:
 - Apply available critical patches and upgrades to the operating system as soon as they become available for the device and after necessary testing as described in Section 5.10.4.1.

- Are configured for local device authentication (see Section 5.13.7.1).
- Use advanced authentication or CSO approved compensating controls as per Section 5.13.7.2.1.
- Encrypt all CJI resident on the device.
- Erase cached information, to include authenticators (see Section 5.6.2.1) in applications, when session is terminated.
- Employ personal firewalls on full-featured operating system devices or run a Mobile Device Management (MDM) system that facilitates the ability to provide firewall services from the agency level.
- Employ malicious code protection on full-featured operating system devices or run a MDM system that facilitates the ability to provide anti-malware services from the agency level.
- Monitor mobile devices to ensure their patch and update state is current.

ⁱ First.org CVSS: Common Vulnerability Scoring System v3.1: User Guide <https://www.first.org/cvss/v3.1/user-guide>

ⁱⁱ National Vulnerability Database <http://nvd.nist.gov/>



Risk Management- Insurance Review Certification

Risk Management has reviewed the certificate(s) of insurance from Town of Huntersville for conformance with City requirements and has determined that the insurance coverages and amounts represented on the certificates of insurance meets both the City's minimum standard and the requirements set forth in contract 2024000021. This insurance is sufficient for the purposes of the purchases defined in the contract.

Comments:

No insurance included

Contract Number: 2024000021

Amendment/Change Order Number _____

Reviewer: Melanie Hopper

Signature: **Melanie Hopper** Digitally signed by Date: 7/12/23
Melanie Hopper
Date: 2023.07.13
00:07:56 -04'00'

**Town of Huntersville
Town Board
August 7, 2023**

To: Town Board

From: Jesse James, Senior Planner

Date: August 7, 2023

Subject: Call a Public Hearing for Petition #R23-08 - Dearness Gardens

EXPLAIN REQUEST:

Call a public hearing for Tuesday September 5, 2023 at 6:00 P.M. at Huntersville Town Hall, 101 Huntersville-Concord Road, Huntersville, NC, on Petition #R23-08, Dearness Gardens, a request by Ken Forster, to rezone six parcels (01707207, 01707236, 01707237, 01707238, 01707239, 01707240) totaling +/- 10.07 acres generally located at 13501 Old Statesville Road from existing Highway Commercial - Conditional District and Neighborhood Residential to Highway Commercial - Conditional District and Neighborhood Residential for boundary and site amendments.

ACTION RECOMMENDED:

Call a Public Hearing

FINANCIAL IMPLICATIONS:

None

ATTACHMENTS:

None

**Town of Huntersville
Town Board
August 7, 2023**

To: Town Board

From: Jesse James, Senior Planner

Date: August 7, 2023

Subject: Call a Public Hearing on Petition #R23-09 - Golden Cow

EXPLAIN REQUEST:

Call a public hearing for Tuesday, September 5, 2023 at 6:00 p.m. at Huntersville Town Hall, 101 Huntersville-Concord Road, Huntersville, NC, on Petition #R23-09, Golden Cow, a request by H2H Holdings, LLC to rezone from the existing Town Center to Town Center - Conditional District for a one-story retail development.

ACTION RECOMMENDED:

Call a public hearing

FINANCIAL IMPLICATIONS:

None

ATTACHMENTS:

None

**Town of Huntersville
Town Board
August 7, 2023**

To: Town Board

From: Lora Mastrofrancesco, Transportation Engineer/Project Manager

Date: August 7, 2023

Subject: Call for Public Hearing - Traffic Calming Measures on Swansboro Ln

EXPLAIN REQUEST:

Call a Public Hearing for Tuesday, September 5, 2023 at 6:00 p.m. at Huntersville Town Hall, 101 Huntersville-Concord Road, Huntersville, NC 28078 to receive public input on traffic calming measures on Swansboro Lane.

ACTION RECOMMENDED:

Approve

FINANCIAL IMPLICATIONS:

None

ATTACHMENTS:

None

**Town of Huntersville
Town Board
August 7, 2023**

To: Town Board

From: Nathan Farber, Planner I

Date: August 7, 2023

Subject: Conduct Public Hearing - Petition #R23-01, Beatties Ford Family Entertainment

EXPLAIN REQUEST:

Conduct public hearing for Petition #R23-01, Beatties Ford Family Entertainment, a request by Jonathan Eury to rezone +/-2.513 acres generally located at the intersection of Beatties Ford Rd and Broadway St. from Rural to Highway Commercial - Conditional District for indoor and outdoor recreation and commercial uses.

ACTION RECOMMENDED:

Conduct Public Hearing

FINANCIAL IMPLICATIONS:

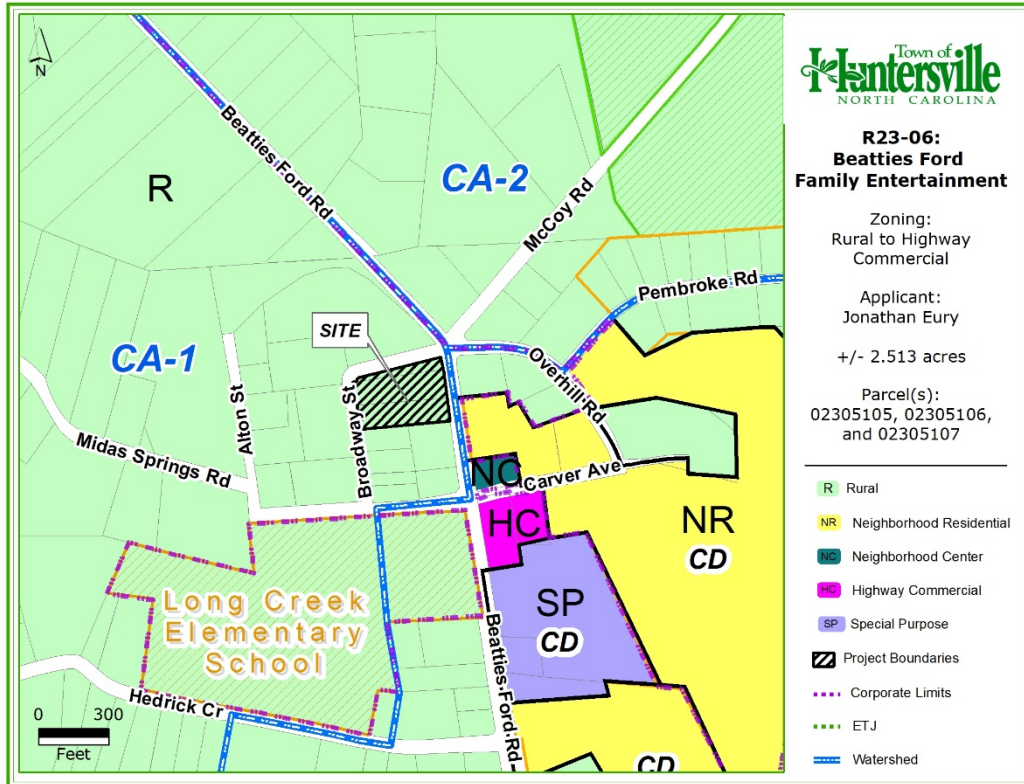
NA

ATTACHMENTS:

1. R23-06 PH Staff Report
2. Attachment A - Application
3. Attachment B - R23-06 Rezoning Plan
4. Attachment C - Neighborhood Meeting Report
5. Attachment D - APO Notification

Petition R23-06 Beatties Ford Family Entertainment

PART 1: PROJECT SUMMARY



Applicant: Jonathan Eury, Katie Carpenter

Property Owner: Jonathan Eury

Property Address: 9349, 9339, 9331 Beatties Ford Rd

Project Size: (+/-) 2.513 acres

Parcel Numbers: 02305105, 02305106, 02305107

Current Zoning: Rural (R)

Current Land Use: Single Family.

Proposed Zoning: Highway Commercial Conditional District (HC-CD)

Proposed Land Use: Commercial & Outdoor Recreation

- Purpose: Rezone +/- 2.513 acres west of Beatties Ford Rd. from Rural to Highway Commercial Conditional District (HC-CD) for indoor and outdoor recreation and commercial uses.
- Adjoining Zoning and Land Uses.
 - North: Rural – Currently Vacant and Single Family (Vacant).
 - South: Rural - Single Family.
 - East: Rural and Neighborhood Residential Conditional District – Single Family (Oak Grove Hill Subdivision Under Construction).
 - West: Rural – Long Creek Elementary & Single Family.
- A neighborhood meeting was held on June 24, 2023, and the questions asked by residents and the responses from the applicants are summarized in the Neighborhood Meeting Report (see Attachment C).
- Notice for this rezoning petition was sent via a postcard to adjoining property owners; a legal ad placed in the Charlotte Observer; and posting of rezoning signs on the property along Beatties Ford Rd.

PART 2: REZONING/SITE PLAN

The proposed Beatties Ford Family Entertainment Conditional District Rezoning Plan is summarized as follows:

- Transforming the existing single-family home into a rentable meeting/ office space.

- Open lawn area for Outdoor Recreation, Farmer's Market, and Movies.
- 30' Buffer along the south of the property will use existing and new vegetation to create a barrier between neighboring residential properties. A modification request has been made regarding this buffer (See below).
- Approximately 270' LF of side path will be installed along Beatties Ford Rd.
- Minimum Tree Preservation (Specimen Trees) for the Highway Commercial District is 30% Specimen Trees. The applicant is proposing to save 85% of existing specimen Trees.
- There are no identified Heritage Trees on site.
- Minimum Parking requirements for Commercial/Industrial/Office uses require 1 space per 500 S.F. The applicant is proposing to provide 16 spaces. The 3,663 S.F. existing structure would require the site to provide 8 spaces. A modification request is being made for parking surface materials (See Below).
- No changes to the elevations of existing structures have been indicated. An open-air covered area is proposed to the south of the home.
- The applicant has stated that the three parcels will be recombined.
- The applicant has noted as a condition of approval that 7000 S.F. of impervious will be transferred from parcel #02305213. The Impervious Transfer is completed administratively. The rezoning area is located within the Mountain Island Lake Critical Area-1 Watershed (6%).
- Planning, Transportation, and Storm Water Engineering staff have outstanding site plan comments that need to be addressed before final plan approval.
- Four (4) Ordinance Modifications are proposed:
 1. Article 4: Lot Type/ Highway Commercial – Building Placement/Parking/Vehicle Access (4) – Requires parking “to be located to the rear and/or side of the building” and “not be placed in any sideyard abutting an intersecting street”.

APPLICANT PROPOSAL – The request to allow for the placement of the parking lot in the sideyard abutting an intersection and not in the rear of the building is not consistent with the intent of the Zoning Ordinance.

STAFF COMMENT – Staff DOES NOT SUPPORT this modification request as it is not consistent with the Zoning Ordinance. *(The applicant has indicated that they will be moving the parking lot to the rear of the building in order to meet the Zoning requirements and negate the need for this modification.)*
 2. Article 6.1 (G): All commercial driveway and parking areas shall be paved with asphalt, concrete, or brick pavers except for areas used for overflow, special events, peak parking, and Riding Academies and Commercial Stables. Any non-paved surface used for overflow, special events, and peak parking that cannot be maintained with healthy, living turf grass or similar ground cover shall be paved with asphalt, concrete, pervious pavement, or brick pavers.

APPLICANT PROPOSAL – The applicant is requesting to pave the driveway through the parking area but use mulch for the individual parking stalls.

STAFF COMMENT – The use of a material not listed for use with a commercial parking area for required parking is not consistent with the intent of the Zoning Ordinance, staff DOES NOT SUPPORT this modification request.
 3. Article 5.1.3: Be bordered by sidewalks on both sides, with the exception of ditch-type local streets, alleys, and the undeveloped edge of parkways (see Article 7.11). Sidewalks on one side of the road may be permitted in the Rural zone as an incentive to protect water quality.

APPLICANT PROPOSAL – The applicant is requesting to not have to install sidewalks along Broadway Street.

STAFF COMMENT – Staff DOES NOT SUPPORT this modification request as it is the intent of the Zoning Ordinance to provide pedestrian access and safety along all public streets. The Beatties Ford Rd Corridor Small Area Plan specifically calls for “creating a network of community-friendly streets that provides for the safe, effective, and efficient movement of all modes of travel including walking, cycling, riding, and driving”. The small area plan would not support the modification request to not provide a sidewalk along Broadway St.

4. Article 7.5.3: Buffer Yards; Function - A buffer yard shall function as an opaque or semi-opaque barrier between the viewer and the use or structure to be buffered.

APPLICANT PROPOSAL – The applicant is requesting to allow an existing storage shed to encroach into the required 30 ft buffer on the south side of the property.

STAFF COMMENT –The existing vegetation and additional vegetation required by the buffer would mitigate the visual impact of the existing structure from the neighboring property. This is in keeping with the Spirit of the Ordinance, staff DOES SUPPORT this modification request.

PART 3: TRANSPORTATION ISSUES

Traffic Impact Analysis (TIA)

A Town TIA for the proposed project was not required.

Intersection Improvement Project

The purpose of the Beatties Ford at McCoy Intersection project is to improve safety and traffic movements by removing one of the five legs of the intersection (Overhill Rd) and installing a traffic signal. Utility coordination with Charlotte Water and Duke Energy is currently underway, and Right-of-Way plans are being finalized.

PART 4: REZONING CRITERIA

Article 11.4.7(d) of the Zoning Ordinance states that “in considering any petition to reclassify property, the Planning Board in its recommendation and the Town Board in its decision shall take into consideration any identified relevant adopted land-use plans for the area including, but not limited to, comprehensive plans, strategic plans, district plans, area plans, neighborhood plans, corridor plans, and other land-use policy documents”.

2040 Huntersville Community Plan



STAFF COMMENT – The 2040 Huntersville Community Plan DOES NOT SUPPORT this project through the following sections:

- **Policy LU 6.1:** A mix of land uses is encouraged in Mixed-Use Centers, Activity Centers, Employment Centers identified on the Future Land Use Map.
STAFF COMMENT: LU 6.1 does not support the request as this rezoning is not located within a Mixed-Use, Activity, or Employment Center. The site is currently surrounded by residential properties.
- **Policy LU 6.2:** Commercial uses are encouraged in the Town Core and as specified in adopted Small Area Plans.
Staff Comment: LU 6.2 does not support the request as the rezoning request is located within the Rural Conservation and Critical Watershed Future Land Use areas.
- **Policy LU 6.3:** Small scale, neighborhood-serving commercial and office uses may be allowed in Town Core and Moderate Density areas specified on the Future Land Use map at key locations if designed in a context sensitive manner.
STAFF COMMENT: LU 6.3 does not support the rezoning as small scale commercial and office uses are specified on the Future Land Use map to be allowed within the Town Core and Moderate Density areas, not in the current Rural Conservation area that the rezoning is located in.
- **EOS 10.2:** Prioritize neighborhood improvements recommended in small area plans.
 - Working with community members to revisit/confirm street and sidewalk improvement recommendations from small area plans, including those in the East Huntersville / Pottstown.**Staff Comment:** EOS 10.2 does not support the rezoning as the Beatties Ford Rd Corridor Small Area Plan specifically calls for “creating a network of community-friendly streets that provides for the safe, effective, and efficient movement of all modes of travel including walking, cycling, riding, and driving”. The small area plan would not support the modification request to not provide a sidewalk along Broadway St.

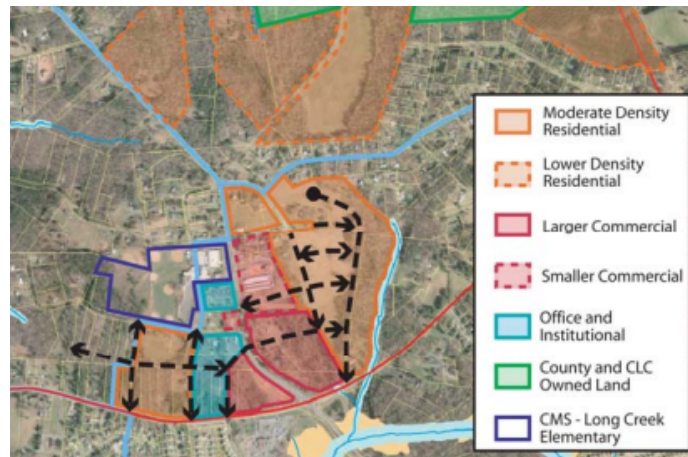
Beatties Ford Rd Corridor Small Area Plan (2007)



Preserve the existing rural character: The study area will continue to develop as a low density, predominantly residential district, as established by the Town's overall planning framework. Future commercial development within the study area should be focused at NC 73 and at Mount Holly - Huntersville Road, with an additional center at the intersection of Hambricht Road with BFR. In conjunction

The Beatties Ford Rd Corridor Small Area Plan created a vision for future land use for which the area should remain and develop as a low-density residential district. The plan calls out the Beatties Ford Rd and Hambricht Intersection as the appropriate area for future commercial development. The rezoning site falls within the study area that should remain low-density and primarily residential.

Beatties Ford Rd./Mt. Holly-Huntersville Rd Small Area Plan (2005)



The Beatties Ford Rd./Mt. Holly-Huntersville Rd Small Area Plan created a vision for the future commercial and residential growth for the intersection at Beatties Ford Rd and Mt. Holly Huntersville Rd. The plan calls for higher intensity commercial development to be focused closer to Hambright Rd and then decrease intensity the farther your travel north on Beatties Ford Rd. The rezoning site does not fall into the plans commercial or residential zones for development.

Article 11 Section 11.4.7(e) of the Zoning Ordinance states that: “in considering any petition to reclassify property the Planning Board in its recommendation and the Town Board in its decision should consider:

- 1. Whether the proposed reclassification is consistent with the overall character of existing development in the immediate vicinity of the subject property.**

STAFF COMMENT:

The property is surrounded by residential properties such that the higher intensity proposed uses would not be consistent with existing development in the immediate vicinity of the subject property. The proposed rezoning for the Beatties Ford Family Entertainment is not consistent with envisioned uses and development patterns set forth in the 2040 Community Plan and Beatties Ford Rd Corridor Small Area Plan.

- 2. The adequacy of public facilities and services intended to serve the subject property, including but not limited to roadways, transit service, parks and recreational facilities, police and fire protection, hospitals and medical services, schools, stormwater drainage systems, water supplies, and wastewater and refuse disposal.**

STAFF COMMENT:

- A Transportation Impact Analysis was not required – see Part 3 of this report.
- The property is currently served by a septic system.
- The property is currently being served by Charlotte Water.

- 3. Whether the proposed reclassification will adversely affect a known archeological, environmental, historical or cultural resource.”**

STAFF COMMENT:

Planning staff has no indication that the request will adversely affect known archeological, environmental, or cultural resources. Currently, the site is not encumbered by any historic easements or deed restrictions. The rezoning site is located

within the Mountain Island Lake Critical Area-1 Watershed. The applicant has noted as a condition of approval that 7000 S.F. of impervious will be transferred from parcel #02305213. The Impervious Transfer is completed administratively.

PART 5: STAFF RECOMMENDATION

In considering the proposed rezoning petition R23-06, Beatties Ford Family Entertainment, Staff does not recommend approval for the following reasons:

- The Rezoning is not consistent with the Huntersville 2040 Community Plan, specifically, Policies LU 6.1, LU 6.2, LU 6.3, and EOS 10.2.
- The Rezoning is not consistent with the Beatties Ford Rd Corridor Small Area Plan and the Beatties Ford Rd / Mt. Holly-Huntersville Rd Small Area Plan.
- The Rezoning is not consistent with the existing development patterns in the vicinity.
- The proposed use is an increase in intensity in an area set aside for low-intensity residential development and would set a precedent to develop Rural Zoned land within a Critical Area Watershed as Commercial.
- Requested modifications of #1 (Parking Location), #2 (Parking Surface Material), and #3 (No Broadway St Sidewalks) are not in keeping with the spirit of the Ordinance and therefore not supported.

PART 6: PUBLIC HEARING COMMENTS

A Public Hearing is scheduled for August 7, 2023.

PART 7: PLANNING BOARD RECOMMENDATION

Planning Board is scheduled for August 22, 2023.

PART 8: TOWN BOARD CONSIDERATION

Town Board consideration is scheduled for September 18, 2023.

PART 9: ATTACHMENTS/ENCLOSURES

Attachments

- A – Rezoning Application
- B – R23-06 Rezoning Plan
- C – Neighborhood Meeting Report (June 24, 2023)
- D – APO Notification

PART 10: CONSISTENCY STATEMENT – R23-06 Beatties Ford Family Entertainment

Planning Department	Planning Board	Board of Commissioners
APPROVAL: NA	APPROVAL: In considering the proposed rezoning application R23-06, Beatties Ford Family Entertainment, the Planning Board recommends approval based on the Plan being consistent with <u>(insert applicable plan reference)</u> . <u>It is reasonable and in the public interest to approve the Rezoning Plan because... (Explain)</u>	APPROVAL: In considering the proposed rezoning application R23-06, Beatties Ford Family Entertainment, the Town Board recommends approval based on the Plan being consistent with <u>(insert applicable plan reference)</u> . <u>It is reasonable and in the public interest to approve the Rezoning Plan because... (Explain)</u>

DENIAL: In considering the proposed rezoning application R23-06, Beatties Ford Family Entertainment, the Planning Department recommends denial based on the Plan being inconsistent with the Huntersville 2040 Community Plan policies LU 6.1, LU 6.2, LU 6.3, EOS 10.2 and with the Beatties Ford Rd. Corridor Small Area Plan and Beatties Ford Rd / Mt. Holly-Huntersville Rd Small Area Plan. It is reasonable and in the public interest to not approve the Rezoning Plan because it is not consistent with the envisioned uses and development pattern set forth in the 2040 Community Plan, Beatties Ford Rd Corridor Small Area Plan, and Beatties Ford / Mt. Holly-Huntersville Rd Small Area Plan. Modifications #1, #2, and #3 are not in keeping with the spirit of the Ordinance and therefore cannot be supported.	DENIAL: In considering the proposed rezoning application R23-06, Beatties Ford Family Entertainment, the Planning Board recommends denial based on the Plan being <u>(consistent OR inconsistent) with (insert applicable plan reference).</u> <u>It is not reasonable and in the public interest to approve the Rezoning Plan because... (Explain)</u>	DENIAL: In considering the proposed rezoning application R23-06, Beatties Ford Family Entertainment, the Town Board recommends denial based on the Plan being <u>(consistent OR inconsistent) with (insert applicable plan reference).</u> <u>It is not reasonable and in the public interest to approve the Rezoning Plan because... (Explain)</u>
--	---	---



General Application

INCOMPLETE SUBMISSIONS WILL NOT BE ACCEPTED. PLEASE CHECK ALL ITEMS CAREFULLY.

1. Application Type

Please indicate the type of application you are submitting. In addition to the application, the submission process for each application type can be found at <https://www.huntersville.org/528/Permits-Process>

- ☐ Change of Use
- ☐ Commercial Site Plan
- ☒ Conditional Rezoning
General Rezoning
- ☐ Master Signage Program
- ☐ Special Use Permit
- ☐ Revision to
Original Project # _____
- ☐ Other _____

- SUBDIVISION CATEGORIES: Per the Huntersville Subdivision Ordinance
- ☐ Sketch Plan
 - ☐ Preliminary Plan
 - ☐ Final Plat (Includes Minor Subdivision)
 - ☐ Exempt Subdivision
 - ☐ Final Plat Revision
 - ☐ Farmhouse Cluster

2. Project Data

Date of Application 4/28/2023

Name of Project Long Creek Family Entertainment

Phase # (if subdivision) _____

Project Address 9339 Beatties Ford Rd Huntersville, NC 28078

Parcel Identification Number(s) (PIN) 02305105, 02305106, 02305107

Current Zoning District R Proposed District (for rezoning only) Highway Commercial

Property Size (acres) .891, 1.004, .618 = 2.513 acres Street Frontage (feet) 860 Feet

Current Land Use Residential

Proposed Land Use(s) Highway Commercial

Is the project within Huntersville's corporate limits?

Yes _____ No X If no, does the applicant intend to voluntarily annex? yes

3. Description of Request

Explain the nature of this request. If a separate sheet is necessary, please attach to this application.

Rezone to allow for a local, small business, owner operated family focused coffee/soda shop with outdoor seating and recreation (cornhole, kubb, lawn games).

We will use the existing home to keep and maintain the aesthetics of the neighborhood and keep the rural feel.

4. Site Plan Submittals

Consult the particular type of *Review Process* for the application type selected above. These can be found at <https://www.huntersville.org/528/Permits-Process>.

5. Outside Agency Information

Other agencies may have applications and fees associated with the land development process. The Review Process list includes plan documents needed for most town and county reviewing agencies. For major subdivisions, commercial site plans, and rezoning petitions please enclose a copy of the Charlotte-Mecklenburg Utility Willingness to Serve letter for the subject property.

6. Applicant

Printed Name Jonathan Eury

Phone 704-674-4223

☐ Corporation ☐ Limited Liability Company ☐ Trust ☐ Partnership ☐ Other: _____

☐ By signature below, I hereby acknowledge, as/on behalf of (circle one) the applicant my understanding this application will be considered in a quasi-judicial proceeding and that neither I, nor anyone on my behalf, may contact the Board of Commissioners except through sworn testimony at the public hearing. (Applicable for Special Use Permits and Subdivisions)

Signature [Signature] Printed Name: Jonathan Eury

Title Property owner Email euryjon@gmail.com

Address of Applicant 9339 Beatties Ford Rd Huntersville NC 28078

7. Property Owner (if different than applicant)

*Printed Name _____

Phone _____

☐ Corporation ☐ Limited Liability Company ☐ Trust ☐ Partnership ☐ Other: _____

☐ By signature below, I hereby acknowledge, as/on behalf of (circle one) the owner my understanding this application will be considered in a quasi-judicial proceeding and that neither I, nor anyone on my behalf, may contact the Board of Commissioners except through sworn testimony at the public hearing. (Applicable for Special Use Permits and Subdivisions)

Signature _____ Printed Name _____

Title _____ Email _____

Address of Property Owner _____

* Property owner hereby grants permission to the Town of Huntersville personnel to enter the subject property for any purpose required in processing this application.

Every owner of each parcel included in this application, or the owner (s) duly authorized agent, must sign this application. If signed by an agent on behalf of the Owner, this application MUST be accompanied by a notarized Limited Power of Attorney signed by the property owner (s), specifically authorizing the agent to act on the owner (s) behalf in signing this application. Failure of each owner, or their duly authorized agent, to sign, or failure to include the authority of the agent signed by the property owner, will result in an INVALID APPLICATION. If additional space is needed for signatures, attach the Town of Huntersville Signature Addendum Form.

8. Development/Design Firm Contact Information

The Isaacs Group	Brian Upton	704-527-3440	bupton@issacsgrp.com
Development Firm	Name of Contact	Phone	Email

Design Firm	Name of Contact	Phone	Email
-------------	-----------------	-------	-------

Contact Information

Town of Huntersville
Planning Department
PO Box 664
Huntersville, NC 28070

Phone: 704-875-7000
Fax: 704-992-5528
Physical Address: 105 Gilead Road, Third Floor
Website: <https://www.huntersville.org/228/Planning-Department>



General Application
Owner/Applicant Signature Addendum

Application Information

Date of Application 4/28/2023 Application Number SPM# 448546
Name of Project Long Creek Family Entertainment Phase # (if subdivision) _____

Additional Owners/Applicants: (Signature indicates intent that this page be affixed to Application.)

* ^ Printed Name Katherine Carpenter Phone Number 585 749 5712
☐ Corporation ☐ Limited Liability Company ☐ Trust ☐ Partnership ☒ Other:

☒ By signature below, I hereby acknowledge, as/on behalf of (circle one) the applicant/owner (circle one) my understanding this application will be considered in a quasi-judicial proceeding and that neither I, nor anyone on my behalf, may contact the Board of Commissioners except through sworn testimony at the public hearing. (Applicable for Special Use Permits and Subdivisions)

Signature [Signature] Parcel ID(s): 02305105, 02305106, 02305107

Title owner Email KCarpenter00@gmail.com

Address of Property Owner/Applicant 9335 Beathes Ford Rd

* ^ Printed Name _____ Phone Number _____
☐ Corporation ☐ Limited Liability Company ☐ Trust ☐ Partnership ☐ Other:

☐ By signature below, I hereby acknowledge, as/on behalf of (circle one) the applicant/owner (circle one) my understanding this application will be considered in a quasi-judicial proceeding and that neither I, nor anyone on my behalf, may contact the Board of Commissioners except through sworn testimony at the public hearing. (Applicable for Special Use Permits and Subdivisions)

Signature _____ Parcel ID(s): _____

Title _____ Email _____

Address of Property Owner/Applicant _____

* ^ Printed Name _____ Phone Number _____
☐ Corporation ☐ Limited Liability Company ☐ Trust ☐ Partnership ☐ Other:

☐ By signature below, I hereby acknowledge, as/on behalf of (circle one) the applicant/owner (circle one) my understanding this application will be considered in a quasi-judicial proceeding and that neither I, nor anyone on my behalf, may contact the Board of Commissioners except through sworn testimony at the public hearing. (Applicable for Special Use Permits and Subdivisions)

Signature _____ Parcel ID(s): _____

Title _____ Email _____

Address of Property Owner/Applicant _____

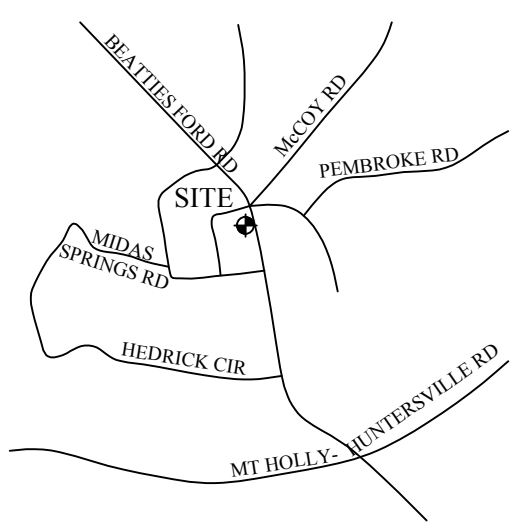
* Property owner hereby grants permission to the Town of Huntersville personnel to enter the subject property for any purpose required in processing this application.

^ If signed by an agent on behalf of the Owner, this petition MUST be accompanied by a Limited Power of Attorney signed by the property owner (s) and notarized, specifically authorizing the agent to act on the owner (s) behalf in signing this application. Failure of each owner, or their duly authorized agent, to sign, or failure to include the authority of the agent signed by the property owner, will result in an INVALID APPLICATION.

LONG CREEK FAMILY ENTERTAINMENT

9339 BEATTIES FORD RD., HUNTERSVILLE, NC

EPM #448946



VICINITY MAP: NOT TO SCALE

PURPOSE:

TO REZONE EXISTING PROPERTY TO HIGHWAY COMMERCIAL
HC-CD IN ORDER TO ALLOW OUTDOOR ENTERTAINMENT
AREAS

GENERAL NOTES:

- THIS MAP IS NOT A CERTIFIED SURVEY. BOUNDARY AND TOPOGRAPHIC INFORMATION PROVIDED BY PROFESSIONAL PROPERTY SURVEYORS, INC. THE PHYSICAL AND TOPOGRAPHIC DATA PROVIDED IN THESE DRAWINGS HAS BEEN COMPILED BY THE ISAACS GROUP AND THE ENGINEER OF RECORD (ENGINEER) IN SUPPORT OF THIS PROJECT AND CANNOT BE RELIED UPON BY OTHERS. "THE ISAACS GROUP" AND "THE ENGINEER OF RECORD" SHALL DEFINE THE TERM OF "ENGINEER" USED IN THE SUBSEQUENT NOTES.
- THE EXISTING UTILITIES SHOWN ARE FOR THE CONTRACTOR'S CONVENIENCE ONLY. THERE MAY BE OTHER UTILITIES NOT SHOWN ON THIS PLAN AND THE UTILITIES SHOWN ON THIS PLAN MAY NOT BE IN THE EXACT LOCATIONS AS SHOWN. THE ISAACS GROUP, P.C. ASSUMES NO RESPONSIBILITY FOR THE LOCATIONS SHOWN OR ANY OMISSIONS IN SHOWING EXISTING UTILITIES THAT MAY BE WITHIN THE PROJECT AREA. THE CONTRACTOR IS 100% RESPONSIBLE FOR UTILIZING A PRIVATE LOCATOR AND APPROPRIATE UTILITY COMPANIES TO LOCATE THE SIZE, LOCATION, INVERTS, DEPTHS AND EXISTENCE OF ALL EXISTING UTILITIES (ELECTRICAL, MECHANICAL, WATER, TELEPHONE, FIBER OPTIC, GAS, ETC.) TO HIS/HER SATISFACTION PRIOR TO COMMENCEMENT OF CONSTRUCTION AND EXCAVATION ACTIVITIES. CONFLICTS BETWEEN EXISTING UTILITIES AND PROPOSED EXCAVATION SHALL BE REPORTED TO THE ENGINEER IMMEDIATELY.
- PROVIDE MINIMUM OF 48 HOUR NOTICE TO OWNER OR REPRESENTATIVE PRIOR TO INTERRUPTION OF ANY EXISTING UTILITY, IF BEING UTILIZED.
- THE CONTRACTOR IS RESPONSIBLE FOR REPAIR AND/OR REPLACEMENT OF ANY UTILITIES DAMAGED DURING CONSTRUCTION. THE CONTRACTOR SHALL BE SOLELY RESPONSIBLE FOR LOCATION & PROTECTION OF EXISTING ABOVE AND BELOW GROUND UTILITIES AND STRUCTURES. ANY AND ALL MAINS OR INDIVIDUAL SERVICES PRESENTLY IN SERVICE WHICH ARE DAMAGED DURING CONSTRUCTION SHALL BE REPAIRED IMMEDIATELY AT NO ADDITIONAL EXPENSE TO THE OWNER OR THE ISAACS GROUP, P.C. ANY AND ALL MAINS OR INDIVIDUAL SERVICES PRESENTLY NOT IN SERVICE AND WHICH ARE TO BE REPLACED DURING THE COURSE OF CONSTRUCTION MAY BE REMOVED AND LEGALLY DISPOSED OF IF DAMAGED DURING CONSTRUCTION.
- THE CONTRACTOR SHALL USE EXTREME CARE WHEN WORKING NEAR ALL UNDERGROUND AND OVERHEAD UTILITIES.
- HANDICAP SIGNAGE TO BE INSTALLED IN ACCORDANCE WITH A.D.A STANDARDS AT H/C PARKING SPACES SHOWN.
- ALL DIMENSIONS ARE TO BACK OF CURB UNLESS OTHERWISE NOTED.
- THE CONTRACTOR IS RESPONSIBLE FOR ENSURING THAT ALL NECESSARY PERMITS AND APPROVALS HAVE BEEN OBTAINED PRIOR TO CONSTRUCTION. THESE PERMITS AND APPROVALS MAY INCLUDE BUT ARE NOT LIMITED TO GRADING, DEMOLITION, ZONING, BUILDING, DRIVEWAY, DETENTION, SUBDIVISION, SPECIAL USE, SEWER AND WATER.
- PROPOSED EXTERIOR ELEVATIONS ALONG BUILDING AND RETAINING WALLS ARE BASED UPON THE SITE GRADING AND DRAINAGE CONSTRAINTS IDENTIFIED BY THE ENGINEER. THE OWNER / DEVELOPER / PROJECT MANAGER IS RESPONSIBLE FOR ENSURING THE ARCHITECT AND STRUCTURAL ENGINEER ARE PROPERLY COORDINATING THE BUILDING EXTERIOR WALL AND RETAINING WALL ELEVATIONS BASED UPON THESE CIVIL DRAWINGS. ANY DISCREPANCIES BETWEEN THE INFORMATION SHOWN ON THESE DRAWINGS AND DRAWINGS PREPARED BY OTHER DESIGN CONSULTANTS NOT SUBCONTRACTING DIRECTLY WITH THE ISAACS GROUP / ENGINEER SHOULD BE REPORTED IMMEDIATELY UPON DISCOVERY AS NEEDED TO RESOLVE.
- PROPOSED DUMPSTER ENCLOSURES SHOWN ON THESE DRAWINGS ARE FOR INFORMATIONAL PURPOSES ONLY. ALL FINAL STRUCTURAL AND ARCHITECTURAL DETAILS AND SPECIFICATIONS FOR DUMPSTER ENCLOSURES SHALL BE PROVIDED BY OTHERS. THE OWNER / DEVELOPER / PROJECT MANAGER IS RESPONSIBLE FOR ENSURING THE FINAL DUMPSTER ENCLOSURE DETAILS FOR CONSTRUCTION ARE COORDINATED BETWEEN ALL DISCIPLINES. ANY DISCREPANCIES BETWEEN THE INFORMATION SHOWN ON THESE DRAWINGS AND DRAWINGS PREPARED BY OTHER DESIGN CONSULTANTS NOT SUBCONTRACTING DIRECTLY WITH THE ISAACS GROUP / ENGINEER SHOULD BE REPORTED IMMEDIATELY UPON DISCOVERY AS NEEDED TO RESOLVE.
- PROPOSED LOCATIONS AND SIZES OF UNDERGROUND UTILITIES SHOWN ON THESE DRAWINGS ARE BASED UPON DESIGN CONSTRAINTS IDENTIFIED BY THE ENGINEER AND SHOULD BE VERIFIED BY THE CONTRACTOR TO ENSURE CONSISTENCY WITH THE MECHANICAL, ELECTRICAL AND PLUMBING PLANS TO ENSURE PROPER COORDINATION AND PLAN CONSISTENCY. ANY DISCREPANCIES BETWEEN THE INFORMATION SHOWN ON THESE DRAWINGS AND DRAWINGS PREPARED BY OTHER DESIGN CONSULTANTS NOT SUBCONTRACTING DIRECTLY WITH THE ISAACS GROUP / ENGINEER SHOULD BE REPORTED IMMEDIATELY UPON DISCOVERY AS NEEDED TO RESOLVE.

023-052-40
BRETT A. GRANBERRY
RICHARD J. WNUK
DB 35691, PG 142
ZONING: R

S.R. #2122
BROADWAY STREET
35' PUBLIC R/W (DB 2439, PG 803)

023-052-60
MARY BURKHEART BRETT
SCOTT BRETT
DB 8530, PG 211
ZONING: R

S.R. #2122
BROADWAY STREET
60' PUBLIC R/W (DB 4552, PG. 386)

023-052-13
KATHERINE CARPENTER
DB 37706, PG 757
ZONING: R

RIGHT-OF-WAY TO BE
RESERVED ALONG BEATTIES
FORD ROAD FOR SIDEWALK

PROP. DUMPSTER WILL BE
SURROUNDED BY A CORRAL TO
MATCH THE LOOK OF THE
EXISTING BUILDING-BRICK
BOTTOM WITH WHITE WALLS

APPROX. EXIST. ROAD CL.
BEATTIES FORD ROAD
PUBLIC R/W VARIES (DB 4552, PG. 386)

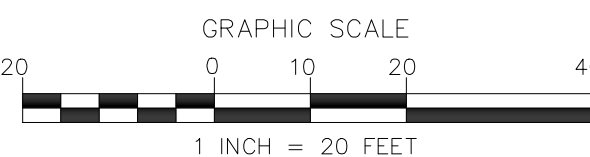
PROP. 10' SIDEWALK W/
GREEN ZONE
(IMPROVEMENTS NEED TO BE
COORDINATED WITH NCDOT
ROAD IMPROVEMENT PLANS)

APPROX. LOCATION OF
TEMPORARY
CONSTRUCTION
EASEMENT

023-051-09
CINDY Y. HOUGH
DB 21636, PG 133
ZONING: R

023-051-08
F.C. HOUGH JR.
MARGARET S. HOUGH
DB 3700, PG 985
ZONING: R

PRELIMINARY
FOR REVIEW PURPOSES ONLY



NO.	BY	DATE	REVISION
1	CBH	3/16/23	REVISED PER TOWN COMMENTS
2	CBH	4/6/23	REVISED PER TOWN COMMENTS
3	BTU	4/24/23	REVISED PER TOWN COMMENTS
4	CBH	6/9/23	REVISED PER TOWN COMMENTS

Project: LONG CREEK
FAMILY ENTERTAINMENT
9339 BEATTIES FORD RD., HUNTERSVILLE, NC

Title: COVER SHEET

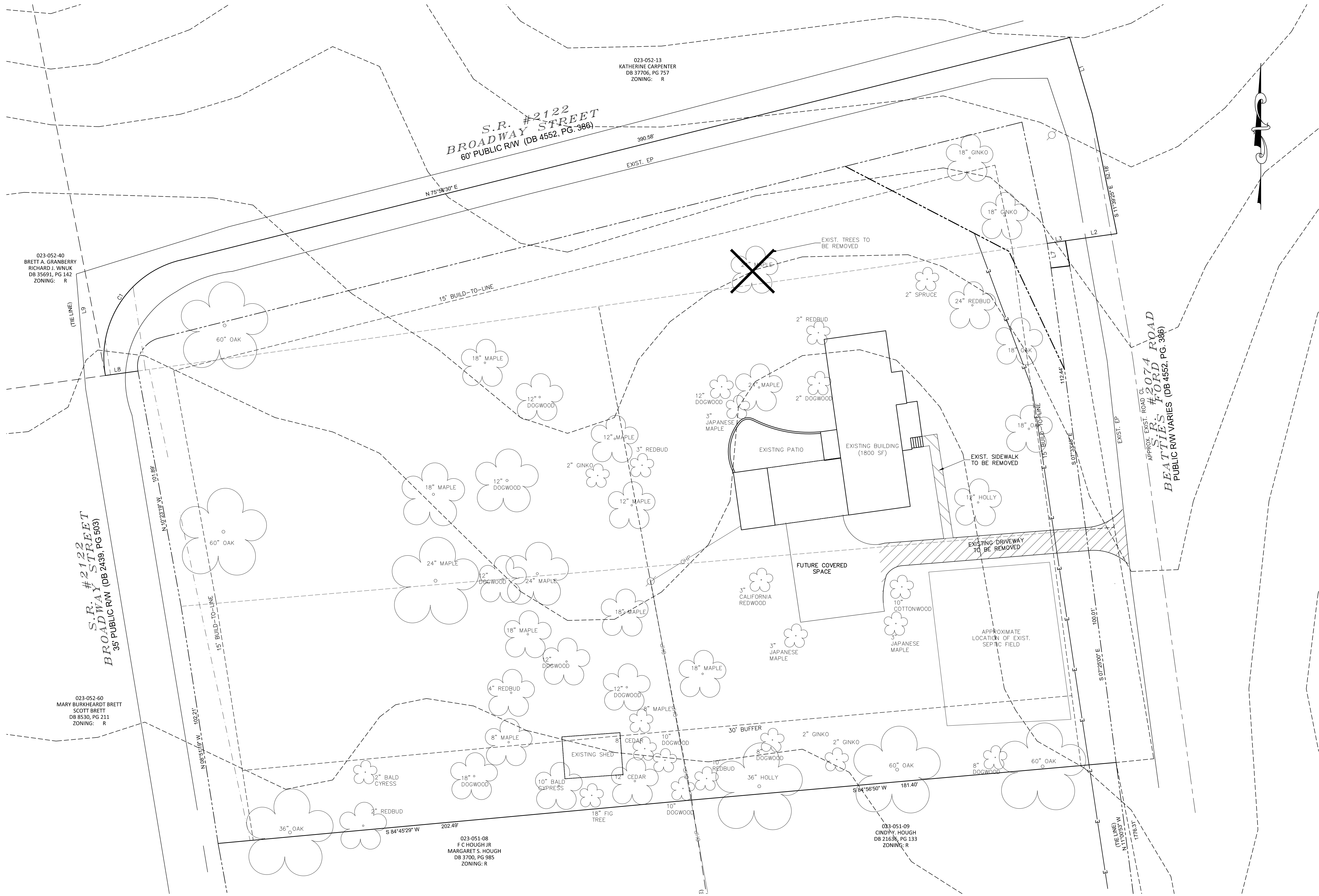
File #22033-9K.DWG Date: 6/20/22 Project Egr: BTU

THE ISAACS GROUP
CIVIL ENGINEERING DESIGN AND SURVEYING

8720 RED OAK BOULEVARD, SUITE 420
CHARLOTTE, N.C. 28217
PHONE (704) 527-3440 FAX (704) 527-8335

Design By: BTU
Drawn By: CBH
Scale: 1"=20'

RZ0.0



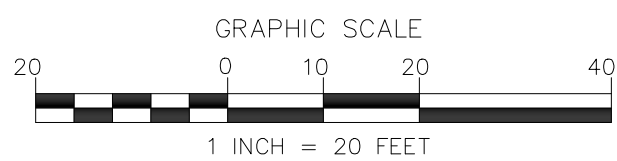
- Oak - O =5
- Dogwood - DW =12
- Maple - M =15
- Japanese Maple - JM =3
- Ginkgo - G =5
- Holly - H =2
- Cedar - C =2
- California Redwood - CR =1
- Bald Cypress - BC =1
- Cottonwood - CW =1
- Spruce - S =1
- Redbud - R =5
- Black Locust - BL =1
- River Birch - RB =1
- Fig tree - F =1
- TOTAL EXISTING TREES =59

SPECIMEN TREE SAVE REQUIREMENT:
FOR HC ZONING, TREE SAVE = 30% OF SPECIMEN TREES
(TREES 24" OR GREATER)

THERE ARE 7 SPECIMEN TREES ON THIS SITE.
30% OF 7 SPECIMEN TREES = 0.30 x 7 = 2.1 TREES (TO BE SAVED)

1 SPECIMEN TREES TO BE REMOVED
6 SPECIMEN TREES TO REMAIN

PRELIMINARY
FOR REVIEW PURPOSES ONLY



NO.	BY	DATE	REVISION
1	CBH	3/16/23	REVISED PER TOWN COMMENTS
2	CBH	4/6/23	REVISED PER TOWN COMMENTS
3	BTU	4/24/23	REVISED PER TOWN COMMENTS
4	CBH	6/9/23	REVISED PER TOWN COMMENTS

Project: LONG CREEK
FAMILY ENTERTAINMENT
9339 BEATTIES FORD RD., HUNTERVILLE, NC

Title: EXISTING CONDITIONS

File #22033-9K.DWG Date: 02/28/23 Project Egr: BTU

Design By: BTU
Drawn By: CBH
Scale: 1"=20'

8720 RED OAK BOULEVARD, SUITE 420
CHARLOTTE, N.C. 28217
PHONE (704) 527-3440 FAX (704) 527-8335

RZ0.1

DEVELOPMENT DATA

PROJECT NAME: LONG CREEK FAMILY ENTERTAINMENT
ADDRESS: 9339 BEATTIES FORD RD.
PLANS PREPARED BY: THE ISAACS GROUP, PC PHONE #: 704-227-9406
ZONING: R TAX PARCEL #: 00925409, 00925410, 02305213
PROPOSED ZONING: HC-CD

JURISDICTION: TOWN OF HUNTERSVILLE
PROPOSED USE: RENTABLE MEETING/OFFICE SPACES FOR COMMUNITY/CLUBS
SUBJECT PROPERTY AREA: 94,830/2.177 SQ. FEET/ACRES
PROPERTY AREA FOR IMPERVIOUS TRANSFER= 180,438/4.143
TOTAL PROPERTY AREA= 275,268/6.32
GROSS FLOOR AREA: 3,663 SF (PER GIS)
EXISTING IMPERVIOUS AREA: 7,103 SQ. FT
EXISTING IMPERVIOUS AREA TO BE REMOVED: 910 SQ. FT
PROPOSED IMPERVIOUS AREA TO BE ADDED: 4,512 SQ. FT/ACRES
TOTAL POST CONSTRUCTION IMPERVIOUS AREA: 10,705 SQ. FT/ACRES
TOTAL POST CONSTRUCTION IMPERVIOUS % 4% IMPERVIOUS
MAX POST CONSTRUCTION IMPERVIOUS % 6% IMPERVIOUS
WATERSHED: MOUNTAIN ISLAND LAKE WATERSHED CA-1

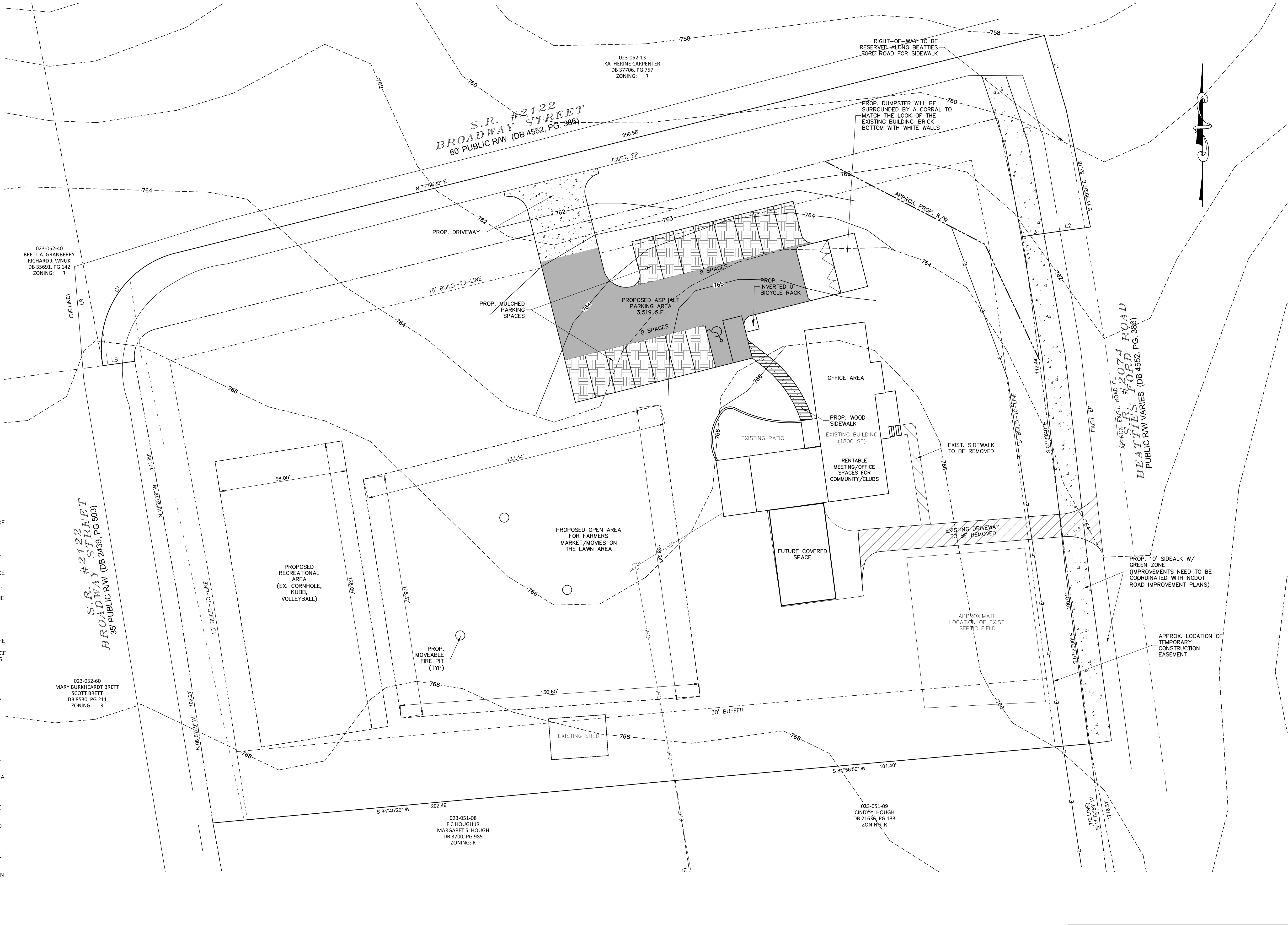
BUILDING SETBACK REQUIREMENTS:
BEATTIES FORD RD: 25' SETBACK BROADWAY STREET: (REAR) 25' SETBACK
BROADWAY STREET: (SIDE) 12.5' SETBACK SIDE: 10' SETBACK
SIDE BUFFER REQUIREMENTS 30' UNDISTURBED

REQUIRED PARKING:
REQUIRED PARKING (COMMERCIAL/INDUSTRIAL/OFFICE) = 1 SPACE PER 500 S.F.
EXISTING BUILDING= 3,663 S.F.

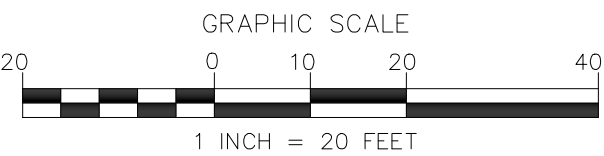
PARKING REQUIRED= 3663/500=7.3 SPACES
PARKING PROVIDED= 16 SPACES (INCLUDES 2 H.C. SPACES)
BICYCLE PARKING REQUIRED= 2 SPACES
BICYCLE PARKING PROVIDED= 2 SPACES

REZONING NOTES:

1. REZONING PETITION. THESE REZONING NOTES COMPRISE THE DEVELOPMENT STANDARDS ('DEVELOPMENT STANDARDS') ASSOCIATED WITH THE REZONING PETITION (THE 'REZONING PETITION') FILED BY JON EURY (PETITIONER) APPROXIMATELY 2.5 ACRE TRACT OF LAND IDENTIFIED ON THIS SITE PLAN AS LONG CREEK FAMILY OUTDOOR HANGOUT (THE 'PROJECT'), THE PURPOSE OF THE REZONING PETITION IS TO CONVERT THE ZONING CLASSIFICATION OF THE PROPERTY FROM RESIDENTIAL (R) TO HIGHWAY COMMERCIAL (HC) PURSUANT TO THE PROVISIONS OF THE TOWN OF HUNTERSVILLE ZONING ORDINANCE (THE 'ORDINANCE').
2. DEVELOPMENT STANDARDS. DEVELOPMENT OF THE PROPERTY WILL BE GOVERNED BY THESE DEVELOPMENT STANDARDS, WHICH ARE PART OF THE REZONING PETITION, AND THE APPLICABLE PROVISIONS OF THE ORDINANCE IN PLACE ON THE DATE OF SUBMITTAL OF THE REZONING PETITION. UNLESS THE REZONING PLAN ESTABLISHES A MORE STRINGENT STANDARD(S), OR UNLESS OTHERWISE NOTED ON THE REZONING PLAN OR IN THESE DEVELOPMENT STANDARDS, THE REGULATIONS ESTABLISHED UNDER THE ORDINANCE IN PLACE ON THE DATE OF SUBMITTAL OF THE REZONING PETITION FOR THE HIGHWAY COMMERCIAL (HC) ZONING GOVERN DEVELOPMENT OF THE PROPERTY AS SHOWN ON THE REZONING PLAN.
3. SCHEMATIC NATURE OF REZONING PLAN. THE PROPOSED IMPROVEMENTS SHOWN ON THE REZONING PLAN ARE SCHEMATIC IN NATURE. MINOR MODIFICATIONS TO THE PLAN MAY OCCUR DURING DESIGN, ENGINEERING AND CONSTRUCTION PHASES OF THE DEVELOPMENT. REMOVAL OF TREES AND VEGETATION, AS GENERALLY SHOWN ON THE REZONING PLAN, IS NECESSARY TO INSTALL THE IMPROVEMENTS.
4. VESTED RIGHTS. THIS REZONING PLAN IS A SITE-SPECIFIC DEVELOPMENT PLAN AND APPROVAL THEREOF CONSTITUTES VESTED RIGHTS IN THE REZONING PLAN PURSUANT TO THE PROVISIONS OF THE ORDINANCE. NOTWITHSTANDING ANY OTHER PROVISIONS OF THESE DEVELOPMENT STANDARDS, IF, AT SOME POINT, MODIFICATIONS ARE MADE TO THE ORDINANCE BY THE TOWN BOARD, PETITIONER MAY VOLUNTARILY AGREE TO APPLY SUCH MODIFICATIONS TO THE REZONING PLAN IN A MANNER CONSISTENT WITH THE ORDINANCE AS IT CHANGES FROM TIME TO TIME, AND WITHOUT PURSUING A REZONING. SUCH MODIFICATIONS TO THE ORDINANCE SHALL IN NO WAY IMPACT THE PETITIONER'S VESTED RIGHTS.
5. PERMITTED USES. THE PROPERTY MAY BE DEVELOPED FOR THE FOLLOWING USES (INCLUDING ACCESSORY USES): RENTABLE MEETING/OFFICE SPACES FOR COMMUNITY/CLUBS, AND AS SHOWN ON THE REZONING PLAN, SUBJECT TO THE DEVELOPMENT STANDARDS ASSOCIATED WITH SUCH USES. ANY LABELING ON THE REZONING PLAN MAY BE AN INDICATION OF THE CURRENT INTENTION ON THE PART OF PETITIONER BUT SHALL NOT RESTRICT THE PROPERTY IN A MANNER THAT CONFLICTS WITH THE PROVISIONS OF THESE DEVELOPMENT NOTES.
6. ACCESS. THE NUMBER OF SITE ACCESS POINTS, DRIVEWAYS AND CONNECTIONS TO ROADS ARE SCHEMATIC IN NATURE. TO THE EXTENT PERMITTED BY APPLICABLE DRIVEWAY PERMIT REQUIREMENTS, FUTURE DRIVEWAYS, ACCESS POINTS AND ROAD CONNECTIONS MAY CROSS THE SETBACK AND SHALL NOT REQUIRE A REZONING OF THE PROPERTY, BUT SHALL OTHERWISE COMPLY WITH APPLICABLE DRIVEWAY PERMIT REQUIREMENTS.
7. SUBDIVISION. THE PROPERTY IS ONE DEVELOPMENT AND MAY BE SUBDIVIDED WITHOUT A REZONING TO ALLOW SEPARATE OWNERS OF INDIVIDUAL PARCELS SO LONG AS SUCH SUBDIVISION IS IN COMPLIANCE WITH APPLICABLE LAW INCLUDING SUBDIVISION REGULATIONS. HOWEVER, RECONMINIZATION, CONDOMINIUMIZATION, OR REDUCTION IN THE NUMBER OF PARCELS MAY OCCUR IN ACCORDANCE WITH THE REGULATIONS OF THE ORDINANCE. REQUIREMENTS THAT ARE MET BY THE PROJECT AS A WHOLE, SUCH AS OPEN SPACE, TREE SAVE AND IMPERVIOUS REQUIREMENTS, NEED NOT BE MET BY INDIVIDUAL PARCELS.
8. AMENDMENT. IN THE EVENT ANY PORTION OF THE PROPERTY IS CONVEYED TO A THIRD PARTY, PETITIONER MAY REQUEST AN AMENDMENT TO THE REZONING PLAN WITHOUT THE WRITTEN CONSENT OF ANY OTHER OWNER OF ALL OR ANY PORTION OF THE PROPERTY UNLESS SUCH AMENDMENT CONSTITUTES A CHANGE IN THE BUILDING OR USE OF THE PORTION OF THE PROPERTY OWNED BY SUCH OWNER. PROVIDED PETITIONER PROVIDES FOR SUCH AMENDMENT RIGHT IN THE RECORDED PRIVATE RESTRICTIVE COVENANTS THAT GOVERN THE PROJECT, ALL REQUIREMENTS IN CONNECTION WITH THE AMENDMENT WILL BE CALCULATED ON THE PROPERTY AS A WHOLE IN THE SAME MANNER SUCH REQUIREMENTS WERE CALCULATED AT THE TIME OF THE INITIAL APPROVAL. THIS NOTE SHALL BE SHOWN ON THE FINAL PLAT WHEN RECORDED.
9. STORM WATER ELEMENTS. BUILT--UPON AREAS SHALL BE IN ACCORDANCE WITH THE ORDINANCE AS REQUIRED FOR THE HIGHWAY COMMERCIAL ZONING DISTRICT. A 7,000 S.F. IMPERVIOUS AREA TRANSFER IS REQUIRED FOR THIS LOT. TRANSFER LOT (PARCEL ID: 02305213) HAS BEEN SECURED AND IT'S APPROVAL IS DEPENDENT ON THE OUTCOME OF THIS REZONING
10. PROPOSED MODIFICATION REQUESTED FOR PARKING LOT LOCATION DUE TO HAVING FRONTAGE ALONG 3 STREETS AND DUE TO THE LOCATION OF UTILITIES/SEPTIC IN THE SOUTH EAST CORNER AS WELL AS TO MAXIMIZE TREE SAVE POTENTIAL ACROSS THE SITE. THE PROPOSED PARKING AREA ALSO MAXIMIZES THE SEPARATION OF PARKING FROM ADJACENT RESIDENTIAL USES. PARKING SPACE MATERIALS WILL BE MULCH W/ THE CENTER DRIVE AISLE BEING A PAVED SURFACE.
11. PROPOSED MODIFICATION REQUESTED TO NOT PROVIDE SIDEWALK ALONG BROADWAY STREET.
12. PROPOSED MODIFICATION REQUESTED TO ALLOW EXISTING SHED TO BE LOCATED IN THE BUFFER ALONG THE SOUTHERN PROPERTY LINE.
13. IF LIGHTS ARE INSTALLED FOR THE PROPOSED RECREATIONAL AREA THEY MUST BE IN COMPLIANCE W/CHAPTER 9.21.5 A-C OF THE TOWN OF HUNTERSVILLE UDO.



PRELIMINARY
FOR REVIEW PURPOSES ONLY



NO.	BY	DATE	REVISION
1	CBH	3/16/23	REVISED PER TOWN COMMENTS
2	CBH	4/6/23	REVISED PER TOWN COMMENTS
3	BTU	4/24/23	REVISED PER TOWN COMMENTS
4	CBH	6/9/23	REVISED PER TOWN COMMENTS

Project: LONG CREEK FAMILY ENTERTAINMENT
9339 BEATTIES FORD RD., HUNTERSVILLE, NC

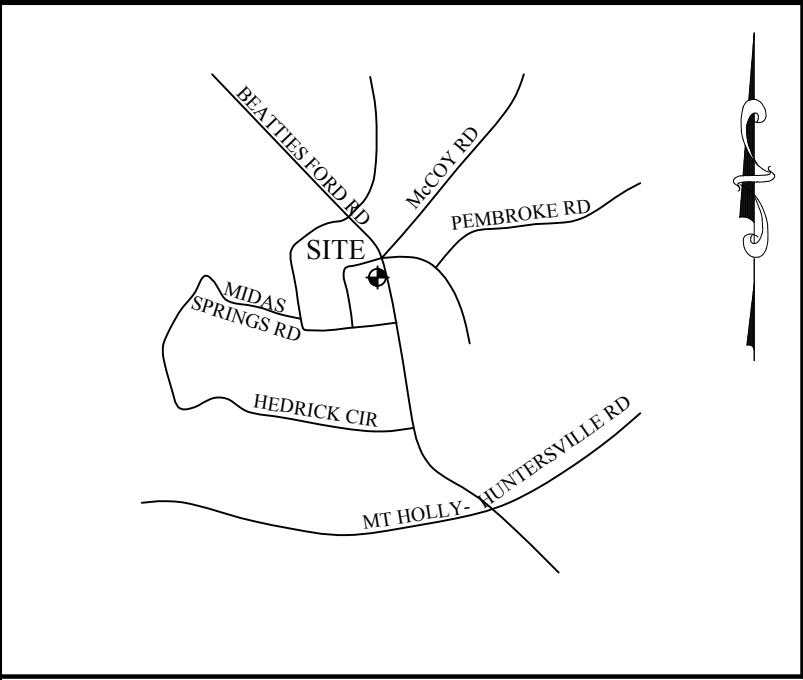
Title: REZONING SITE PLAN

File #22033-9K.DWG Date: 03/28/23 Project Egr: BTU

Design By: BTU
Drawn By: CBH
Scale: 1"=20'

8720 RED OAK BOULEVARD, SUITE 420
CHARLOTTE, N.C. 28217
PHONE (704) 527-3440 FAX (704) 527-8335

RZ1.0



VICINITY MAP: NOT TO SCALE

GENERAL PLANTING NOTES:

1. THIS PLAN FOR PLANTING LOCATIONS ONLY. IF FOUND CONDITIONS VARY FROM THIS, CONTRACTOR TO CONTACT OWNER'S REPRESENTATIVE FOR RESOLUTION. FAILURE TO DO SO WILL RESULT IN CONTRACTOR'S LIABILITY TO REPLACE PLANT MATERIALS.
2. CONTRACTOR TO COORDINATE WITH OWNER'S REPRESENTATIVE FOR EXISTING PLANT MATERIAL TO BE REMOVED AND/OR RELOCATED.
3. CONTRACTOR WILL BE RESPONSIBLE FOR LOCATING AND PROTECTING ALL UNDERGROUND AND ABOVE GROUND UTILITIES. CONTRACTOR SHALL BE LIABLE FOR DAMAGE TO ANY AND ALL PUBLIC OR PRIVATE UTILITIES. CONTRACTOR WILL BE HELD RESPONSIBLE FOR THE COST OF REPAIR TO ALL DAMAGED UTILITIES.
4. CONTRACTOR SHALL BE SOLELY RESPONSIBLE FOR ALL PLANT MAINTENANCE, INCLUDING SHRUBS AND GROUNDCOVER, AND SHALL MAINTAIN AREA IN A WEED AND DEBRIS FREE CONDITION, THROUGHOUT GUARANTEE PERIOD.
5. WHERE TREES ARE PLANTED IN ROWS, THEY SHALL BE UNIFORM IN SIZE AND SHAPE.
6. SIZES SPECIFIED IN THE PLANT LIST ARE MINIMUM SIZES TO WHICH THE PLANTS ARE TO BE JUDGED. FAILURE TO MEET MINIMUM SIZE ON ANY PLANT WILL RESULT IN REJECTION OF THAT PLANT.
7. PLANTING SIZE DETERMINATION:
SHADE TREES: HEIGHT SHALL BE MEASURED FROM THE CROWN OF THE ROOT BALL TO THE TOP OF MATURE GROWTH. SPREAD SHALL BE MEASURED TO THE END OF BRANCHING EQUALLY AROUND THE CROWN FROM THE CENTER OF THE TRUNK. MEASUREMENTS ARE NOT TO INCLUDE ANY TERMINAL GROWTH. SINGLE TRUNK TREES SHALL BE FREE OF "V" CROTCHES THAT COULD BE POINTS OF WEAK LIMB STRUCTURE OR DISEASE INFESTATION.
SHRUBS: HEIGHT SHALL BE MEASURED FROM THE CROWN OF THE ROOT BALL TO THE AVERAGE HEIGHT OF THE TOP OF THE PLANT. SPREAD SHALL BE MEASURED TO THE END OF BRANCHING EQUALLY AROUND THE SHRUB MASS. MEASUREMENTS ARE NOT TO INCLUDE ANY TERMINAL GROWTH.
8. ALL PLANTS SHALL BE FRESHLY DUG, SOUND, HEALTHY, VIGOROUS, WELL BRANCHED, FREE OF DISEASE, INSECT EGGS, AND LARVAE, AND SHALL HAVE ADEQUATE ROOT SYSTEMS.
9. ALL CONTAINER GROWN MATERIAL SHALL BE HEALTHY, VIGOROUS, WELL-ROOTED PLANTS AND ESTABLISHED IN THE CONTAINER IN WHICH THEY ARE SOLD. THE PLANTS SHALL HAVE TOPS WHICH ARE GOOD QUALITY AND ARE IN A HEALTHY GROWING CONDITION. ALL ROOT BOUND PLANTS SHALL BE REJECTED.
10. GROUPS OF SHRUBS SHALL BE PLACED IN A CONTINUOUS MULCH BED WITH SMOOTH CONTINUOUS LINES. ALL MULCHED BED EDGES SHALL BE CURVILINEAR IN SHAPE FOLLOWING THE CONTOUR OF THE PLANT MASS. TREES LOCATED WITHIN FOUR FEET OF SHRUB BEDS SHALL SHARE SAME MULCH BED.
11. CONTRACTOR TO SLIGHTLY ADJUST PLANT LOCATIONS IN THE FIELD AS NECESSARY TO BE CLEAR OF DRAINAGE SWALES AND UTILITIES. FINISHED PLANTING BEDS SHALL BE GRADED SO AS TO NOT IMPIDE DRAINAGE AWAY FROM BUILDINGS. IF SIGNIFICANT RELOCATIONS ARE REQUIRED, CONTRACTOR SHALL CONTACT OWNER'S REPRESENTATIVE FOR RESOLUTION. FAILURE TO MAKE SUCH RELOCATIONS KNOWN TO THE OWNER'S REPRESENTATIVE WILL RESULT IN CONTRACTOR'S LIABILITY OF PLANT MATERIALS.
12. ALL PLANT MATERIAL SHALL BE SPACED AND LOCATED PER PLAN. IF CONFLICTS ARISE BETWEEN ACTUAL SIZE OF AREA AND PLANS, CONTRACTOR SHALL CONTACT OWNER'S REPRESENTATIVE FOR RESOLUTION. FAILURE TO MAKE SUCH CONFLICTS KNOWN TO THE OWNER'S REPRESENTATIVE WILL RESULT IN CONTRACTOR'S LIABILITY TO RELOCATE MATERIALS.
13. ALL SUBSTITUTIONS OF PLANT MATERIAL ARE TO BE REQUESTED IN WRITING TO THE OWNER'S REPRESENTATIVE AND APPROVED IN WRITING BY THE OWNER PRIOR TO INSTALLATION. FAILURE TO OBTAIN SUBSTITUTION APPROVAL IN WRITING MAY RESULT IN LIABILITY TO THE CONTRACTOR.
14. ALL CONTRACTORS SHALL BE REQUIRED TO COMPLETELY REMOVE ALL TRASH, DEBRIS AND EXCESS MATERIALS FROM THE WORK AREA AND THE PROPERTY (ESPECIALLY AT ALL CURBS, GUTTERS AND SIDEWALKS) DAILY DURING INSTALLATION.
15. CONTRACTOR SHALL GUARANTEE ALL LANDSCAPE IMPROVEMENTS, INCLUDING SEEDING. CONTRACTOR MUST CONTACT THE OWNER AT LEAST 10 WORKING DAYS IN ADVANCE TO SCHEDULE ACCEPTANCE INSPECTION(S). CONTRACTOR MUST REPLACE ALL DEAD OR UNACCEPTABLE PLANTS DURING THE FOLLOWING RECOMMENDED PLANTING SEASON.
16. ADJUST TREE PLANTING LOCATIONS TO AVOID UNDERGROUND UTILITIES WHERE POSSIBLE. CONTRACTOR'S REPRESENTATIVE FOR A COORDINATED SOLUTION FOR ANY UTILITY CONFLICTS. CONTRACTOR SHALL BE LIABLE FOR DAMAGE TO ANY AND ALL PUBLIC OR PRIVATE UTILITIES.
17. REFER TO PLANTING DETAILS FOR ADDITIONAL PLANTING INFORMATION.
18. ALL PLANTINGS SHALL COMPLY WITH CURRENT LOCAL ORDINANCES AND GUIDELINES.
19. LANDSCAPE AREAS TO BE IRRIGATED WITH AUTOMATIC IRRIGATION SYSTEM.

LANDSCAPE LEGEND		
SYMBOL	SPECIES	QUANTITY
	SOUTHERN MAGNOLIA (BUFFER TREE) MAGNOLIA GRANDIFLORA (MIN. 2" CALIPER AND 8' AT TIME OF PLANTING) LARGE MATURING EVERGREEN	11
	TULIP-POPLAR LIRIODENDRON TULIPIFERA (MIN. 2" CALIPER AND 8' AT TIME OF PLANTING) LARGE MATURING DECIDUOUS	17
	FOSTER HOLLY (BUFFER TREE) ILEX ATTENUATA "FOSTER" (MIN. 2" CALIPER AND 8' AT TIME OF PLANTING) SMALL MATURING EVERGREEN	8
	ARBORVITAE THUJA ORIENTALIS (MIN. 2" CALIPER AND 8' AT TIME OF PLANTING) SMALL MATURING EVERGREEN	5
	MENTOR BARBERRY BERBERIS MENTORENSIS (MIN. 3" AT TIME OF PLANTING, MIN. 6' AT MATURITY)	107
	EXISTING TREE TO REMAIN	54

* THE SPECIES SPECIFIED ON THE PLANS MAY BE SUBSTITUTED WITH SOMETHING ELSE AS LONG AS THEY MEET THE TOWN'S CRITERIA

GENERAL PLANTING NOTES:

1. TURF AREAS WILL BE SEEDED OR SODDED WITH REBEL II FESCUE WITH EXCEPTION OF SOD WITHIN THE FLOOR OF STORMWATER MANAGEMENT AND WATER QUALITY BASINS AND FILTERS. SOD WILL BE REQUIRED NEXT TO BUILDING STRUCTURES, DRIVEWAYS ENTRANCES AND AREAS DISTURBED IN THE FRONT SETBACK AS NOTED ON PLAN. LANDSCAPE CONTRACTOR TO SEED ALL OTHER DISTURBED AREAS.
2. PINE NEEDLE MULCH IS THE GENERALLY ACCEPTED MULCH. FOR THE INITIAL PLANTING, IT IS ALSO ACCEPTABLE TO UTILIZE DOUBLE HAMMERED BARK MULCH FOR GOOD SOIL AND BED, THOUGH, WILL REQUIRE THE PROPERTY TO BE CONVERTED TO PINE NEEDLES.

PLANTING NOTES:

1. ALL PERIMETER SCREENING SHRUBS MUST BE NO LESS THAN 36" IN HEIGHT AT PLANTING
2. ALL PARKING LOT SHRUBS MUST BE NO LESS THAN 24" IN HEIGHT AT PLANTING

BUFFER PLANTING -- REQUIRED 30' BUFFER
- 4 TREES / 1000 SF BUFFER
- 50% LARGE MATURING TREE, 50% SMALL MATURING TREE, 25% EVERGREEN
- 7 SHRUBS / 1000 SF, 100% EVERGREEN
- 15 EXISTING AND 19 PROPOSED TREES PROVIDED

STREET TREE--BEATTIES FORD RD.
REQUIRED: 1 TREE PER 40 LF (213/40=5 TREES REQUIRED)
STREET TREES PROVIDED: 3 EXIST.+ 2 PROP. TREES

STREET TREE--BROADWAY ST.
REQUIRED: 1 TREE PER 40 LF (391/40=10 TREES REQUIRED)
STREET TREES PROVIDED: 2 EXIST.+ 8 PROP. TREES

STREET TREE--BROADWAY ST.
REQUIRED: 1 TREE PER 40 LF (204/40=5 TREES REQUIRED)
STREET TREES PROVIDED: 2 EXIST.+ 3 PROP. TREES

023-052-13
KATHERINE CARPENTER
DB 37706, PG 757
ZONING: R

S.R. #2122
BROADWAY STREET
60' PUBLIC R/W (DB 4552, PG. 386)

S.R. #2122
BROADWAY STREET
35' PUBLIC R/W (DB 2439, PG 503)

023-052-40
BRETT A GRANBERY
RICHARD J. WNUK
DB 35691, PG 142
ZONING: R

023-052-60
MARY BURKHEARDT BRETT
SCOTT BRETT
DB 8530, PG 211
ZONING: R

023-051-08
F.C. HOUGH JR.
MARGARET'S HOUSE
DB 3700, PG 985
ZONING: R

023-051-09
CINDY V. HOUGH
DB 21636, PG 133
ZONING: R

IRRIGATION SLEEVING NOTES:

1. GENERAL CONTRACTOR SHALL LAY ALL SLEEVES AND CONDUIT AT 2'-0" BELOW THE FINISH GRADE OF THE TOP OF PAVEMENT.
2. CONTRACTOR SHALL MARK THE LOCATION OF ALL SLEEVES AND CONDUIT WITH THE SLEEVING MATERIAL "TIE" TO 2'-0" ABOVE FINISH GRADE AND CAPPED.
3. CONTRACTOR SHALL FURNISH THE IRRIGATION DESIGNER WITH AN "AS-BUILT" DRAWING SHOWING ALL SLEEVES AND THE RESPECTIVE DEPTHS BELOW THE FINISH GRADE AND/OR PAVEMENT.
4. EXTEND ALL SLEEVES TO 2'-0" BEYOND THE EDGE OF ALL PAVEMENT.
5. ADD 4" DIAMETER SLEEVES TO ALL ISOLATED PLANTING AREAS NOT SHOWN ON THIS DRAWING, OR UNDER PAVEMENT, ADDED AFTER THIS PLAN WAS COMPLETED.
6. ALL SLEEVES SHALL BE SCHEDULED 40 PVC.

1.1 PLANTING SOIL MIX:

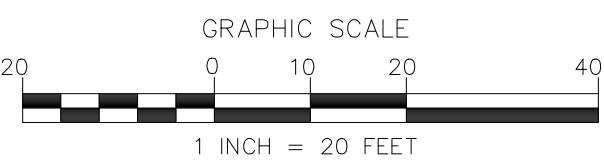
1. A FINAL CERTIFICATE OF OCCUPANCY MAY BE ISSUED PRIOR TO THE INSTALLATION OF TREES AND SHRUBS, EXCLUDING YARD TREES, DURING THE NON-PLANTING SEASON IF A CASH BOND, SURETY BOND OR LETTER OF CREDIT IS ISSUED FOR 100% OF THE COST OF MATERIALS AND INSTALLATION. PLANTING SHALL BE COMPLETED DURING THE NEXT PLANTING SEASON.
2. THE PLANTING SEASON SHALL RUN FROM OCTOBER 15 TO MARCH 15, EXCEPT FOR EXTREME WEATHER CONDITIONS AS DETERMINED BY STAFF. A FINAL CERTIFICATE OF OCCUPANCY SHALL NOT BE GIVEN DURING THE PLANTING SEASON UNLESS ALL OF THE LANDSCAPING IS COMPLETELY INSTALLED ACCORDING TO THIS ARTICLE.

MAINTENANCE SURETY REQUIRED

1. DEVELOPERS SHALL ENTER INTO A MAINTENANCE SURETY AGREEMENT WITH MEDELBURG COUNTY GUARANTEEING THE VIABILITY OF STREET TREES AND TREES AND SHRUBS PLANTED IN BUFFER YARDS FOR A PERIOD OF 1 YEAR FOLLOWING PLANTING. THE AMOUNT OF THE SURETY SHALL BE EQUAL TO 50% OF THE VALUE OF THE NEW TREES OR LANDSCAPE MATERIAL AND THEIR INSTALLATION. THE MAINTENANCE SURETY SHALL

1.1 PLANTING SOIL MIX:

1. MIX TOPSOIL WITH THE FOLLOWING SOIL AMENDMENTS IN THE FOLLOWING QUANTITIES:
1. WEIGHT OF LIME PER 1000 SQ. FT.
2. QUANT OF LOOSE COMPOST TOPSOIL, BY VOLUME: 1:4
3. RATIO OF LOOSE WOOD DERIVATIVES TO TOPSOIL BY VOLUME:
4. WEIGHT OF BOMBAK PER 1000 SQ. FT.
5. WEIGHT OF COMMERCIAL FERTILIZER PER 1000 SQ. FT.
6. WEIGHT OF SLOW-RELEASE FERTILIZER PER 1000 SQ. FT.
2. SOIL TEST PROVIDED BY CONTRACTOR REQUIRED FOR TOPSOIL MIX.



PRELIMINARY
FOR REVIEW PURPOSES ONLY

NO.	BY	DATE	REVISION
1	CBH	3/16/23	REVISED PER TOWN COMMENTS
2	CBH	4/6/23	REVISED PER TOWN COMMENTS
3	CBH	6/9/23	REVISED PER TOWN COMMENTS

TREE PLANTING NOTES:

1. ALL TREES SHALL BE PLANTED PER TOWN OF HUNTERSVILLE STANDARDS AND DETAILS.
2. ALL STRAPPING AND TOP 2/3 OF WIRE BASKET MUST BE CUT AWAY AND REMOVED FROM THE ROOT BALL PRIOR TO BACKFILLING PLANTING PIT.
3. LARGE MATURING TREES MAY NOT BE PLANTED WHERE OVERHEAD DISTRIBUTION OR TRANSMISSION LINES EXIST. IF TREES CONFLICT WITH POWER LINES OR SIGNS, CALL THE URBAN FORESTER TO RESOLVE BEFORE PLANTING.
4. ADJUST TREE PLANTING LOCATIONS TO AVOID UNDERGROUND UTILITIES.
5. NEW TREES SHALL BE A MINIMUM 2" CALIPER FOR STREET TREE REQUIREMENTS.
6. SEE TREE PRESERVATION NOTES ON GRADING AND EROSION CONTROL SHEETS.
7. ALL TREES ARE TO BE NURSERY GROWN, BALL AND BURLAP (BAB) PREFERRED. MINIMUM TREE SIZE IS 2" CALIPER MEASURED 4" ABOVE ROOT BALL, 8" MINIMUM HEIGHT.
8. STAKING IS OPTIONAL. RUBBER HOSE AND ROPE OR WIRE FOR STAKING IS NOT RECOMMENDED. NO WIRE OR ROPE IS TO BE IN DIRECT CONTACT WITH TRUNK. REMOVE ALL TRUNK WRAP, TREE STRAPS, AND STAKING WIRE OR ROPE AFTER ONE GROWING SEASON.
9. CUT WIRES ARE NOT PERMITTED IN THE STREET RIGHT-OF-WAY.
10. ALL TREES AND SHRUBS SHALL MEET THE NORMAL REQUIREMENTS FOR THE AMERICAN ASSOCIATION OF NURSERYMEN (AAN).
11. NEW AND EXISTING TREES ARE PERMITTED WITHIN SITE TRIANGLE, BUT MUST BE LINED UP TO 8' HEIGHT CLEARANCE PER ADA REQUIREMENTS.
12. SIMILAR CRITERIA FOR TREE PLACEMENT AND PRUNING UP SHOULD BE CONSIDERED AT DRIVEWAY/STREET INTERSECTIONS.
13. CONTRACTOR TO MAINTAIN CLEAR LEVEL BETWEEN 30" AND 72" ABOVE STREET. AREA MUST BE TREE OF LIMBS AND FOLIAGE FOR SAFE CROSS VISIBILITY.

TREE PROTECTION NOTES:

PROTECTIVE BARRICADES SHALL BE PLACED AROUND ALL PROTECTED TREES DESIGNATED TO REMAIN IN DEVELOPMENT AREA, PRIOR TO THE START OF DEVELOPMENT ACTIVITIES OR GRADING. PROTECTIVE BARRICADES SHALL REMAIN IN PLACE UNTIL DEVELOPMENT ACTIVITIES ARE COMPLETE OR CONSTRUCTION IN ACCORDANCE WITH STANDARDS SET FORTH IN THIS SECTION COMMENCES. THE AREA WITHIN THE PROTECTIVE BARRICADE SHALL REMAIN FREE OF ALL BUILDING MATERIALS, DIRT OR OTHER CONSTRUCTION DEBRIS. CONSTRUCTION TRAFFIC, STORAGE OF VEHICLES AND MATERIALS, AND GRADING SHALL NOT TAKE PLACE WITHIN THE DRIPLINE OF THE EXISTING TREES TO BE PROTECTED. BARRICADES SHALL BE ERECTED AT A MINIMUM DISTANCE FROM THE BASE OF PROTECTED TREES ACCORDING TO THE FOLLOWING STANDARDS:

- A. FOR TREES 10" OR LESS DBH, PROTECTIVE BARRICADES SHALL BE PLACED A MINIMUM DISTANCE OF 5' FROM THE BASE OF EACH PROTECTED TREE, OR OUTSIDE THE DRIPLINE, WHICHEVER IS GREATER.
- B. FOR TREES GREATER THAN 10" DBH, PROTECTIVE BARRICADES SHALL BE PLACED AT A MINIMUM DISTANCE EQUAL TO 10' FROM THE BASE OF THE PROTECTED TREE PLUS AN ADDITIONAL 1' FOR EACH ADDITIONAL 1" DBH GREATER THAN 10" DBH, OR OUTSIDE THE DRIPLINE, WHICHEVER IS GREATER.
- C. CONSTRUCTION ACCESS TO A SITE SHOULD OCCUR WHERE AN EXISTING OR PROPOSED ENTRANCE EXIST IS LOCATED.
- D. EXCEPT FOR DRIVEWAY ACCESS POINTS, SIDEWALKS, CURB AND GUTTER, NO PAVING WITH CONCRETE OR OTHER IMPERMEABLE MATERIALS WITHIN A TREE DRIPLINE SHALL BE ALLOWED.
- E. WHERE GRADING WITHIN A TREE DRIPLINE CANNOT BE AVOIDED.
- F. LIMIT CUT AND FILLS TO 1/4 TO 1/2 THE AREA WITHIN THE DRIPLINE.
- G. AVOID WHERE GRADING LEAVES ROOTS EXPOSED, CUT ROOTS CLEAN.
- H. WHERE GRADING LEAVES ROOTS EXPOSED, CUT ROOTS CLEAN.
- I. AVOID FILLING WITHIN THE DRIPLINE OF A TREE WITHOUT SOME MECHANISM TO ALLOW AIR AND WATER TO REACH THE ROOTS.

APPROX. EXIST. ROAD CL.
BEATTIES FORD RD
PUBLIC R/W VARIES (DB 4552, PG. 386)

PROP. 10' SIDEWALK W/
GREEN ZONE
(IMPROVEMENTS NEED TO BE
COORDINATED WITH NCDOT
ROAD IMPROVEMENT PLANS)

APPROX. LOCATION OF
TEMPORARY
CONSTRUCTION
EASEMENT

ISAACS GROUP
CIVIL ENGINEERING DESIGN AND SURVEYING

Project: LONG CREEK FAMILY ENTERTAINMENT
15605 N OLD STATESVILLE RD., HUNTERSVILLE, NC
Title: LANDSCAPE PLAN
File #20033-90.000 Date: 02/28/23 Project Egr: BTU
Design By: BTU
Drawn By: CBH
Scale: 1"=20'
8720 RED OAK BOULEVARD, SUITE 420
CHARLOTTE, N.C. 28217
PHONE (704) 527-3440 FAX (704) 527-8335

RZ2.0

Long Creek Family Entertainment
Neighbor Meeting held on June 24th, 2023
Location: 9339 Beatties Ford Rd

Attendees:

Concerns:

- Is noise going to be an issue and what parameters are being set in place?
 - We discussed that Mecklenburg County and Huntersville do not have set quiet hours. However, we will be respectful of noise levels and they will be monitored by us as owners. If ever we are too loud, we encourage the neighbors to come over, call or report.
- Will this business increase traffic levels?
 - There will be an increase in some traffic coming to the business and those coming to the business will typically stay for 1 or more hours keeping the number of vehicle “turns” low. The intersection improvement that is already in place by the NCDOT for Beatties Ford Rd/McCoy will help with traffic patterns.
- Will crime rates increase?
 - We do not believe that this business will attract additional crime to the area.
- Will patrons conduct themselves inappropriately?
 - As business owners, we have a moral and professional obligation to ensure the safety, wellbeing and appearance of our patrons and facility. We will address any issues should they arise.
- Will this rezoning decrease the property values of the neighbors directly around this property?

- We have not found any studies showing that rezoning devalues other neighbor properties and the neighbor could not provide us with any of their own research. For some locations, their properties will increase in value.

Positive Feedback:

- One neighbor expressed that this type of atmosphere (full family friendly) is needed more in the area and he is looking forward to being able to play volleyball and bring his family.
- Having a gathering space like this for families and clubs will be a great addition to the area especially with the new developments having little to no yard spaces.
- One neighbor stated that as a couple with kids, this will be a great place to spend time and let the kids enjoy the outside and meet new people.
- One neighbor suggested we reach out to the school in the future to partner with different classrooms/teachers for field trips to see the garden club and learn about growing plants.

Changes Suggested:

- Could a fence be installed along the back of the property to increase a neighbor buffer?
 - Yes, we will look into options to see if this is feasible and the plans show/call for screening trees along the property borders.
- Will there be natural materials used for seating outside?
 - We will look into options and think it's a great idea and fits the feel we're going for.
- The plan shows 16 parking spaces - will that be enough?
 - We believe it'll be enough for daily use and we do have allocated space for overflow parking on the property. With this suggestion, we will be contacting neighboring commercial facilities to inquire about using their parking lots on occasion.

Sign In

Name	Van Address
Will Eury	DAKE WALK 
Nancy Eury	
Zachary Jacobs	
Zachary & Owen Jacobs	
Shelley Bonanis	Huntersville
Shirley M. Hunt	
Brian Richards	Town of Huntersville
Amber Kovacs	Town of Huntersville
Robert Kovacs	207 Creechway
Stephen Fendall	Huntersville

Sign In

Address

CINDY HOUGH
JIM HUSTLER
Mark Nelson
Cheryl Nelson
Allisia Bergsman
Ron Collins
DAD Boone
Curt & Pam Phillips
Fay Cox
Denny Brett
Scott David
Alysa Shepard
Josh Shepard
Cory Neal





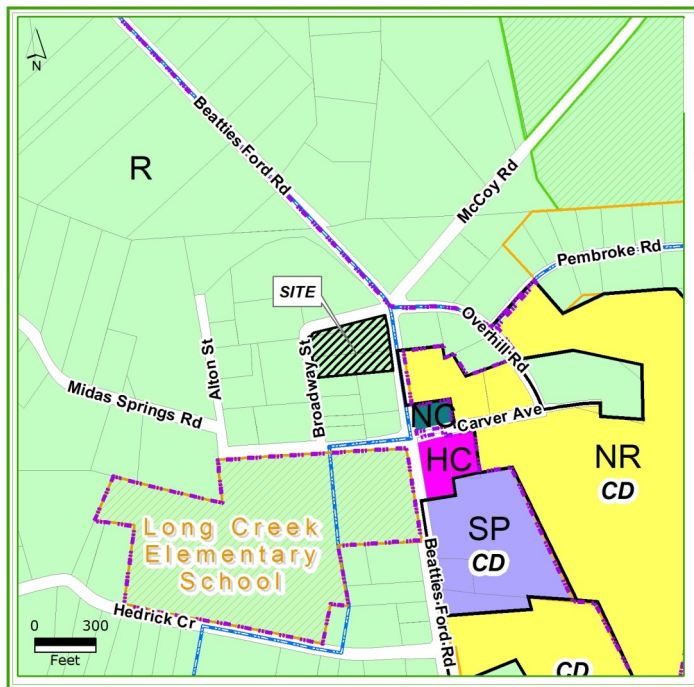

PO Box 664
Huntersville NC 28070

PUBLIC HEARING

Date: August 7, 2023
Time: 6:00 pm
Location: **In Person:** Huntersville Town Hall 101 Huntersville-Concord Rd.
Livestream Listen Only: <https://www.youtube.com/@townofhuntersvillenc28078/>
Applicant: Jonathan Eury
Case #: R23-06

Public Meeting Dates		
Meeting Type	Purpose	Date & Time
Community Meeting	Informational	June 24, 2023
Public Hearing	Public Meeting	August 7, 2023 @ 6 pm
Planning Board *	Recommendation	August 22, 2023 @ 6:30 pm
Town Board *	Approval/Denial	September 18, 2023 @ 6 pm
* Tentative—check www.huntersville.org for latest dates		

PUBLIC HEARING NOTICE DATE: August 7, 2023 | **R23-06** Beatties Ford Family Entertainment NOTICE OF PUBLIC HEARING FOR REZONING REQUEST



A Rezoning Petition has been submitted to rezone 2.513 acres from Rural (R) to Highway Commercial (HC) with Conditions (CD) to allow indoor and outdoor recreation with commercial uses. The “Site” (see inset map) is located south of Hambright Road, east of Everette Keith Road (Parcels # : 02305105, 02305106, 02305107).

A public hearing will be held in person at Town Hall located at 101 Huntersville-Concord Drive, Huntersville, NC 28078, and livestreamed to listen only at <https://www.youtube.com/@townofhuntersvillenc28078/streams>. The public is invited to attend in person if you wish to comment during the public hearing for this request. Please check the meeting agenda for all final meeting arrangements which may be adjusted to address public safety concerns as necessary at the time of the meeting.

YouTube Livestream:



Zoning Legend:

R = Rural
HC = Highway Commercial
NR = Neighborhood Residential

Site = Parcels requesting rezoning

NC—Neighborhood Center
SP = Special Purpose
[CD = Conditional District]

Project Page:



FOR ADDITIONAL INFORMATION:

CONTACT Nathan Farber AICP, Planner II

Phone: 704-766-2237

Email: nfarber@huntersville.org

Online: www.huntersville.org - search: **R23-06**

OFFICIAL TOWN OF HUNTERSVILLE PUBLIC HEARING NOTICE

**Town of Huntersville
Town Board
August 7, 2023**

To: Town Board

From: David Peete, Principal Planner

Date: August 7, 2023

Subject: Conduct Public Hearing - Petition #R23-07, EPCON Communities Carolinas, LLC

EXPLAIN REQUEST:

Conduct a public hearing

ACTION RECOMMENDED:

Conduct a public hearing

FINANCIAL IMPLICATIONS:

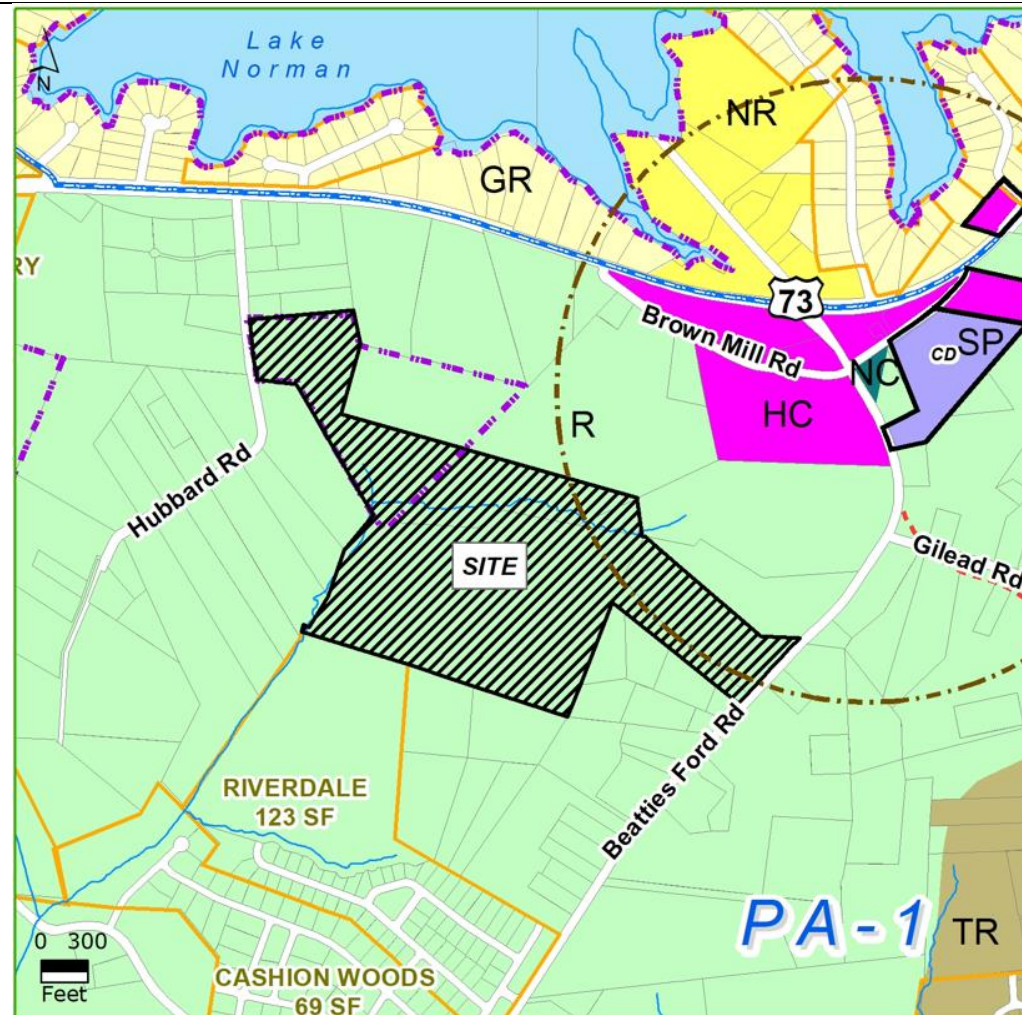
N/A

ATTACHMENTS:

1. R23-07 Public Hearing Staff Report (8-7-23)
2. Attachment A-1 - General Application (EPCON)
3. Attachment A-2 - General Application (Signature Addendum Browning)
4. Attachment B - EPCON - Beatties Ford Road (Courtyards at Walters Farm)
Rezoning & Sketch Plan 07.21.23
5. Attachment C - EPCON - Beatties Ford Rd Community Mtg summary 7.24.23

Petition R23-07 EPCON – Beatties Ford Road Conditional District (now titled “EPCON – Courtyards at Walters Farm”)

PART 1: PROJECT SUMMARY



R – Rural
TR – Transitional Residential
SP – Special Purpose
NR – Neighborhood Residential
GR – General Residential
HC – Highway Commercial

Applicant: EPCON Communities Carolinas, LLC.

Property Owner: Paul & Ruth Walters Family, LLC & Fred T. & Sandra R. Browning (see Attachment A).

Property Address: 15131 Beatties Ford Road.

Project Size: (+/-) 78.7-acres

Parcel Number(s):

01313125, 01313126, 01313142, 01313143, 01313144, 01313116.

Current Zoning: Rural (R).

Current Land Use: Large-lot, Single-Family Homes & vacant.

Proposed Zoning: Transitional Residential – Conditional District (TR - CD).

Proposed Land Use:

118 age-restricted (55+), single-family homes.

1. Purpose: To rezone 78.7-acres located west of Beatties Ford Road (near the intersection of Beatties Ford Road and Gilead Road) from Rural (R) to Transitional Residential – Conditional District (TR-CD), (see map above). The proposed rezoning is for a 118 age-restricted, single-family home subdivision. If the proposed rezoning is approved, a Subdivision Sketch Plan will be reviewed by staff for compliance.
2. Adjoining Zoning and Land Uses.
North: Rural (R) – a church (Gilead Church) & vacant.
South: Rural (R) – large-lot, single-family homes & one (1) new single-family home subdivision, currently under construction (Riverdale – Phase 2).
East: Rural (R) – Beatties Ford Rd. & large-lot, single-family homes.
West: Rural (R) – Large-lot, single-family residential.

3. One Community Meeting was held on Monday, July 24, 2023, at the Huntersville Arts & Cultural Center on Old Statesville Road. A Summary of the meeting is included in Attachment C.
4. Notice for this rezoning petition was given via postcards sent to adjoining property owners within 250 ft. of the project limits; a legal ad placed in the Charlotte Observer; and posting of rezoning signs on the property in two (2) locations.

PART 2: REZONING/SITE PLAN ISSUES

This proposed EPCON – Beatties Ford Road Conditional District Rezoning / Sketch Plan is generally compliant with the Zoning Ordinance and Subdivision Regulations, with significant elements as follows:

- Proposed principal use is a 118 age-restricted, single-family home subdivision.
- Three (3) Urban Open Spaces (Mini parks) are to be provided on site.
- Forty percent (40%) open space is the minimum required in the Transitional Residential district and 31.59-acres (40.1%) is proposed.
- Thirty-five percent (35%) tree save is the minimum required in the Transitional Residential district and 21.0-acres (35.9%) is proposed. Minimum required specimen tree save is 35% and 52.9% is proposed to be saved.
- Access is provided by one (1) main entry from Beatties Ford Road and a connection to Riverdale – Phase 2 (under construction). In addition, two (2) stubs are provided for future connections as adjacent properties redevelop.
- If approved, the portion of the subdivision along the north that is not within the Town limits would be offered for voluntary annexation.

ISSUES:

The applicant requests the following five (5) modifications to Ordinance requirements (see CD Rezoning Plan Sheet RZ-201.

- a) “Remove landscaped median requirement at the entrance of the subdivision.”
STAFF COMMENT: **Staff can support this modification request.** Per Article 3.2.2.d.2.i, “...a landscaped median at least 20 ft. in width shall be required at all entrances into the subdivision”. A landscaped median along Beatties Ford Road would not be in keeping with the rural esthetic of the corridor.
- b) “Increase the driveway width to 18 ft. for lots less than 60 ft. wide.”
STAFF COMMENT: **Staff does not support this modification request.** Per Article 8.16.3, “...lots 60 feet wide or less, driveways shall be no more than 14 feet wide as measured along the public street right-of-way for a detached house”. Developments throughout Town with lots under 60 feet in width function well with the 14 ft. limit. 2) With a proposed build-to range of 20 – 45 feet in depth for this development, there is sufficient room to maneuver vehicles.
- c) “Increase the maximum length of a cul-de-sac by +/- 470 ft. due to constraints imposed by existing easements.”
STAFF COMMENT: **Staff can support this modification request.** The total length of the cul-de-sac is 768 feet, which includes a gas line easement crossing. By deleting the 105 ft. easement width, the remaining cul-de-sac is 663 feet in length. Cul-de-sacs are limited to 350 feet in length.
- d) “Allow disturbance in the first 20 ft. of the undisturbed buffer were noted on the plan. This disturbed area will be replanted according to the Zoning Ordinance and as shown on the site plan.”
STAFF COMMENT: **Staff does not support this modification request.** Per Article 7.5 of the Zoning Ordinance, “Any major residential subdivision abutting a property zoned residential or developed residential, not internal to a planned community” is required to have a buffer “40 feet minimum when density is two times greater than the existing development. This buffer standard was adopted in March of this year and is intended to protect

existing development. The 2040 Community Plan recommends encouraging open space and tree preservation and preserving 40 feet of undisturbed buffer along the subdivision edge will further that goal.

- e) “Allow a wet pond, rather than traditional water quality measures, to be used for the density of the site.”
STAFF COMMENT: **Staff can support this modification request.** Article 8.17.13 of the Zoning Ordinance (Low Impact Development (LID) Approach) states that “the use of LID BMP’s is required by this Ordinance unless mitigation practices are approved and implemented”. The Town can work with the applicant to utilize acceptable alternative techniques to meet the intent of the Water Quality Ordinance and provide desired outcome for the development.

OTHER SITE PLAN ISSUES:

1. Per Article 5.5 – Elements of Street Design – part d.3. requires that “an on-street parking lane on at least one side of the street is required on streets serving ... detached houses with lots 60 ft. or less in width”. Per the diagram on Sheet RZ-201, the majority of lots do not front the required 57 ft. width street cross-section. In addition, Town streets are 51 ft. without on-street parking or 57 ft. with on-street parking. 50 ft. and 55.5 ft. are shown on plans, respectively, and must be revised.
2. A berm is proposed within the 100 ft. buffer along Beatties Ford Road, to be installed subject to the requirements of Article 7.4.2.g. This includes approval by the Planning Board.

PART 3: TRANSPORTATION ISSUES

A TIA Determination of Need form for the development was submitted on April 13, 2023, and on April 19, 2023, it was determined the Town would not require a TIA. However, NCDOT did require a TIA and the following improvements are to be installed:

- 150 ft. left turn at proposed development entrance.
- 100 ft. right turn at proposed development entrance.

In addition, the Town finds the entry road width at Beatties Ford Road unacceptable and needs to be limited to 26 ft. maximum.

All outstanding redline comments must also be addressed.

PART 4: REZONING CRITERIA

Article 11.4.7(d) of the Zoning Ordinance states that “in considering any petition to reclassify property, the Planning Board in its recommendation and the Town Board in its decision shall take into consideration any identified relevant adopted land-use plans for the area including, but not limited to, comprehensive plans, strategic plans, district plans, area plans, neighborhood plans, corridor plans, and other land-use policy documents”.

The current Zoning Map (shown above) indicates the area of this request is in the Rural zoning district, with a portion of the entry area also located within an Activity Center.

The 2040 Huntersville Community Plan could support this project through the following sections:

- **Policy LU-2: Encourage residential development that follows the pattern outlined in the future land use map.**
 - LU 2.2: Lower intensity residential uses are expected within the Residential Edge and Rural Conservation areas identified on the Future Land Use Map.

STAFF COMMENT: While both the Rural Conservation and Residential Edge areas would both be considered low intensity; the future land use map extended the Residential Edge designation to the outer limits of the Activity Center boundary. Per the 2040 Community Plan, “Planned Activity Centers include a mix of non-residential uses

and are usually located at key intersections of major or minor thoroughfares. “Residential uses include a mix of housing types centered around shopping, service or civic uses. Residential uses transition to lower gross density with more open space away from Activity Centers. This boundary is not specific, but rather indicates the extent of a ¼ mile walkable distance. This proposed development does not connect to the current uses within the Activity Center. Once outside of the Activity Center, the Future Land Use Map indicates Rural Conservation should be preserved.

- **Policy LU-6: Support a mix of land uses in key locations.**

- LU 6.1: A mix of land uses is encouraged in Mixed Use Centers, Activity Centers, Employment Centers identified on the Future Land Use Map.

STAFF COMMENT: The portion of this subdivision, if developed under Rural zoning, would provide low-density housing at the outer edge of an Activity Center. At this time, there is no connection between the proposed subdivision and the rest of the Activity Center.

- **Policy LU-9: New residential development should follow appropriate housing design principles.**

- LU 9.2: Within lower intensity areas including Moderate Density, Residential Edge, Rural Conservation, and Critical Watershed areas conservation design & farmhouse clusters are encouraged.
 - Scenic nature of roadways should be preserved
 - Development should be clustered away from key natural features.
 - Site design should minimize grading and maximize preservation of existing stands of mature, native trees.

STAFF COMMENT: The 100 ft. buffer along Beatties Ford Road will serve to protect the road’s historic character and hide the differing house-pattern behind a landscaped berm. The homes are located somewhat close to stream buffers but are not close enough to impact them. And while there are several stands of significant trees located along the entry area, the development is meeting the minimum TR standard for tree preservation. It should be noted that the R zone has a higher standard of tree preservation.

- **Policy LU-10: Encourage a diversity of housing options.**

- LU 10.1: Align housing options with resident needs and promote attainable housing options.
 - Accommodate a mix of housing by type, tenure, and location to serve a growing and increasingly diverse population. Housing offerings should align with workforce opportunities, including management, professional positions, and service positions.
- LU 10.2: Continue to encourage a mix of lot sizes in new developments.
- LU 10.4: Consider allowing additional flexibility in site design in exchange for more quality open space preservation to allow for conservation of natural resources in the Transitional and Rural zoning districts.

STAFF COMMENT: The proposed subdivision consists of age-restricted, single-family homes, which contributes to the mix of housing within town. There are also three (3) different lots sizes, consisting of 55 ft., 68 ft. and 78 ft. wide lots, however, only 7 of the 118 lots are 78 ft. wide.

- **Policy LU-12: Preserve historic structures and landscapes in Huntersville.**

- LU 12.2: Utilize notable projects list from the Architectural Survey, State Historic Preservation Office (SHPO) data, and other resources during design and development review.
- LU 12.3: Blend new development with existing neighborhoods, structures and landscapes through the use of transitions in building types and placement of open space, buffers, and other site features.

STAFF COMMENT: The Gilead Church, located near the entrance along Beatties Ford Road, has been identified as historically significant and the (min.) 40 ft. buffer along the shared border with this church and its cemetery will play a critical role in protecting this community asset.

- **Policy EOS-2: Encourage conservation subdivision design in Residential Edge and Rural Conservation areas.**
 - EOS 2.1: Continue to require and incentivize open space reservation in Moderate Density, Residential Edge, Rural Conservation, and Critical Watershed areas.
 - Encourage new development to have at least 40% open space in new development in these areas
 - The Residential Edge and Rural Conservation areas on the Future Land Use map are associated with the Transitional and Rural zoning districts. These zoning districts offer a sliding scale in allowable density depending on the amount of open space preserved.
 - EOS 2.2: In the Transitional and Rural zoning districts, consider allowing additional flexibility in site design in exchange for more quality open space preservation, which promotes conservation of natural resources.

STAFF COMMENT: The subdivision proposes the minimum amount of open space (40.1%) and tree preservation.

- **Policy EOS-3: Prioritize tree canopy preservation in the lower intensity areas (Residential Edge, Rural Conservation, and Critical Watershed areas).**

STAFF COMMENT: This subdivision proposes to save 52.9% of existing specimen trees and 35% of existing canopy. The current Rural zoning district requires 50% specimen tree save and 50% existing tree canopy, which goes further to prioritize tree canopy preservation.

- **Policy EOS-6: Preserve elements of rural character.**
 - EOS 6.1: Enforce existing standards and evaluate new design standards to preserve the character of scenic country roads.
 - McCauley Road, Black Farms Road, Beatties Farm Road, and Ramah Church Road have been identified as scenic resources and should have corridor-specific design controls that preserve scenic beauty.
 - For instance, the planned cross-section for Beatties Ford Road includes a 100ft buffer and multi-use trail

STAFF COMMENT: The subdivision has a 100-ft. wide buffer along the frontage of Beatties Ford Road to preserve the rural character of the corridor. A landscaped berm will be planted within this buffer, as there is very little existing vegetation in that area.

- **Policy EOS-10: Improve bicycle and pedestrian facilities throughout Town.**
 - EOS 10.1: Implement the Bicycle and Pedestrian Committee's 30-by-30 plan.
 - Connect all parks, schools, neighborhoods, major shopping into the Greenway System by 2030 incrementally over the next 10 years.
 - Include Greenways, sidewalks, multi-use paths, trails, and dirtways.

STAFF COMMENT: The goals of the 30 x 30 Bike and Pedestrian Plan are furthered by the provision of a 10 ft. wide sidepath along the frontage of Beatties Ford Road. There are no public greenway linkages through this area.

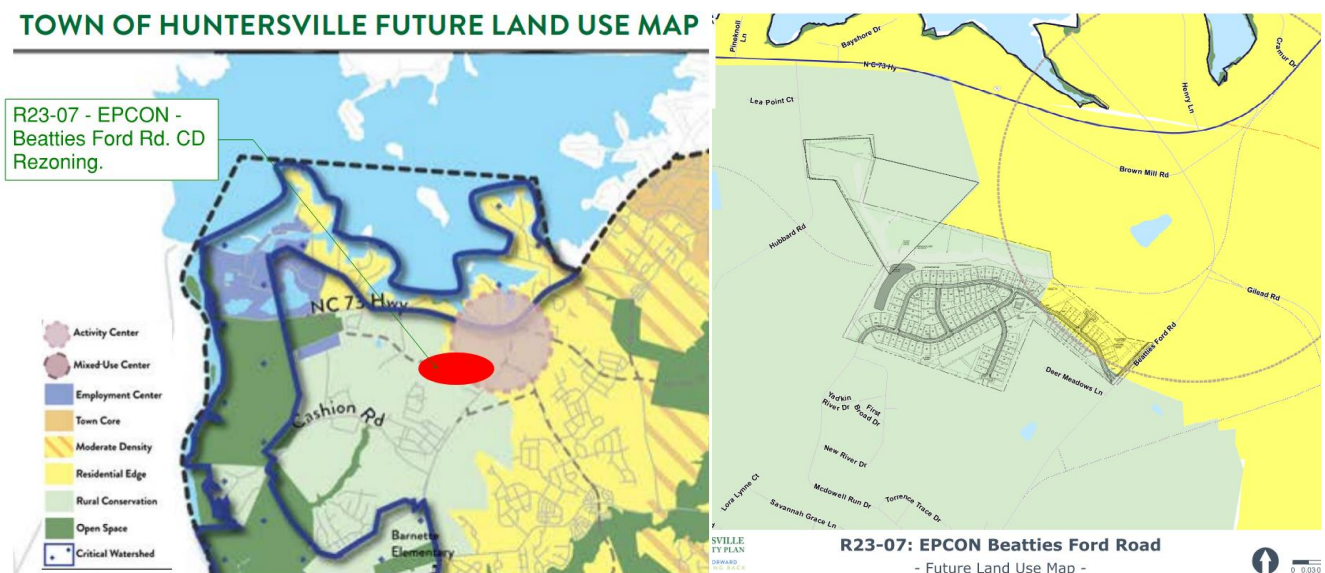
- **Policy T-3: Improve connectivity throughout the study area.**

STAFF COMMENT: Access is provided by one (1) main entry from Beatties Ford Road and a connection to Riverdale – Phase 2 (under construction). In addition, two (2) stubs are provided for future connections as adjacent properties redevelop.

The 2040 Huntersville Community Plan **does not support** this project through the following sections:

- **Policy LU-1: Encourage a development pattern that follows the Future Land Use Map.**
 - LU 1.1: Utilize the Future Land Use Map during development approval process to ensure compatibility with long-range plans.

STAFF COMMENT: The parcels requested to be rezoned are shown below. The majority of the subdivision is zoned Rural (R) and is located in the 2040 Community Plan's Rural Conservation designation. The request is to rezone the property to Transitional Residential (TR), which is not adjacent, nor located anywhere on the west side of Beatties Ford Road. Within the Future Land Use Map, the Residential Edge designation – which would accommodate the TR zoning district – is adjacent to the properties. The majority of the Residential Edge area overlaid onto the parcels that make up the Activity Center shown on the Future Land Use Map (see circle area, below). The Residential Edge designation was not carried over to the parcels west of Beatties Ford Road, to limit the level of development within this very rural area.



- **Policy LU-3: Manage residential growth in the eastern and western parts of Huntersville's planning jurisdiction.**
 - LU 3.1: Discourage rezonings to higher intensity residential districts in the Residential Edge and Rural Conservation future land use character areas.
 - There is constant pressure to rezone to higher density districts on the edges of town. Growth management was the #1 priority for survey responses. There needs to be a concerted effort to uphold previous policy decisions to limit density and increase open space preservation in the more undeveloped areas outside of the Town Core.

STAFF COMMENT: Again, once the TR zoning district is introduced on the west side of Beatties Ford, with the available acreage that is vacant or under-developed, there will be more pressure to rezone additional properties.

- **Policy LU-7: Require new development to follow design principles that reinforce the vision for the Town as expressed in this plan and other adopted plans.** The town has committed to traditional town planning and urban design principles that are meant to preserve the character of the town. This commitment is noted in adopted plans and the zoning ordinance and has been expressed in new development over the last 25 years.
 - LU 7.1: Require all new development to adhere to the following design principles:
 - In lower intensity areas (including MD, RE, RC, CW) preservation of rural character and natural resources are prioritized.
 - In these areas, structures can be set back further from the road and should blend into the landscape and the scenic nature of roadways should be preserved.

STAFF COMMENT: The current Rural zoning district requires a minimum open space reservation of 45%. This subdivision proposes 40% open space, including the Urban Open Space areas, which is the minimum for the TR zone, but is not in keeping with the Rural Conservation goal of preservation of rural character and natural resources.

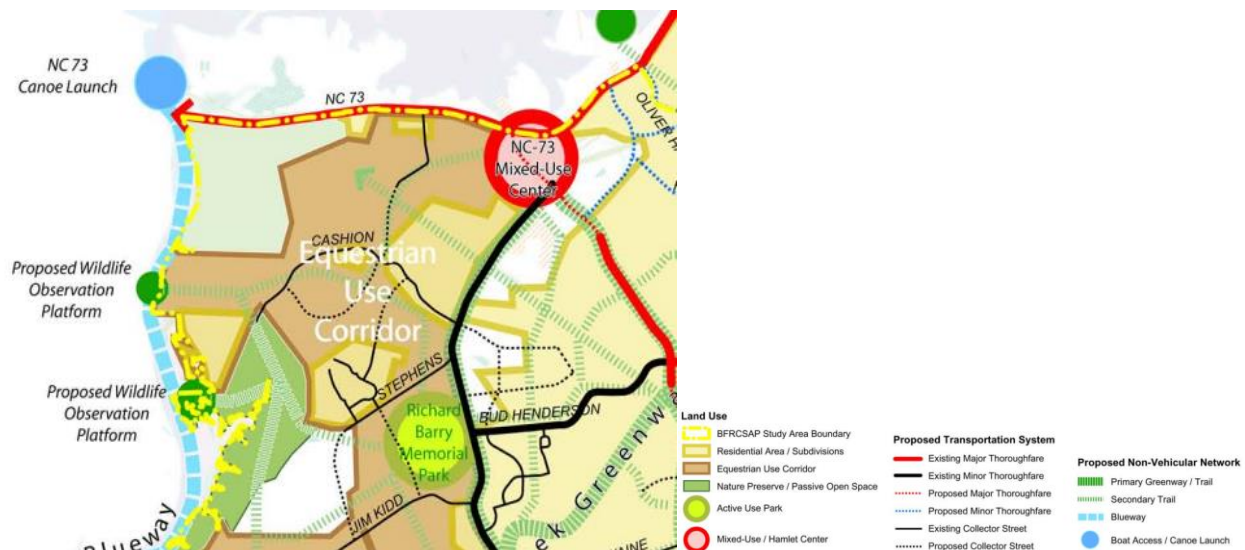
- **Policy LU-11: Protect Existing Housing Stock.**
 - LU 11.2: Along existing streets, encourage new buildings to respect the general spacing of structures, building mass and scale, and street frontage relationships of existing buildings.

STAFF COMMENT: While the proposed lot pattern and lot size are not in keeping with the majority of the existing housing, the lot pattern is similar to the Riverdale – Phase 2 development. Without the appropriate buffers along the exterior project boundaries, this development would not respect the existing development pattern.

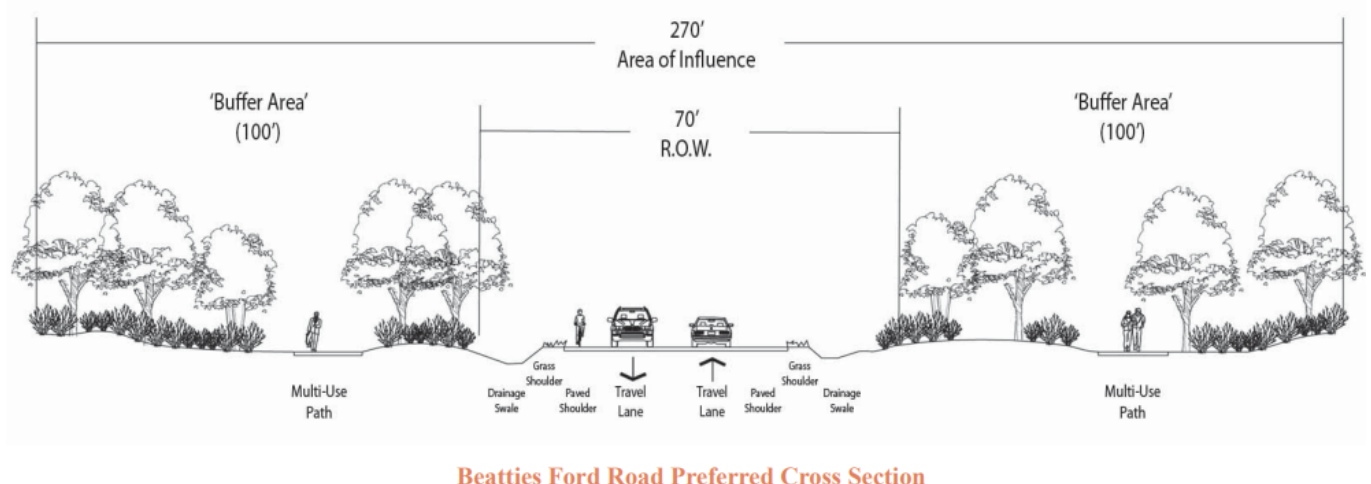
The Beatties Ford Road Corridor Small Area Plan (SAP) (adopted 2007) addresses this request as follows:

The proposed EPCON – Beatties Ford Road development is located in the “Residential Area / Subdivisions” (shown in beige, below) area.

STAFF COMMENT: Section 7.2 – Land Use and Zoning, of the Small Area Plan, recommends to “continue the low-density development pattern within the study area”.



The future cross-section for Beatties Ford Road is shown below and the proposed road improvements in the CD Rezoning / Sketch Plan are consistent with what is shown.



Article 11 Section 11.4.7(e) of the Zoning Ordinance states that: “in considering any petition to reclassify property the Planning Board in its recommendation and the Town Board in its decision should consider:

1. Whether the proposed reclassification is consistent with the overall character of existing development in the immediate vicinity of the subject property.

STAFF COMMENT:

The proposed EPCON – Beatties Ford Road - Conditional District Rezoning is not supported by the 2040 Community Plan, which calls for the majority of the property to be Rural Conservation, which the existing Rural zoning district most-directly lines-up with. This support is due to development being limited to 0.9-units per acre with a maximum of 45% open space preservation. Rezoning to TR would increase the density in this area to 1.5 units per acre, while reducing minimum required open space to 40%. Tree-save percentage is also reduced in TR, which is not supported by the 2040 Community Plan. Of primary concern is the introduction of TR zoning west of Beatties Ford Road where none exists. The closet TR zoning is located to the east of Beatties Ford Road. Once a pattern of increased-density development is established, a precedent for similar development along the corridor will follow, as there is a significant amount of vacant or under-developed property in the general area. 2040 Community Plan Implementation Policy LU-3.1 states “there is constant pressure to rezone to higher density districts on edges of town. Growth management was the #1 priority for survey responses. There needs to be a concerted effort to uphold previous policy decisions to limit density and increase open space preservation in the more undeveloped areas outside of the Town Core”.

2. The adequacy of public facilities and services intended to serve the subject property, including but not limited to roadways, transit service, parks and recreational facilities, police and fire protection, hospitals and medical services, schools, storm water drainage systems, water supplies, and wastewater and refuse disposal.

STAFF COMMENT:

- A Transportation Impact Analysis (TIA) was not required by the Town for this rezoning, however NCDOT did require transportation improvements – see Part 3 of this report.
- A Willingness-to-serve letter from Charlotte Water was issued by Charlotte Water on 5-5-23.
- A Conceptual Storm Water Drainage Plan (PCO-1) is under review and must be approved by staff.
- The CD Rezoning Plan was sent to Charlotte-Mecklenburg School (CMS) for consideration (see Attachment D).

3. Whether the proposed reclassification will adversely affect a known archeological, environmental, historical or cultural resource.”

STAFF COMMENT:

Planning staff has no indication that the request will adversely affect known archeological, environmental, historical or cultural resources.

PART 5: STAFF RECOMMENDATION

The EPCON – Beatties Ford Road Conditional District Rezoning Plan from Rural (R) to Transitional Residential – Conditional District (TR-CD) is not supported by staff for the reasons outlined in Part 4 of this report. If the Town Board were to rezone the property, as proposed, the following conditions should apply:

- Staff can support modification “a” – (entry median).
- Staff **does not** support modification “b” (increased driveway width).
- Staff can support modification “c” (cul-de-sac length).
- Staff **does not** support modification “d” (buffer disturbance).
- Staff does support modification “e” (wet pond).
- On-street parking must be provided on (at least) one side for all lots under 60 feet in width.
- All outstanding redline comments must be addressed.
- RECOMMEND – Add a walking trail throughout the subdivision.

PART 6: PUBLIC HEARING COMMENTS

Public Hearing scheduled for Monday, August 7, 2023.

PART 7: PLANNING BOARD RECOMMENDATION

Planning Board scheduled to review on August 22, 2023.

PART 8: SCHEDULED FINAL TOWN BOARD ACTION

Final Action scheduled for September 18, 2023.

PART 9: ATTACHMENTS/ENCLOSURES

Attachments

- A – General Application (Rezoning).
- B – EPCON – Beatties Ford Road CD Rezoning Plan.
- C – Community Meeting Report from July 24, 2023 – to be provided prior to public hearing.
- D – CMS Report – to be provided prior to public hearing.

PART 10: CONSISTENCY STATEMENT - R 23-07 EPCON – Beatties Ford Road Conditional District Rezoning.

Planning Department	Planning Board	Board of Commissioners
APPROVAL:	APPROVAL: In considering the proposed rezoning application R23-07; EPCON – Beatties Ford Road CD Rezoning, the Planning Board recommends approval based on the Plan being consistent with <u>(insert applicable plan reference)</u>. <u>It is reasonable and in the public interest to approve the Rezoning Plan because... (Explain)</u>	APPROVAL: In considering the proposed rezoning application R23-07; EPCON – Beatties Ford Road CD Rezoning, the Town Board recommends approval based on the Plan being consistent with <u>(insert applicable plan reference)</u>. <u>It is reasonable and in the public interest to approve the Rezoning Plan because... (Explain)</u>
DENIAL: In considering the proposed rezoning application R23-07; EPCON – Beatties Ford Road Conditional District Rezoning, Town Staff DOES NOT RECOMMEND APPROVAL of the rezoning as it is not consistent with Implementation Goals LU-1, LU-3, LU-7, & LU-11 of the 2040 Community Plan. <u>It is not reasonable, nor in the public interest to rezone these 78.7-acres from Rural (R) to Transitional Residential (TR) to Corporate Business – Conditional District (CB-CD) BECAUSE it would be inconsistent with the 2040 Community Plan.</u>	DENIAL: In considering the proposed rezoning application R23-07; EPCON – Beatties Ford Road CD Rezoning, the Planning Board recommends denial based on the Plan being <u>(consistent OR inconsistent) with (insert applicable plan reference)</u>. <u>It is not reasonable and in the public interest to approve the Rezoning Plan because... (Explain)</u>	DENIAL: In considering the proposed rezoning application R23-07; EPCON – Beatties Ford Road CD Rezoning, the Town Board recommends denial based on the Plan being <u>(consistent OR inconsistent) with (insert applicable plan reference)</u>. <u>It is not reasonable and in the public interest to approve the Rezoning Plan because... (Explain)</u>



General Application

INCOMPLETE SUBMISSIONS WILL NOT BE ACCEPTED. PLEASE CHECK ALL ITEMS CAREFULLY.

1. Application Type

Please indicate the type of application you are submitting. In addition to the application, the submission process for each application type can be found at <https://www.huntersville.org/528/Permits-Process>

- ☐ Change of Use
- ☐ Commercial Site Plan
- ☒ Conditional Rezoning
- ☐ General Rezoning
- ☐ Master Signage Program
- ☐ Special Use Permit
- ☐ Revision to
Original Project # _____
- ☐ Other _____

SUBDIVISION CATEGORIES: Per the
Huntersville Subdivision Ordinance

- ☒ Sketch Plan
- ☐ Preliminary Plan
- ☐ Final Plat (Includes Minor Subdivision)
- ☐ Exempt Subdivision
- ☐ Final Plat Revision
- ☐ Farmhouse Cluster

2. Project Data

Date of Application 04-25-2023

Name of Project Beatties Ford Road Residential Phase # (if subdivision) _____

Project Address 15201 Beatties Ford Road, Huntersville, NC 28078

Parcel Identification Number(s) (PIN) 01313125, 01313126, 01313142,
01313143, 01313144 & 01313116

Current Zoning District R Proposed District (for rezoning only) TR

Property Size (acres) 78.7 AC Street Frontage (feet) 574 ft

Current Land Use Vacant / Single Family Residential

Proposed Land Use(s) Single Family Detached Residential

Is the project within Huntersville's corporate limits?

Yes X No _____ If no, does the applicant intend to voluntarily annex? _____

3. Description of Request

Explain the nature of this request. If a separate sheet is necessary, please attach to this application.

Proposed Conditional District Rezoning from R to TR

4. Site Plan Submittals

Consult the particular type of *Review Process* for the application type selected above. These can be found at <https://www.huntersville.org/528/Permits-Process>.

5. Outside Agency Information

Other agencies may have applications and fees associated with the land development process. The *Review Process* list includes plan documents needed for most town and county reviewing agencies. For major subdivisions, commercial site plans, and rezoning petitions please enclose a copy of the Charlotte-Mecklenburg Utility *Willingness to Serve* letter for the subject property.

6. Applicant

Printed Name Epcon Communities Carolinas, LLC Phone 704-607-0152
☐ Corporation ☒ Limited Liability Company ☐ Trust ☐ Partnership ☐ Other: _____

☒ By signature below, I hereby acknowledge, as/on behalf of (circle one) the applicant my understanding this application will be considered in a quasi-judicial proceeding and that neither I, nor anyone on my behalf, may contact the Board of Commissioners except through sworn testimony at the public hearing. (Applicable for Special Use Permits and Subdivisions)

Signature Andy Gibbon Printed Name: Andy Gibbon

Title Land Development Director Email agibbon@epconcommunities.com

Address of Applicant 11020 David Taylor Drive, Suite 105, Charlotte, NC 28262

7. Property Owner (if different than applicant)

*Printed Name Paul & Ruth Walters Family LLC Phone _____
☐ Corporation ☒ Limited Liability Company ☐ Trust ☐ Partnership ☐ Other: _____

☐ By signature below, I hereby acknowledge, as/on behalf of (circle one) the owner my understanding this application will be considered in a quasi-judicial proceeding and that neither I, nor anyone on my behalf, may contact the Board of Commissioners except through sworn testimony at the public hearing. (Applicable for Special Use Permits and Subdivisions)

Signature Paul Walters Printed Name PAUL S. WALTERS

Title Mgr. Email Jim@LWENGINEERS.COM

Address of Property Owner 102 Sherwood Drive, Huntersville, NC 28078

* Property owner hereby grants permission to the Town of Huntersville personnel to enter the subject property for any purpose required in processing this application.

Every owner of each parcel included in this application, or the owner (s) duly authorized agent, must sign this application. If signed by an agent on behalf of the Owner, this application MUST be accompanied by a notarized Limited Power of Attorney signed by the property owner (s), specifically authorizing the agent to act on the owner (s) behalf in signing this application. Failure of each owner, or their duly authorized agent, to sign, or failure to include the authority of the agent signed by the property owner, will result in an INVALID APPLICATION. If additional space is needed for signatures, attach the Town of Huntersville Signature Addendum Form.

8. Development/Design Firm Contact Information

Bowman Development Group	Whitney Hodges	704-929-8396	whitneyhodges@gmail.com
Development Firm	Name of Contact	Phone	Email
Timmons Group	Andrew Allison	704-227-1564	andrew.allison@timmons.com
Design Firm	Name of Contact	Phone	Email

Contact Information

Town of Huntersville	Phone:	704-875-7000
Planning Department	Fax:	704-992-5528
PO Box 664	Physical Address:	105 Gilead Road, Third Floor
Huntersville, NC 28070	Website:	https://www.huntersville.org/228/Planning-Department



General Application
Owner/Applicant Signature Addendum

Application Information

Date of Application 04-25-2023 Application Number _____

Name of Project Beatties Ford Road Residential Phase # (if subdivision) _____

Additional Owners/Applicants: (Signature indicates intent that this page be affixed to Application.)

* ^ Printed Name Fred T & Sandra R Browning Phone Number 704-408-3673
☐ Corporation ☐ Limited Liability Company ☐ Trust ☐ Partnership ☒ Other: _____

☐ By signature below, I hereby acknowledge, as/on behalf of (circle one) the applicant/owner (circle one) my understanding this application will be considered in a quasi-judicial proceeding and that neither I, nor anyone on my behalf, may contact the Board of Commissioners except through sworn testimony at the public hearing. (Applicable for Special Use Permits and Subdivisions)

Signature Fred T. Browning Parcel ID(s): 01313125

Title Owner Email Browningf@roadrunner.com

Address of Property Owner/Applicant 15201 Beatties Ford Rd, Huntersville, NC 28078

* ^ Printed Name Fred T & Sandra R Browning Phone Number _____
☐ Corporation ☐ Limited Liability Company ☐ Trust ☐ Partnership ☐ Other: _____

☐ By signature below, I hereby acknowledge, as/on behalf of (circle one) the applicant/owner (circle one) my understanding this application will be considered in a quasi-judicial proceeding and that neither I, nor anyone on my behalf, may contact the Board of Commissioners except through sworn testimony at the public hearing. (Applicable for Special Use Permits and Subdivisions)

Signature _____ Parcel ID(s): 01313125

Title _____ Email _____

Address of Property Owner/Applicant 15201 Beatties Ford Rd, Huntersville, NC 28078

* ^ Printed Name _____ Phone Number _____
☐ Corporation ☐ Limited Liability Company ☐ Trust ☐ Partnership ☐ Other: _____

☐ By signature below, I hereby acknowledge, as/on behalf of (circle one) the applicant/owner (circle one) my understanding this application will be considered in a quasi-judicial proceeding and that neither I, nor anyone on my behalf, may contact the Board of Commissioners except through sworn testimony at the public hearing. (Applicable for Special Use Permits and Subdivisions)

Signature _____ Parcel ID(s): _____

Title _____ Email _____

Address of Property Owner/Applicant _____

* Property owner hereby grants permission to the Town of Huntersville personnel to enter the subject property for any purpose required in processing this application.

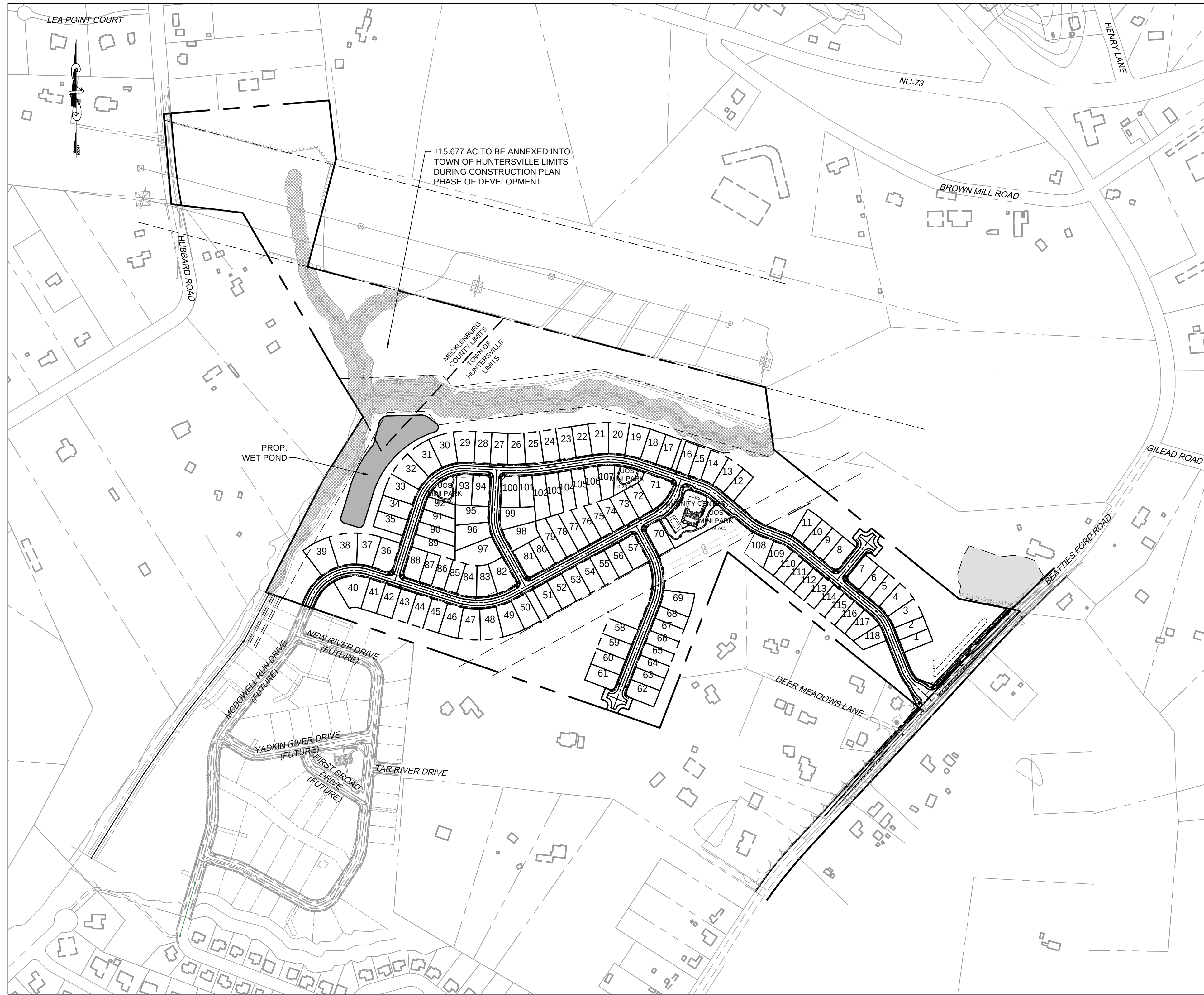
^ If signed by an agent on behalf of the Owner, this petition MUST be accompanied by a Limited Power of Attorney signed by the property owner (s) and notarized, specifically authorizing the agent to act on the owner (s) behalf in signing this application. Failure of each owner, or their duly authorized agent, to sign, or failure to include the authority of the agent signed by the property owner, will result in an INVALID APPLICATION.

EPCON - COURTYARDS AT WALTERS FARM

CONDITIONAL DISTRICT REZONING / SKETCH PLAN

15131 BEATTIES FORD RD
HUNTERSVILLE, NORTH CAROLINA

EPM PROJECT NO. 449924
REZONING NO. R23-07



VICINITY MAP
SCALE: 1" = 250'

Sheet List Table	
Sheet Number	Sheet Title
RZ-000	COVER
RZ-100	EXISTING CONDITIONS
RZ-101	EXISTING SLOPE ANALYSIS
RZ-102	TREE SURVEY
RZ-103	ADJACENT PROPERTY OWNERS
RZ-104	ADJACENT PROPERTY OWNERS INFORMATION & TREE LIST
RZ-105	FOUR STEP DESIGN PROCESS
RZ-200	REZONING PLAN
RZ-201	SITE NOTES AND DETAILS
RZ-202	SITE NOTES AND DETAILS
RZ-300	CONCEPTUAL GRADING & DRAINAGE PLAN
RZ-400	CONCEPTUAL PLANTING PLAN
RZ-500	CONCEPTUAL URBAN OPEN SPACE PLAN

APPROVAL OF THIS SKETCH / CONCEPT PLAN DOES NOT IMPLY OR GUARANTEE APPROVAL AND / OR VESTING OF THE FINAL PRELIMINARY / CONSTRUCTION PLAN. FINAL PRELIMINARY / CONSTRUCTION PLAN WILL BE REVIEWED FOR COMPLIANCE PER ALL TOWN, COUNTY, AND STATE REGULATIONS IN EFFECT AT TIME OF SUBMITTAL.

PROPERTY OWNER INFORMATION

PARCEL ID: 01313125
FRED & SANDRA BROWNING
15201 BEATTIES FORD ROAD, HUNTERSVILLE, NC 28078

PARCEL ID'S: 01313116, 01313126, 01313142, 01313143 & 01313144
PAUL & RUTH WALTERS FAMILY LLC
102 SHERWOOD DRIVE, HUNTERSVILLE, NC 28078

REQUIRED NCDOT ROAD IMPROVEMENTS FOR BEATTIES FORD ROAD

150' LEFT TURN LANE AT PROPOSED DEVELOPMENT ENTRANCE
100' RIGHT TURN LANE AT PROPOSED DEVELOPMENT ENTRANCE



PRELIMINARY
FOR REVIEW
PURPOSES ONLY

THIS DRAWING PREPARED AT THE
CHARLOTTE OFFICE
610 E. Morehead Street, Suite 250 | Charlotte, NC 28202
TEL 704.602.8600 FAX 704.376.1076 www.timmons.com
North Carolina License No. C-1652

EPCON[®]
COMMUNITIES
11020 DAVID TAYLOR DR, SUITE 105
CHARLOTTE, NC 28262

REVISION DESCRIPTION

REVISED PER TOWN COMMENTS

DATE

DATE

07/21/2023

DRAWN BY

A. CLARK

DESIGNED BY

A. ALLSION

CHECKED BY

A. ALLSION

SCALE

AS SHOWN

YOUR VISION ACHIEVED THROUGH OURS.

TIMMONS GROUP

EPCON - COURTYARDS AT WALTERS FARM
HUNTERSVILLE, NORTH CAROLINA

JOB NO.

57770

SHEET NO.

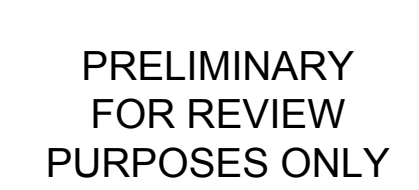
RZ-000



- CONTRACTOR IS FULLY RESPONSIBLE FOR CONTACTING APPROPRIATE PARTIES AND ASSURING THAT EXISTING UTILITIES ARE LOCATED PRIOR TO CONSTRUCTION.
- CONTRACTOR IS RESPONSIBLE FOR PLACING BARRICADES USING FLAG MEN ETC. AS NECESSARY TO INSURE SAFETY TO THE PUBLIC.
- ALL FURNISHED CUTS, CONCRETE OR ASPHALT ARE TO BE REPLACED ACCORDING TO STANDARDS OF THE NORTH CAROLINA DEPARTMENT OF TRANSPORTATION AND TOWN OF HUNTERSVILLE UTILITIES SPECIFICATIONS.
- SHORING WILL BE ACCORDING TO OWNER TRENCHING STANDARDS PART 108 SUBPART F, OR AS AMENDED.



1. CONTRACTOR IS FULLY RESPONSIBLE FOR CONTACTING APPROPRIATE PARTIES AND ASSURING THAT EXISTING UTILITIES ARE LOCATED PRIOR TO CONSTRUCTION.
2. CONTRACTOR IS RESPONSIBLE FOR PLACING BARRICADES USING FLAG MEN, ETC. AS NECESSARY TO INSURE SAFETY TO THE PUBLIC.
3. ALL PAVEMENT CUTS, CONCRETE OR ASPHALT, ARE TO BE REPLACED ACCORDING TO STANDARDS OF THE NORTH CAROLINA DEPARTMENT OF TRANSPORTATION AND TOWN OF HUNTERSVILLE UTILITIES SPECIFICATIONS.
4. SHORING WILL BE ACCORDING TO OSHA TRENCHING STANDARDS.



THIS DRAWING PREPARED AT THE
CHARLOTTE OFFICE
610 E. Morehead Street, Suite 250 | Charlotte, NC 28202
TEL 704.602.8600 FAX 704.376.1076 www.timmons.com
North Carolina License No. C-1652



EPCON COMMUNITIES
11020 DAVID TAYLOR DR, SUITE 105
CHARLOTTE, NC 28262

DATE	07/21/2023
DRAWN BY	A. CLARK
DESIGNED BY	A. ALLSION
CHECKED BY	A. ALLISON
SCALE	1" = 100'

YOUR VISION ACHIEVED THROUGH OURS.

TIMMONS GROUP

EPCON - COURTYARDS AT WALTERS FARM

HUNTERSVILLE, NORTH CAROLINA

EXISTING CONDITIONS

00	0	EXISTING CONDITIONS	these plans and associated documents are the exclusive property of TIMMONS GROUP and may not be reproduced in whole or in part and shall not be used for any purpose whatsoever, inclusive, but not
----	---	---------------------	---

JOB NO.
57770

SHEET NO.
RZ-100

S:\0457776-Business Farm Residential\Epcon\DWG\Sheet\Resizing\57776-C102-AJCL.dwg | Printed on 7/21/2023 2:12 PM | by Andy Clark



SCALE 1"=150'

SEE SHEET RZ-104 FOR ADJACENT PROPERTY OWNER INFORMATION

North Carolina 811

www.nc811.org

PRELIMINARY FOR REVIEW PURPOSES ONLY

THIS DRAWING PREPARED AT THE
CHARLOTTE OFFICE
 610 E. Morehead Street, Suite 250 | Charlotte, NC 28202
 TEL 704.602.8600 FAX 704.376.1076 www.timmons.com
 North Carolina License No. C-1652

EPCON[®]
 COMMUNITIES

EPCON COMMUNITIES
 11020 DAVID TAYLOR DR, SUITE 105
 CHARLOTTE, NC 28262

YOUR VISION ACHIEVED THROUGH OURS.

TIMMONS GROUP

EPCON - COURTYARDS AT WALTERS FARM
 HUNTERSVILLE, NORTH CAROLINA
 ADJACENT PROPERTY OWNERS

DATE
07/21/2023

DATE
07/21/2023

DRAWN BY
A. CLARK

DESIGNED BY
A. ALLSION

CHECKED BY
A. ALLSION

SCALE
1" = 150'

JOB NO.
57776

SHEET NO.
RZ-103

REVISION DESCRIPTION

REVISED PER TOWN COMMENTS

These plans and associated documents are the exclusive property of TIMMONS GROUP and may not be reproduced in whole or in part and shall not be used for any purpose whatsoever, inclusive, but not limited to construction, bidding, and/or construction taking without the express written consent of TIMMONS GROUP.

ADJACENT PROPERTY OWNERS				
PARCEL	PARCEL NO.	OWNER	MAILING ADDRESS	ZONING
1	01313114	WICKER, JOHN MWICKER, PATRICIA M	5827 DEER MEADOWS LANE HUNTERSVILLE NC 28078	R
2	01313132	DIETRICH, ERIC	5835 DEER MEADOWS LN HUNTERSVILLE NC 28078	R
3	01313128	TILLEY, KIMBERLY DTILLEY, KENNETH LEROY	5925 DEER MEADOWS LN HUNTERSVILLE NC 28078	R
4	01313127	DIGIOIA, DAVIDDIGIOIA, NANCY	16216 WALCOT LN CORNELIUS NC 28031	R
5	01313129	ADAMS, KAITLYN ANNEADAMS, JACOB LAWRENCE	15101 BEATTIES FORD RD HUNTERSVILLE NC 28078	R
6	01313130	SPERLING, BRANDON STEWARTSPERLING, MINDY J	5910 DEER MEADOWS LN HUNTERSVILLE NC 28078	R
7	01313131	GOTTS, A JEANGOTTS, ROBERT C	5826 DEER MEADOWS LN HUNTERSVILLE NC 28078	R
8	01312227	ANDREA LANIER, PUTNAM, RONALD GLENN JR	15027 BEATTIES FORD RD HUNTERSVILLE NC 28078	R
9	01312228	BURCH, DOROTHY F.BURCH, CARLISE	15025 BEATTIES FORD RD HUNTERSVILLE NC 28078	R
10	01312229	BROWNING, MITCHELL	15019 BEATTIES FORD RD HUNTERSVILLE NC 28078	R
11	01312282	MTS CLT LLC,	2857 WESTOIRT RD CHARLOTTE NC 28208	R
12	01319104	PEREZ, DAVIDAINSUE-PEREZ, REBECCA LEE	15510 HUBBARD RD HUNTERSVILLE NC 28078	R
13	01319115	ROLLO, ARTHURROLLO, LORRAINE J	8 GEOFFREY LN KINGS PARK NY 11754	R
14	01319102	MASKULYAK, JAMES W JRMASKULYAK, JENNIFER	15608 HUBBARD RD HUNTERSVILLE NC 28078	R
15	01319101	WHITAKER, ROBERTA S	15620 HUBBARD RD HUNTERSVILLE NC 28078	R
16	01313112	MCDONALD, KENNETH D	15648 HUBBARD RD HUNTERSVILLE NC 28078	R
17	01313123	BREWER, DENNISBREWER, CINDIE	15820 HUBBARD RD HUNTERSVILLE NC 28078	R
18	01313122	SCHELL, MICHAEL	15900 HUBBARD RD HUNTERSVILLE NC 28078	R
19	01313139	BREWER, DENNISBREWER, CINDIE	15820 HUBBARD RD HUNTERSVILLE NC 28078	R
20	01313110	GRASSROOTS LAND LLC,	15550 STUMPTOWN RD HUNTERSVILLE NC 28078	R
21	01313105	MAGNOLIA EQUESTRIAN CENTER LLC,	14210 LITHGOW PL HUNTERSVILLE NC 28078	R
22	01313103	PHILLIPS, MADELINE PHILLIPS, DANIEL E (B/W)	14720 BROWNS MILL RD HUNTERSVILLE NC 28078	R
23	01313102	GILEAD ASSOCIATE REFORMED, PRESBYTERIAN CH	RFD 3 BOX 108 HUNTERSVILLE NC 28078	R
24	01501107	BIGGERS, EDGAR M III	17115 GRENACHE CT CORNELIUS NC 28031	R
25	01501108	VOYER, MEUSSAVOYER, CLEMENT LEON III	15308 BEATTIES FORD RD HUNTERSVILLE NC 28078	R
26	01501112	NICHOLSON, JAMES R	15124 BEATTIES FORD RD HUNTERSVILLE NC 28078	R
27	01501109	SCHAMU, MARIKA MSCHAMU, CARL W	23985 N PATUXENT BEACH RD CALIFORNIA MD 20619	R
28	01314101	MOORE, DAVID FRANKTARA LYNN,	15619 HUBBARD RD HUNTERSVILLE NC 28078	R
29	01314102	MABE, SHELLEY ADOUGLAS M LAWRMORE,	15815 HUBBARD RD HUNTERSVILLE NC 28078	R
30	01314129	WILLIAMSON, ELIZABETH ANN	15823 HUBBARD RD HUNTERSVILLE NC 28078	R
31	01314130	ZARNOCH, ROBERT A	14111 LEA POINT CT HUNTERSVILLE NC 28078	R



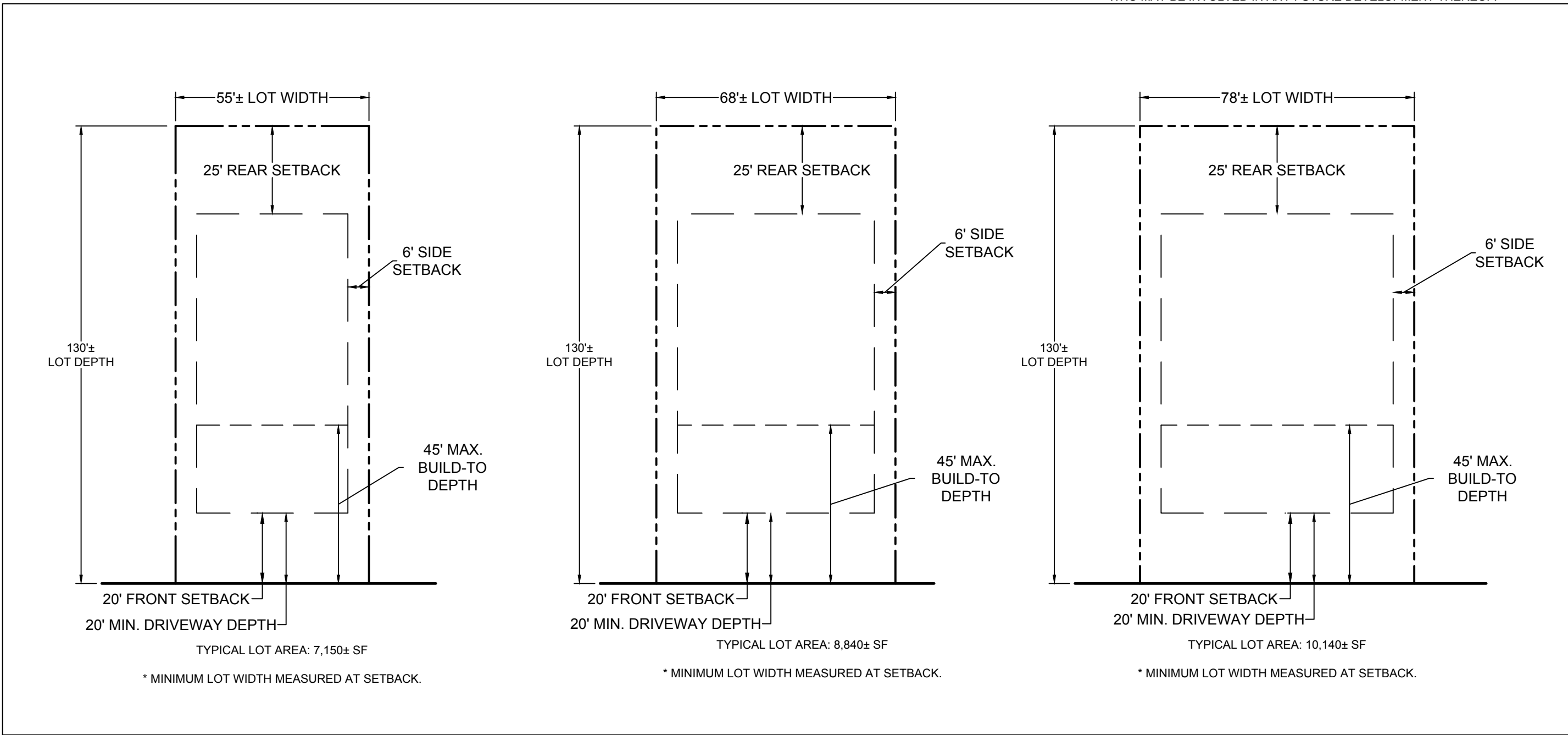
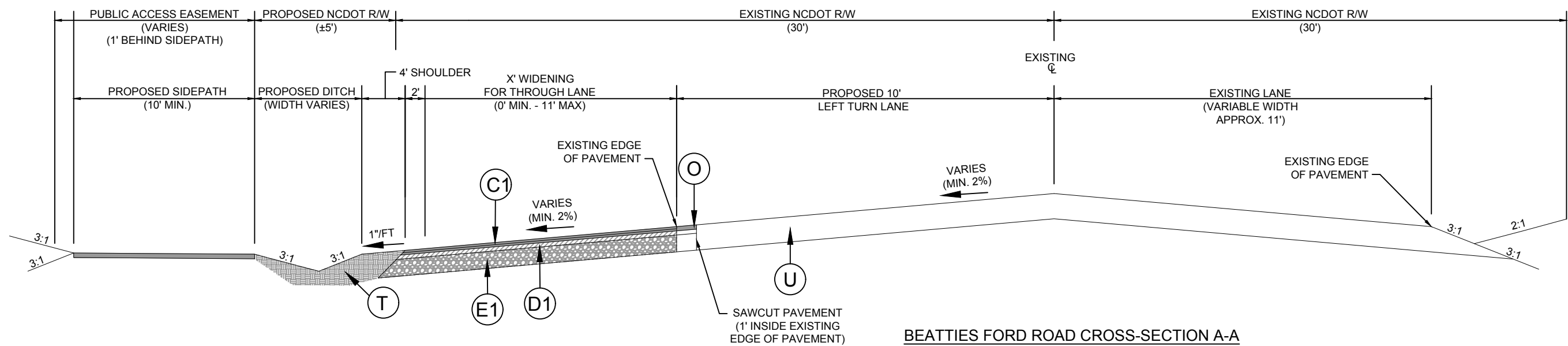
SHEET NO.
RZ-104

S:\0457776-Business Ford Residential\Epcor\DWG\Sheet\Resizing\57776-C200-SITE.dwg Plotted on 7/21/2023 1:12 PM by Andy Clark



BLOCK LENGTH DIAGRAM
AND STREET TYPE MAP
N.T.S

BEATTIES FORD ROAD PAVEMENT SCHEDULE	
C1	ASPHALT SURFACE COURSE (1.5" OF 59.5C, 2 LIFTS, RATE 112 LBS/SY/INCH)
D1	ASPHALT INTERMEDIATE COURSE (2.5" OF 119.0C, RATE 114 LBS/SY/INCH)
E1	ASPHALT BASE COURSE (8" OF 825.0C, 2 LIFTS, FIRST "P" EXTENDING 6" BEHIND CURB, SECOND LIFT 3", RATE 114 LBS/SY/INCH)
O	ASPHALT OVERLAY (1.5" 59.5C, RATE 112 LBS/SY/INCH)
T	EARTH MATERIAL
U	EXISTING PAVEMENT



GENERAL PROVISIONS

- THESE DEVELOPMENT STANDARDS FORM A PART OF THE REZONING PLAN ASSOCIATED WITH THE REZONING APPLICATION FOR EPM PROJECT NO. "R23-07" (449924) FILED BY EPCON COMMUNITIES (THE "PETITIONER") ON MAY 26, 2023 (THE "FILING DATE") FOR AN APPROXIMATELY 78.70 ACRE SITE LOCATED OFF OF BEATTIES FORD ROAD, IN HUNTERVILLE, NORTH CAROLINA, WHICH SITE IS MORE PARTICULARLY DEPICTED ON THE REZONING PLAN (THE "SITE"). THE SITE IS COMPOSED OF TAX PARCEL NOS. 01313125, 01313126, 01313142, 01313143, 01313144, AND 01313116. THE CURRENT ZONING OF THE SITE IS RURAL DISTRICT (R) LOCATED IN HUNTERVILLE AND MECKLENBURG COUNTY. THE PURPOSE OF THE REZONING PLAN AND ANNEXATION IS TO CONVERT THE ZONING CLASSIFICATION OF THE ENTIRE SITE TO TRANSITIONAL RESIDENTIAL DISTRICT (TR) WITHIN THE TOWN OF HUNTERVILLE.
- DEVELOPMENT OF THE SITE WILL BE GOVERNED BY THE REZONING PLAN, THESE DEVELOPMENT STANDARDS AND THE APPLICABLE PROVISIONS OF THE TOWN OF HUNTERVILLE ZONING ORDINANCE AND SUBDIVISION ORDINANCE IN PLACE ON THE FILING DATE (THE "ORDINANCE").
- UNLESS THE REZONING PLAN OR THESE DEVELOPMENT STANDARDS ESTABLISH OTHER STANDARDS, THE REGULATIONS ESTABLISHED UNDER THE ORDINANCE FOR THE TRANSITIONAL RESIDENTIAL DISTRICT (TR) ZONING DISTRICT SHALL GOVERN ALL DEVELOPMENT TAKING PLACE ON THE SITE.
- THE LOTS AND PROPOSED IMPROVEMENTS, INCLUDING LOCATION OF STREETS, LOTS, DRIVEWAYS, AND COMMON AREAS, TREE SAVE, SHOWN ON THE SKETCH/REZONING PLAN ARE SCHEMATIC IN NATURE AND MAY BE ALTERED, OR MODIFIED DURING CONSTRUCTION DOCUMENT PHASE 50 LONG AS SUCH MODIFICATION IS COMPATIBLE WITH THE LAYOUT AND LOCATION OF LOTS AND IMPROVEMENTS SHOWN ON THE SKETCH/REZONING PLAN. MODIFICATIONS TO THE SITE PLAN MUST BE APPROVED BY THE TOWN OF HUNTERVILLE PLANNING AND ENGINEERING STAFF.
- THE DEVELOPMENT OF THE SITE AS GENERALLY DEPICTED ON THE REZONING PLAN MAY BE PHASED. ANY PROPOSED PHASING MUST ALIGN WITH REQUIRED INFRASTRUCTURE AND STORMWATER IMPROVEMENTS, PROVIDED, HOWEVER, EACH PHASE OR SEQUENCE OF IMPROVEMENTS IN THE SITE WILL MEET ALL ORDINANCE REQUIREMENTS, UTILITIES, INFRASTRUCTURE, AND GRADING SHALL BE DELIVERED TO EACH INDIVIDUAL PHASE AS EACH IS DEVELOPED.
- IN DEVELOPING THE PROPERTY, THE LAND MAY NEED TO BE RECOMBINED AND SUBDIVIDED FOR CONVEYANCE OR FINANCING PURPOSES. ANY SUCH RECOMBINATION OR SUBDIVISION WILL MEET THE REQUIREMENTS OF THE ORDINANCE. IN THE COURSE OF DEVELOPMENT, A REDUCTION OF LOTS MAY OCCUR IN ACCORDANCE WITH THE REGULATIONS OF THE ORDINANCE.
- FUTURE AMENDMENTS TO THE REZONING PLAN AND/OR THESE DEVELOPMENT STANDARDS MAY BE APPLIED FOR BY THE THEN OWNER OR OWNERS OF THE SITE IN ACCORDANCE WITH THE PROVISIONS OF THE ORDINANCE. PROVIDED, HOWEVER, IN THE EVENT ANY PORTION OF THE SITE IS CONVEYED TO A THIRD PARTY, PETITIONER MAY REQUEST AN AMENDMENT TO THE REZONING PLAN WITHOUT THE WRITTEN CONSENT OF ANY OTHER OWNER OF ALL OR ANY PORTION OF THE SITE UNLESS SUCH AMENDMENT CONSTITUTES A CHANGE IN THE BUILDING OR USE OF THE PORTION OF THE SITE OWNED BY SUCH OWNER. ALL REQUIREMENTS IN CONNECTION WITH THE AMENDMENT WILL BE CALCULATED ON THE SITE AS A WHOLE IN THE SAME MANNER SUCH REQUIREMENTS WERE CALCULATED AT THE TIME OF THE INITIAL APPROVAL.
- THE REZONING PLAN IS A SITE-SPECIFIC DEVELOPMENT PLAN, AND APPROVAL THEREOF CONSTITUTES VESTED RIGHTS IN THE REZONING PLAN NOTWITHSTANDING ANY OTHER PROVISIONS OF THESE DEVELOPMENT STANDARDS. IF, AT SOME POINT, MODIFICATIONS ARE MADE TO THE TOWN'S ZONING ORDINANCE BY THE TOWN BOARD, PETITIONER MAY VOLUNTARILY AGREE TO APPLY SUCH MODIFICATIONS TO THE REZONING PLAN IN A MANNER CONSISTENT WITH THE ORDINANCE AS IT CHANGES FROM TIME TO TIME, AND WITHOUT PURSUING A REZONING. PROVIDED ORDINANCE MODIFICATIONS DO NOT CONSTITUTE A MAJOR AMENDMENT. SUCH MODIFICATIONS TO THE ORDINANCE SHALL IN NO WAY IMPACT THE PETITIONER'S VESTED RIGHTS.
- APPROVAL OF THE REZONING PLAN SHALL CONSTITUTE ESTABLISHMENT OF VESTED RIGHTS IN THE LANDOWNER (AND ITS SUCCESSORS AND ASSIGNS) FOR A PERIOD OF THREE YEARS PURSUANT TO N.C. GEN. STAT. §160A-385.1.

PERMITTED USES

- THE SITE MAY BE DEVELOPED FOR ANY USES THAT ARE PERMITTED BY RIGHT OR PERMITTED WITH CONDITIONS, UNDER THE ORDINANCE, INCLUDING ACCESSORY USES, IN THE TRANSITIONAL RESIDENTIAL DISTRICT, SUBJECT TO THE DEVELOPMENT STANDARDS ASSOCIATED WITH SUCH USE. ANY LABELING ON THE REZONING PLAN MAY BE AN INDICATION OF THE CURRENT INTENTION ON THE PART OF PETITIONER BUT SHALL NOT RESTRICT THE SITE IN A MANNER THAT CONFLICTS WITH THESE DEVELOPMENT NOTES.

TRANSPORTATION/ACCESS/STREET IMPROVEMENTS

- VEHICULAR ACCESS TO THE SITE SHALL BE AS GENERALLY DEPICTED ON THE REZONING PLAN. THE PLACEMENT AND CONFIGURATION OF EACH VEHICULAR ACCESS POINT ARE SUBJECT TO ANY MINOR MODIFICATIONS REQUIRED TO ACCOMMODATE FINAL SITE AND CONSTRUCTION PLANS AND DESIGNS AND TO ANY ADJUSTMENTS REQUIRED FOR APPROVAL BY THE TOWN OF HUNTERVILLE AND/OR THE NORTH CAROLINA DEPARTMENT OF TRANSPORTATION.
- THE ALIGNMENTS OF THE INTERNAL DRIVES AND PARKING AREAS TO BE LOCATED ON THE SITE ARE SUBJECT TO ANY MINOR MODIFICATIONS OR ALTERATIONS REQUIRED DURING THE DESIGN DEVELOPMENT AND CONSTRUCTION PERMITTING PROCESSES.
- PETITIONER SHALL INSTALL SIDEWALKS, STREET TREES, PLANTING STRIPS, OR OTHER STREET IMPROVEMENTS AS SHOWN ON THE REZONING PLAN.
- PER THE TRAFFIC IMPACT ANALYSIS (TIA) APPLICATION FOR DETERMINATION OF TIA NEED REVIEWED BY THE TOWN AND ISSUED ON 4/19/2023, A TIA IS NOT REQUIRED FOR THIS DEVELOPMENT. THE FOLLOWING IMPROVEMENTS ARE REQUIRED TO BEATTIES FORD ROAD BY NCDOT:
 - 150' LEFT TURN LANE
 - 100' RIGHT TURN LANE

LANDSCAPING/BUFFERS

- DEVELOPMENT OF THE SITE SHALL COMPLY WITH THE LANDSCAPING AND SCREENING REQUIREMENTS OF THE ORDINANCE.
- AN UNDISTURBED BUFFER YARD IS INTENDED TO BE A NATURAL, WOODED AREA AND SHALL COUNT TOWARD THE PROVISION OF OPEN SPACE AND TREE SAVE FOR THE DEVELOPMENT WHERE THE BUFFER CONTAINS EXISTING VEGETATION, IS A MINIMUM OF 20' FEET, AND IS NOT PART OF INDIVIDUAL LOTS. ONLY PORTIONS OF UNDISTURBED BUFFER YARD WITH EXISTING TREE COVER SHALL BE COUNTED AS TREE SAVE.
- AREAS OF THE PERIMETER BUFFER AND LANDSCAPE AREA THAT ARE DISTURBED SHALL BE REPLANTED ACCORDING TO STANDARDS OUTLINED IN CHAPTER 7 OF THE ORDINANCE. EXISTING VEGETATION MAY BE INCLUDED TO SATISFY BUFFER REQUIREMENTS.
- PETITIONER SHALL SHOW WALKING PATHS WITHIN OPEN SPACE AND URBAN OPEN SPACE AS SCHEMATICALLY SHOWN ON THE REZONING PLAN. THE ACTUAL LOCATION AND DETAILS OF SUCH PATHS AND URBAN OPEN SPACE TO BE DETERMINED DURING THE CONSTRUCTION DOCUMENT PHASE.
- THE 20' UNDISTURBED PERIMETER BUFFER WITHOUT EXISTING VEGETATION MAY BE DISTURBED IN ORDER TO PLANT NEW VEGETATION.
- RESIDENTIAL LOT TREES WILL BE PROVIDED AS FOLLOWS:
LOTS LESS THAN 10,000 SF: 1 FRONT YARD, 1 REAR YARD TREE REQUIRED
LOTS 10,000 SF - 15,000 SF: 1 FRONT YARD, 2 REAR YARD TREES REQUIRED

UTILITY PROVISIONS

- NEW WATER MAINS WILL BE PLACED UNDER SIDEWALK PER CHARLOTTE WATER STANDARDS.
- NEW SANITARY SEWER MAINS WILL BE PLACED PER CHARLOTTE WATER STANDARDS.

BINDING EFFECT OF THE REZONING DOCUMENTS AND DEFINITIONS

- IF THIS REZONING APPLICATION IS APPROVED, ALL CONDITIONS APPLICABLE TO THE USE AND DEVELOPMENT OF THE SITE IMPOSED UNDER THESE DEVELOPMENT STANDARDS AND THE REZONING PLAN WILL, UNLESS AMENDED IN THE MANNER PROVIDED UNDER THE ORDINANCE, BE BINDING UPON AND INURE TO THE BENEFIT OF PETITIONER AND THE CURRENT AND SUBSEQUENT OWNERS OF THE SITE AND THEIR RESPECTIVE SUCCESSORS IN INTEREST AND ASSIGNS.
- THROUGHOUT THESE DEVELOPMENT STANDARDS, THE TERM "PETITIONER" SHALL BE DEEMED TO INCLUDE THE HEIRS, DEVISEES, PERSONAL REPRESENTATIVES, SUCCESSORS IN INTEREST AND ASSIGNS OF PETITIONER OR THE OWNER OR OWNERS OF THE SITE FROM TIME TO TIME WHO MAY BE INVOLVED IN ANY FUTURE DEVELOPMENT THEREOF.

ZONING CODE SUMMARY

PARCEL NUMBERS	01313125 9.6 ACRES 01313126 43.86 ACRES 01313142 9.403 ACRES 01313143 0.977 ACRES 01313144 1.215 ACRES 01313116 14.63 ACRES	OWNER: FRED T & SANDRA R BROWNING OWNER: PAUL & RUTH WALTERS FAMILY LLC OWNER: PAUL & RUTH WALTERS FAMILY LLC OWNER: PAUL & RUTH WALTERS FAMILY LLC OWNER: PAUL & RUTH WALTERS FAMILY LLC OWNER: PAUL & RUTH WALTERS FAMILY LLC
TOTAL PARCEL AREA	78.74 AC	
EXISTING ZONING	R	
PROPOSED ZONING	TR	
EXISTING LAND USE:	SINGLE FAMILY RESIDENTIAL	
PROPOSED LAND USE:	SINGLE FAMILY RESIDENTIAL	
BUILDING TYPE:	SINGLE FAMILY DETACHED	
TOTAL PROPOSED LOTS	118 LOTS	
55' WIDTH	54 LOTS (45.8%)	
66' WIDTH	57 LOTS (48.3%)	
78' WIDTH	7 LOTS (5.9%)	
MAXIMUM DENSITY:	1.5 DUA (WITH 40% OPEN SPACE)	
PROVIDED DENSITY:	118 LOTS / 78.7 AC = 1.5 DUA	
AMENITY SIZE:	±3,360 SF AMENITY BUILDING WITH POOL	
TYPICAL LOT SIZE:	55' X 130' (7,150 SF) 66' X 130' (8,580 SF) 78' X 130' (10,140 SF)	
AVERAGE LOT SIZE:	62.64' X 130' (8,144 SF)	
REQUIRED SETBACKS		
SIDE SETBACK	6'	
FRONT SETBACK	SEE BUILD-TO-LINE	
REAR SETBACK	25'	
CORNER SETBACK	10'	
BUILD-TO-LINE	20' TO 45' MAX. FROM RIGHT-OF-WAY	
REQUIRED BUFFER	20'/40' UNDISTURBED BUFFER, 20' UNDISTURBED/20' DISTURBED BUFFER	
OPEN SPACE REQUIRED	31.48± ACRES (40%)	
OPEN SPACE PROVIDED	31.59± ACRES (40.1%)	
URBAN OPEN SPACE	0.87± ACRES (2.75%)	
COMMON OPEN SPACE	9.72± ACRES (30.77%)	
NATURAL OPEN SPACE:	21.00± ACRES (66.48%)	
TREE SAVE REQUIRED:	20.47± ACRES (35% OF 58.49± AC EXISTING CANOPY)	
TREE SAVE PROVIDED:	21.00± ACRES	
SOILS:	CeB2, CeD2, EriD, MO, P&E	
WATERSHED:	MTN, ISLAND LAKE HIGH DENSITY	
PERCENTAGE OF IMPERVIOUS ALLOWED:	70% WITH BMP (±55.09 ACRES)	
IMPERVIOUS AREA:		

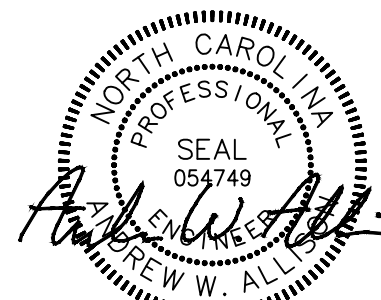
IMPERVIOUS AREA INSIDE LOTS:
BUILDING / FUTURE IMPROVEMENTS*: 14.11 ACRES
DRIVEWAYS: 1.65 ACRES
*1.00% OF LOT AREA (BUT NOT LESS THAN 150 SF PER LOT) RESERVED FOR ADDITIONS OF FUTURE IMPERVIOUS AREA
IMPERVIOUS AREA INSIDE RIGHT-OF-WAY: 5.38 ACRES
TOTAL SITE IMPERVIOUS AREA: 21.14 ACRES (26.86% BUA)
NOTE: BREAKDOWN OF IMPERVIOUS AREA TO BE ALLOCATED FOR EACH LOT TO BE PROVIDED WITH CALCULATIONS AND ON CONSTRUCTION PLAN SET

GENERAL NOTES

- ALL DEVELOPMENT AND CONSTRUCTION SHALL COMPLY WITH ALL ZONING AND SUBDIVISION STANDARDS OF THE TOWN OF HUNTERVILLE, MECKLENBURG COUNTY, AND NCDOT, AS APPLICABLE.
- THIS PROPERTY MAY BE SUBJECT TO ANY EASEMENTS AND/OR RIGHT-OF-WAY OF RECORD.
- ALL AREAS DESIGNATED AS COMMON AND/OR URBAN OPEN SPACE SHALL BE OWNED AND MAINTAINED BY THE HOMEOWNERS ASSOCIATION AND DEDICATED FOR PERPETUITY.
- ACCESS (INGRESS/EGRESS) LOCATION AND DESIGN SHOWN ON THIS SKETCH PLAN AREA SUBJECT TO ACHIEVING VERTICAL AND HORIZONTAL SIGHT DISTANCES, TURN LANE IMPROVEMENTS (INCLUDING RIGHT-OF-WAY AND INTERSECTION WITH ADJACENT AND OPPOSING ACCESS POINTS, MODIFICATIONS TO PLAN MAY RESULT.
- LARGE MATURING TREES WILL BE PLANTED 45' O.C. WITHIN THE REQUIRED PLANTING STRIP ALONG ALL STREETS WITH THE EXCEPTION OF RURAL PARKWAYS WHERE EXISTING TREES CAN SATISFY THE STREET TREE REQUIREMENT. SMALL MATURING TREES ARE TO BE USED WHERE OVERHEAD POWER LINES EXIST.
- CLUSTER BOX UNITS (CBUs) WILL BE PROVIDED FOR MAIL DELIVERY. LOCATION SHOWN ON PLANS IS APPROXIMATE AND SUBJECT TO CHANGE PENDING UTILS APPROVAL.
- THE PROPOSED DEVELOPMENT WILL BE SERVED BY PUBLIC WASTE MANAGEMENT FOR TRASH COLLECTION.
- ARTICLE 8.16.1 & 2 OF THE TOWN OF HUNTERVILLE ZONING ORDINANCE SHALL APPLY.
- ARTICLE 8.16.3 & 5 OF THE TOWN OF HUNTERVILLE ZONING ORDINANCE SHALL APPLY.
- DIRECT ACCESS FROM LOTS TO A THOROUGHFARE IS PROHIBITED.
- THE TOWN OF HUNTERVILLE DEFINES THE BUILD-TO LINE AS A LINE EXTENDING THROUGH A LOT WHICH IS GENERALLY PARALLEL TO THE FRONT PROPERTY LINE AND MARKS THE LOCATION FROM WHICH THE PRINCIPLE VERTICAL PLANE OF THE FRONT BUILDING ELEVATION, EXCLUSIVE OF PORCHES, BAY WINDOWS AND SIMILAR APPURTENANCES, MUST BE ERRECTED, INTENDED TO CREATE AN EVEN BUILDING FACADE LINE ON A STREET. THE BUILD-TO LINE IS ESTABLISHED ON THE RECORD PLAT (FINAL PLAT).

MODIFICATION REQUESTS

- REMOVE LANDSCAPED MEDIAN REQUIREMENT AT THE ENTRANCE OF THE SUBDIVISION.
- INCREASE THE DRIVEWAY WIDTH TO 18' FOR LOTS LESS THAN 60' WIDE.
- INCREASE THE MAXIMUM LENGTH OF A CUL-DE-SAC BY ±470' DUE TO CONSTRAINTS IMPOSED BY EXISTING EASEMENTS.
- ALLOW DISTURBANCE IN THE FIRST 20' OF THE UNDISTURBED BUFFER WHERE NOTED ON THE SITE PLAN. THIS DISTURBED AREA WILL BE REPLANTED ACCORDING TO THE ZONING ORDINANCE AND AS SHOWN ON THE SITE PLAN.
- ALLOW A WET POND RATHER THAN TRADITIONAL WATER QUALITY MEASURES FOR THE DENSITY OF THE SITE.



PRELIMINARY
FOR REVIEW
PURPOSES ONLY

THIS DRAWING PREPARED AT THE
CHARLOTTE OFFICE
610 E. Morehead Street, Suite 250 | Charlotte, NC 28202
TEL 704.602.8600 FAX 704.376.1076 www.timmons.com
North Carolina License No. C-1652



EPCON COMMUNITIES
11020 DAVID TAYLOR DR., SUITE 05
CHARLOTTE, NC 28262

YOUR VISION ACHIEVED THROUGH OURS.

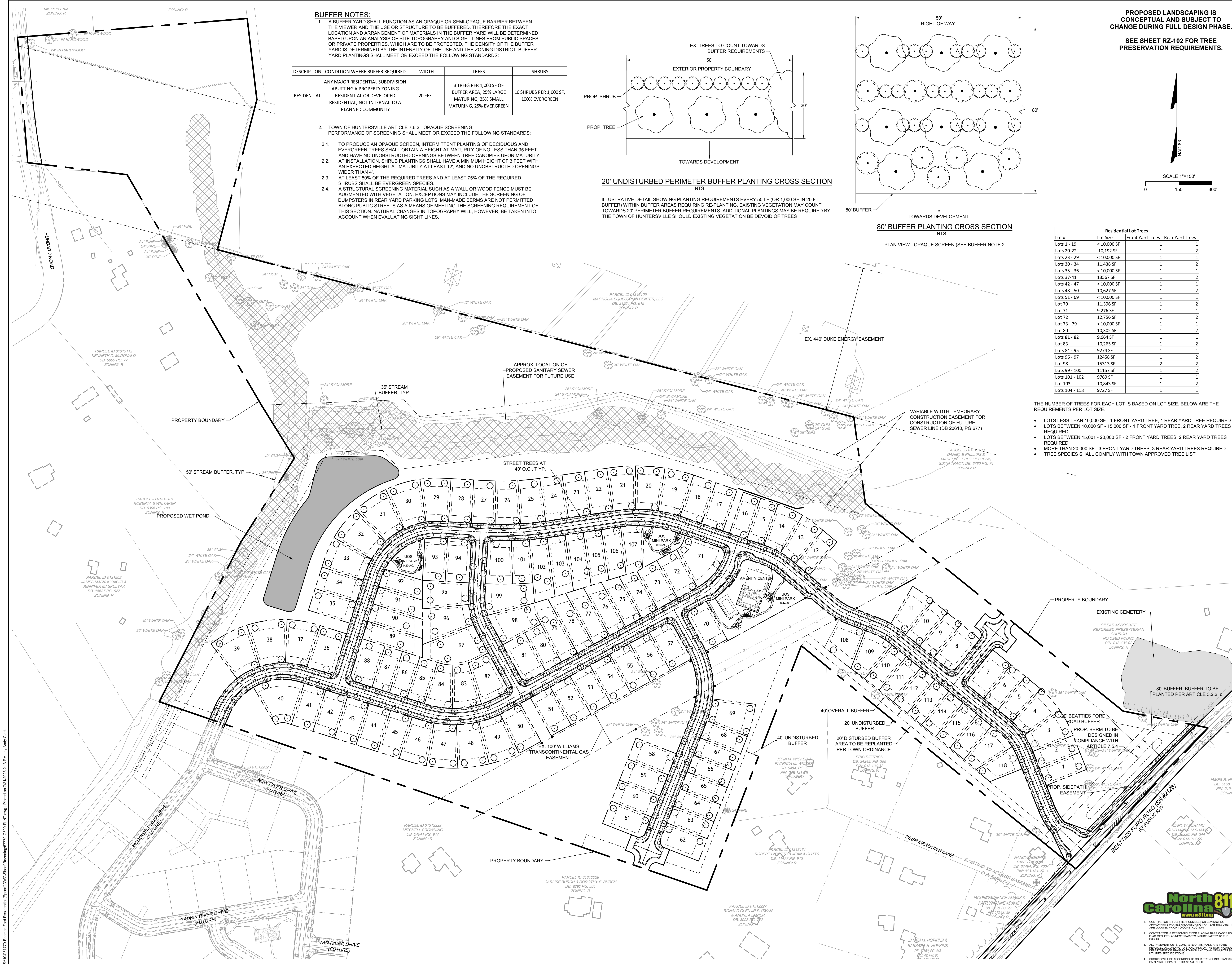
EPCON - COURTYARDS AT WALTERS FARM
HUNTERVILLE, NORTH CAROLINA
SITE NOTES AND DETAILS

JOB NO.
57770
SHEET NO.
RZ-201



- CONTRACTOR IS FULLY RESPONSIBLE FOR CONTACTING APPROPRIATE PARTIES AND ASSURING THAT EXISTING UTILITIES ARE LOCATED PRIOR TO CONSTRUCTION.
- CONTRACTOR IS RESPONSIBLE FOR PLACING BARRICADES USING FLAG MEN ETC. AS NECESSARY TO INSURE SAFETY TO THE PUBLIC.
- ALL FURNISHED CUL-DE-SACS OR BAY AREAS ARE TO BE DESIGNED AND CONSTRUCTED TO STANDARDS OF THE NORTH CAROLINA DEPARTMENT OF TRANSPORTATION AND TOWN OF HUNTERVILLE UTILITIES SPECIFICATIONS.
- SHOWERS WILL BE ACCORDING TO DRAINAGE DRAINAGE STANDARDS PART 108 SUBPART F, OR AS AMENDED.

S:\0457776-Business Farm Residential-Epcon\DWG\Sheet\Resizing\57776-C500-PLT.dwg | Plotted on 7/21/2023 at 2:13 PM | by Andy Clark



BUFFER NOTES:

1. A BUFFER YARD SHALL FUNCTION AS AN OPAQUE OR SEMI-OPAQUE BARRIER BETWEEN THE VIEWER AND THE USE OR STRUCTURE TO BE BUFFERED. THEREFORE THE EXACT LOCATION AND ARRANGEMENT OF MATERIALS IN THE BUFFER YARD WILL BE DETERMINED BASED UPON AN ANALYSIS OF SITE TOPOGRAPHY AND SIGHT LINES FROM PUBLIC SPACES OR PRIVATE PROPERTIES, WHICH ARE TO BE PROTECTED. THE DENSITY OF THE BUFFER YARD IS DETERMINED BY THE INTENSITY OF THE USE AND THE ZONING DISTRICT. BUFFER YARD PLANTINGS SHALL MEET OR EXCEED THE FOLLOWING STANDARDS:

DESCRIPTION	CONDITION WHERE BUFFER REQUIRED	WIDTH	TREES	SHRUBS
RESIDENTIAL	ANY MAJOR RESIDENTIAL SUBDIVISION ABUTTING A PROPERTY ZONING RESIDENTIAL OR DEVELOPED RESIDENTIAL, NOT INTERNAL TO A PLANNED COMMUNITY	20 FEET	3 TREES PER 1,000 SF OF BUFFER AREA, 25% LARGE MATURING, 25% SMALL MATURING, 25% EVERGREEN	10 SHRUBS PER 1,000 SF, 100% EVERGREEN

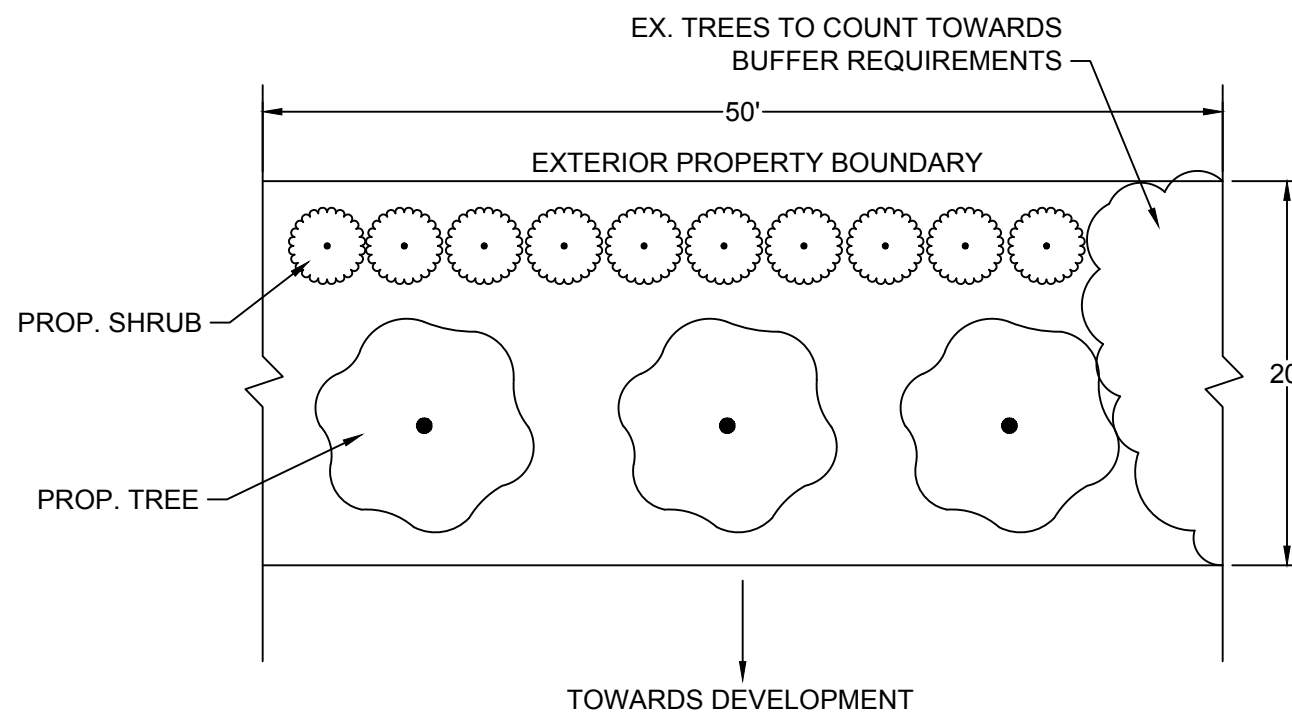
2. TOWN OF HUNTERSVILLE ARTICLE 7.6.2. OPAQUE SCREENING: PERFORMANCE OF SCREENING SHALL MEET OR EXCEED THE FOLLOWING STANDARDS:

2.1. TO PRODUCE AN OPAQUE SCREEN, INTERMITTENT PLANTING OF DECIDUOUS AND EVERGREEN TREES SHALL OBTAIN A HEIGHT AT MATURITY OF NO LESS THAN 35 FEET AND HAVE NO UNOBSTRUCTED OPENINGS BETWEEN TREE CANOPIES UPON MATURITY.

2.2. AT INSTALLATION, SHRUB PLANTINGS SHALL HAVE A MINIMUM HEIGHT OF 3 FEET WITH AN EXPECTED HEIGHT AT MATURITY AT LEAST 12', AND NO UNOBSTRUCTED OPENINGS WIDER THAN 4'.

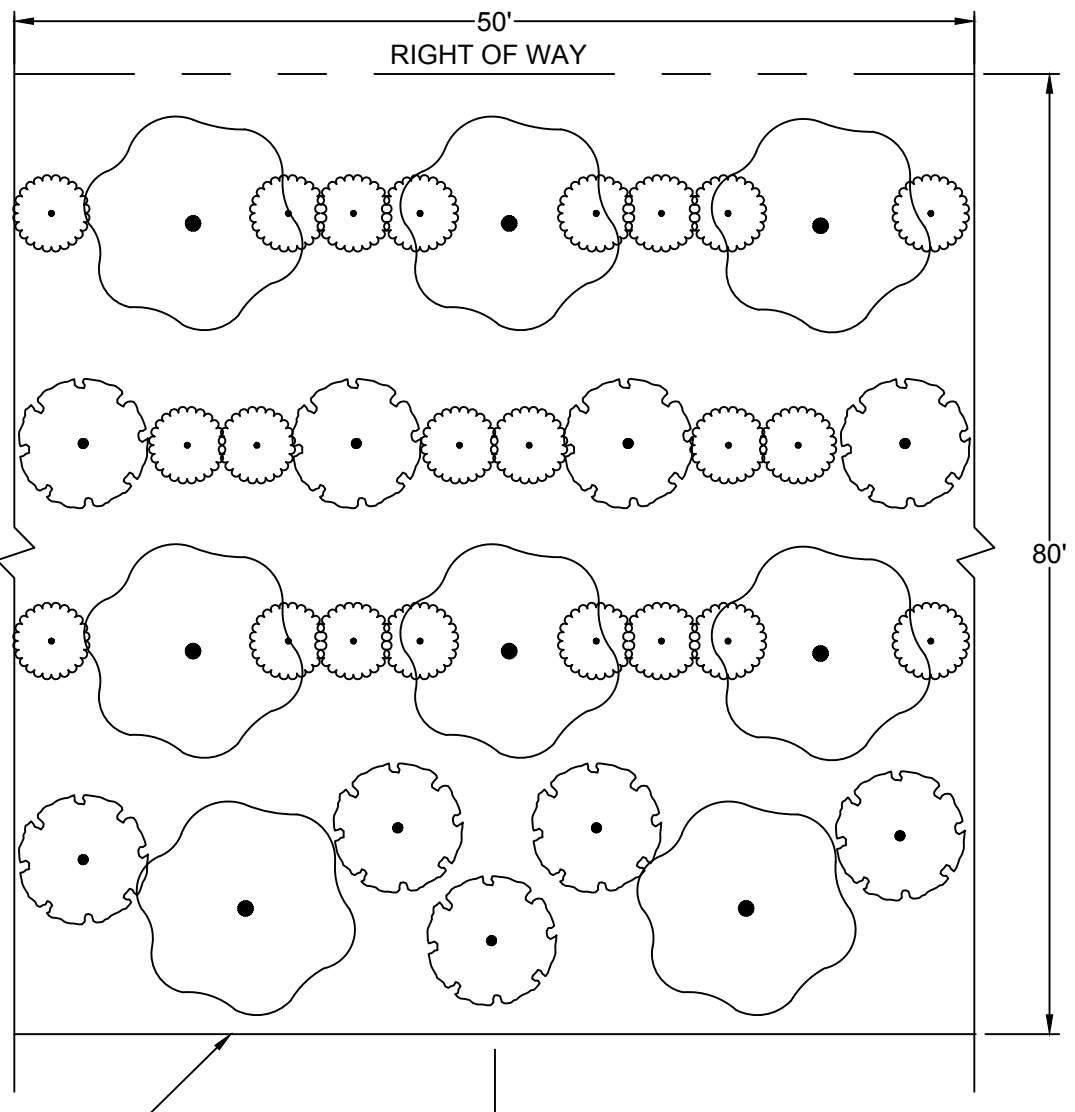
2.3. AT LEAST 50% OF THE REQUIRED TREES AND AT LEAST 75% OF THE REQUIRED SHRUBS SHALL BE EVERGREEN SPECIES.

2.4. A STRUCTURAL SCREENING MATERIAL SUCH AS A WALL OR WOOD FENCE MUST BE AUGMENTED WITH VEGETATION. EXCEPTIONS MAY INCLUDE THE SCREENING OF DUMPSTERS IN REAR YARD PARKING LOTS. MAN-MADE BERMS ARE NOT PERMITTED ALONG PUBLIC STREETS AS A MEANS OF MEETING THE SCREENING REQUIREMENT OF THIS SECTION. NATURAL CHANGES IN TOPOGRAPHY WILL, HOWEVER, BE TAKEN INTO ACCOUNT WHEN EVALUATING SIGHT LINES.



20' UNDISTURBED PERIMETER BUFFER PLANTING CROSS SECTION
NTS

ILLUSTRATIVE DETAIL SHOWING PLANTING REQUIREMENTS EVERY 50 LF (OR 1,000 SF IN 20 FT BUFFER) WITHIN BUFFER AREAS REQUIRING RE-PLANTING. EXISTING VEGETATION MAY COUNT TOWARDS 20' PERIMETER BUFFER REQUIREMENTS. ADDITIONAL PLANTINGS MAY BE REQUIRED BY THE TOWN OF HUNTERSVILLE SHOULD EXISTING VEGETATION BE DEVOID OF TREES

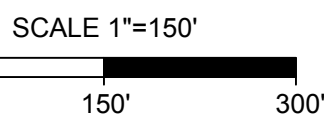


80' BUFFER PLANTING CROSS SECTION
NTS

PLAN VIEW - OPAQUE SCREEN (SEE BUFFER NOTE 2)

PROPOSED LANDSCAPING IS
CONCEPTUAL AND SUBJECT TO
CHANGE DURING FULL DESIGN PHASE.

SEE SHEET RZ-102 FOR TREE
PRESERVATION REQUIREMENTS.



Residential Lot Trees				
Lot #	Lot Size	Front Yard Trees	Rear Yard Trees	
Lots 1 - 19	< 10,000 SF	1	1	
Lots 20-22	10,192 SF	1	2	
Lots 23 - 29	< 10,000 SF	1	1	
Lots 30 - 34	11,438 SF	1	2	
Lots 35 - 36	< 10,000 SF	1	1	
Lots 37-41	13,567 SF	1	2	
Lots 42 - 47	< 10,000 SF	1	1	
Lots 48 - 50	10,627 SF	1	2	
Lots 51 - 69	< 10,000 SF	1	1	
Lot 70	11,396 SF	1	2	
Lot 71	9,276 SF	1	1	
Lot 72	12,756 SF	1	2	
Lot 73 - 79	< 10,000 SF	1	1	
Lot 80	10,302 SF	1	2	
Lots 81 - 82	9,664 SF	1	1	
Lot 83	10,265 SF	1	2	
Lots 84 - 95	9,274 SF	1	1	
Lots 96 - 97	12,458 SF	1	2	
Lot 98	15,133 SF	2	2	
Lots 99 - 100	11,157 SF	1	2	
Lots 101 - 102	9,769 SF	1	1	
Lot 103	10,843 SF	1	2	
Lots 104 - 118	9,727 SF	1	1	

THE NUMBER OF TREES FOR EACH LOT IS BASED ON LOT SIZE. BELOW ARE THE REQUIREMENTS PER LOT SIZE:

- LOTS LESS THAN 10,000 SF - 1 FRONT YARD TREE, 1 REAR YARD TREE REQUIRED
- LOTS BETWEEN 10,000 SF - 15,000 SF - 1 FRONT YARD TREE, 2 REAR YARD TREES REQUIRED
- LOTS BETWEEN 15,001 - 20,000 SF - 2 FRONT YARD TREES, 2 REAR YARD TREES REQUIRED
- MORE THAN 20,000 SF - 3 FRONT YARD TREES, 3 REAR YARD TREES REQUIRED.
- TREE SPECIES SHALL COMPLY WITH TOWN APPROVED TREE LIST

TIMMONS GROUP

YOUR VISION ACHIEVED THROUGH OURS.

EPCON - COURTYARDS AT WALTERS FARM
HUNTERSVILLE, NORTH CAROLINA
CONCEPTUAL PLANTING PLAN

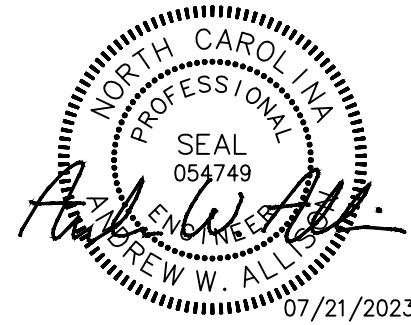
JOB NO.
57770
SHEET NO.
RZ-400

EPCON[®]
COMMUNITIES

EPCON COMMUNITIES
11020 DAVID TAYLOR DR, SUITE 105
CHARLOTTE, NC 28262

THIS DRAWING PREPARED AT THE
CHARLOTTE OFFICE
610 E. Morehead Street, Suite 250 | Charlotte, NC 28202
TEL 704.602.8600 FAX 704.376.1076 www.timmons.com
North Carolina License No. C-1652

PRELIMINARY
FOR REVIEW
PURPOSES ONLY



REVISION DESCRIPTION

REVISED PER TOWN COMMENTS

DATE

07/21/2023

DRAWN BY

A. CLARK

DESIGNED BY

A. ALLISON

CHECKED BY

A. ALLISON

SCALE

1" = 100'

DATE

07/21/2023

DRAWN BY

A. CLARK

DESIGNED BY

A. ALLISON

CHECKED BY

A. ALLISON

SCALE

1" = 100'

DATE

07/21/2023

DRAWN BY

A. CLARK

DESIGNED BY

A. ALLISON

CHECKED BY

A. ALLISON

SCALE

1" = 100'

DATE

07/21/2023

DRAWN BY

A. CLARK

DESIGNED BY

A. ALLISON

CHECKED BY

A. ALLISON

SCALE

1" = 100'

DATE

07/21/2023

DRAWN BY

A. CLARK

DESIGNED BY

A. ALLISON

CHECKED BY

A. ALLISON

SCALE

1" = 100'

DATE

07/21/2023

DRAWN BY

A. CLARK

DESIGNED BY

A. ALLISON

CHECKED BY

A. ALLISON

SCALE

1" = 100'

DATE

07/21/2023

DRAWN BY

A. CLARK

DESIGNED BY

A. ALLISON

CHECKED BY

A. ALLISON

SCALE

1" = 100'

DATE

07/21/2023

DRAWN BY

A. CLARK

DESIGNED BY

A. ALLISON

CHECKED BY

A. ALLISON

SCALE

1" = 100'

DATE

07/21/2023

DRAWN BY

A. CLARK

DESIGNED BY

A. ALLISON

CHECKED BY

A. ALLISON

SCALE

1" = 100'

DATE

07/21/2023

DRAWN BY

A. CLARK

DESIGNED BY

A. ALLISON

CHECKED BY

A. ALLISON

SCALE

1" = 100'

DATE

07/21/2023

DRAWN BY

A. CLARK

DESIGNED BY

A. ALLISON

CHECKED BY

A. ALLISON

SCALE

1" = 100'

DATE

07/21/2023

DRAWN BY

A. CLARK

DESIGNED BY

A. ALLISON

CHECKED BY

A. ALLISON

SCALE

1" = 100'

DATE

07/21/2023

DRAWN BY

A. CLARK

DESIGNED BY

A. ALLISON

CHECKED BY

A. ALLISON

SCALE

1" = 100'

DATE

07/21/2023

DRAWN BY

A. CLARK

DESIGNED BY

A. ALLISON

CHECKED BY

A. ALLISON

SCALE

1" = 100'

DATE

07/21/2023

DRAWN BY

A. CLARK

DESIGNED BY

A. ALLISON

CHECKED BY

A. ALLISON

SCALE

1" = 100'

DATE

07/21/2023

DRAWN BY

A. CLARK

DESIGNED BY

A. ALLISON

CHECKED BY

A. ALLISON

SCALE

1" = 100'

DATE

07/21/2023

DRAWN BY

A. CLARK

DESIGNED BY

A. ALLISON

CHECKED BY

A. ALLISON

SCALE

1" = 100'

DATE

07/21/2023

DRAWN BY

A. CLARK

DESIGNED BY

A. ALLISON

CHECKED BY

A. ALLISON

SCALE

1" = 100'

DATE

07/21/2023

DRAWN BY

A. CLARK

DESIGNED BY

A. ALLISON

CHECKED BY

A. ALLISON

SCALE

1" = 100'

DATE

07/21/2023

DRAWN BY

A. CLARK

DESIGNED BY

A. ALLISON

CHECKED BY

A. ALLISON

SCALE

1" = 100'

DATE

07/21/2023

DRAWN BY

A. CLARK

DESIGNED BY

A. ALLISON

CHECKED BY

A. ALLISON

SCALE

1" = 100'

DATE

07/21/2023

DRAWN BY

A. CLARK

DESIGNED BY

A. ALLISON

CHECKED BY

A. ALLISON

SCALE

1" = 100'

DATE

07/21/2023

DRAWN BY

A. CLARK

DESIGNED BY

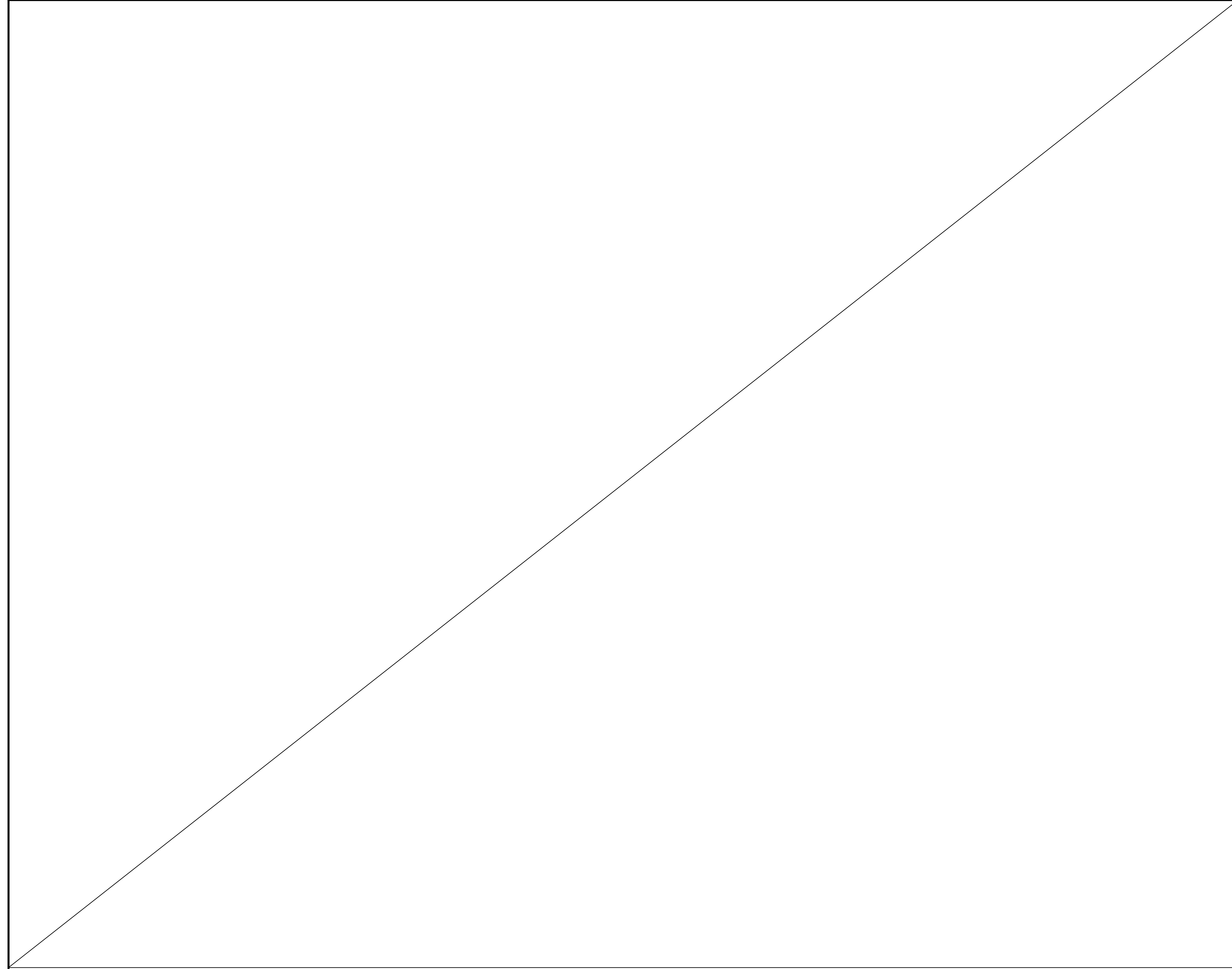
A. ALLISON

CHECKED BY

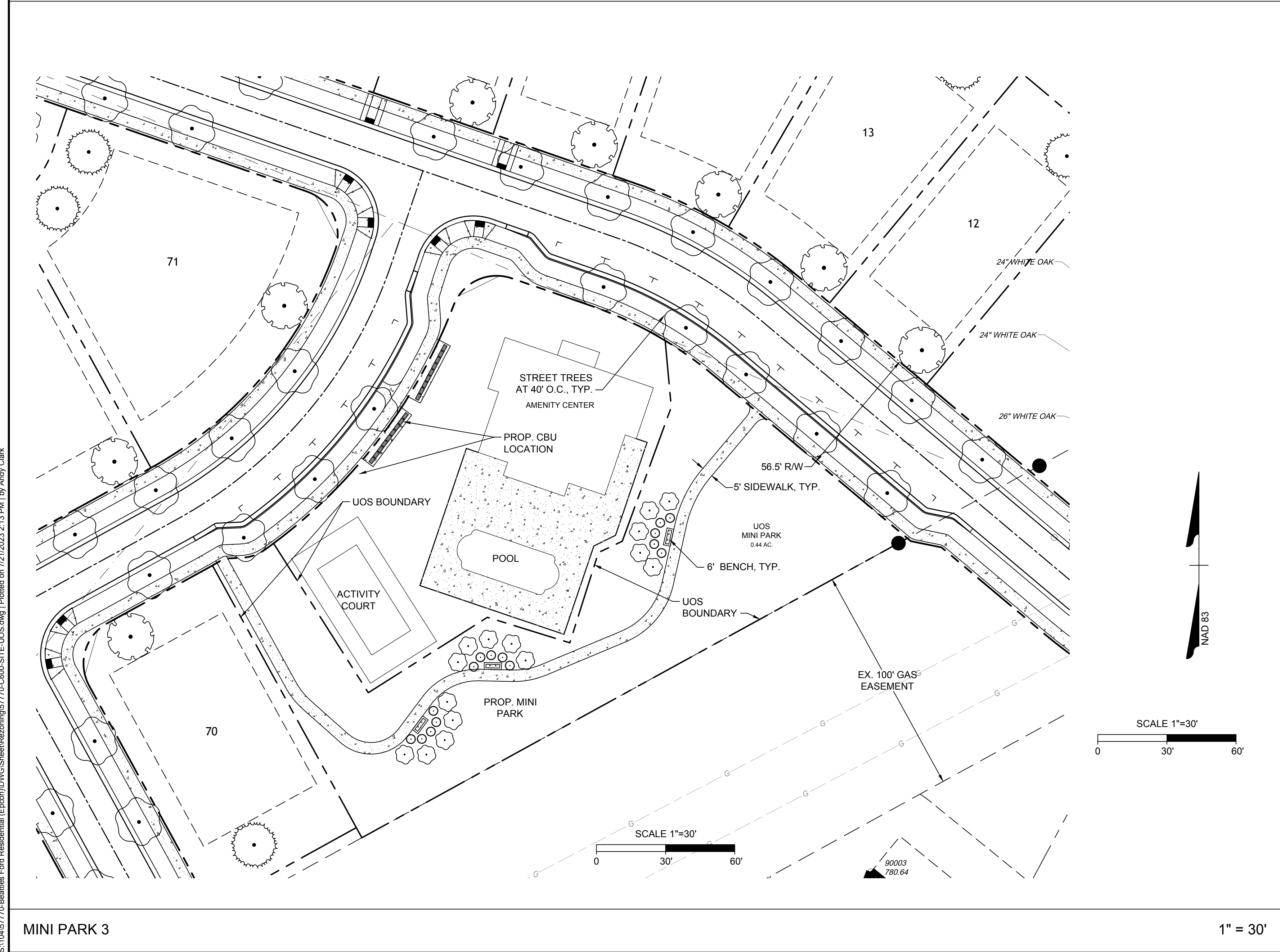
A. ALLISON

SCALE

1" = 100'

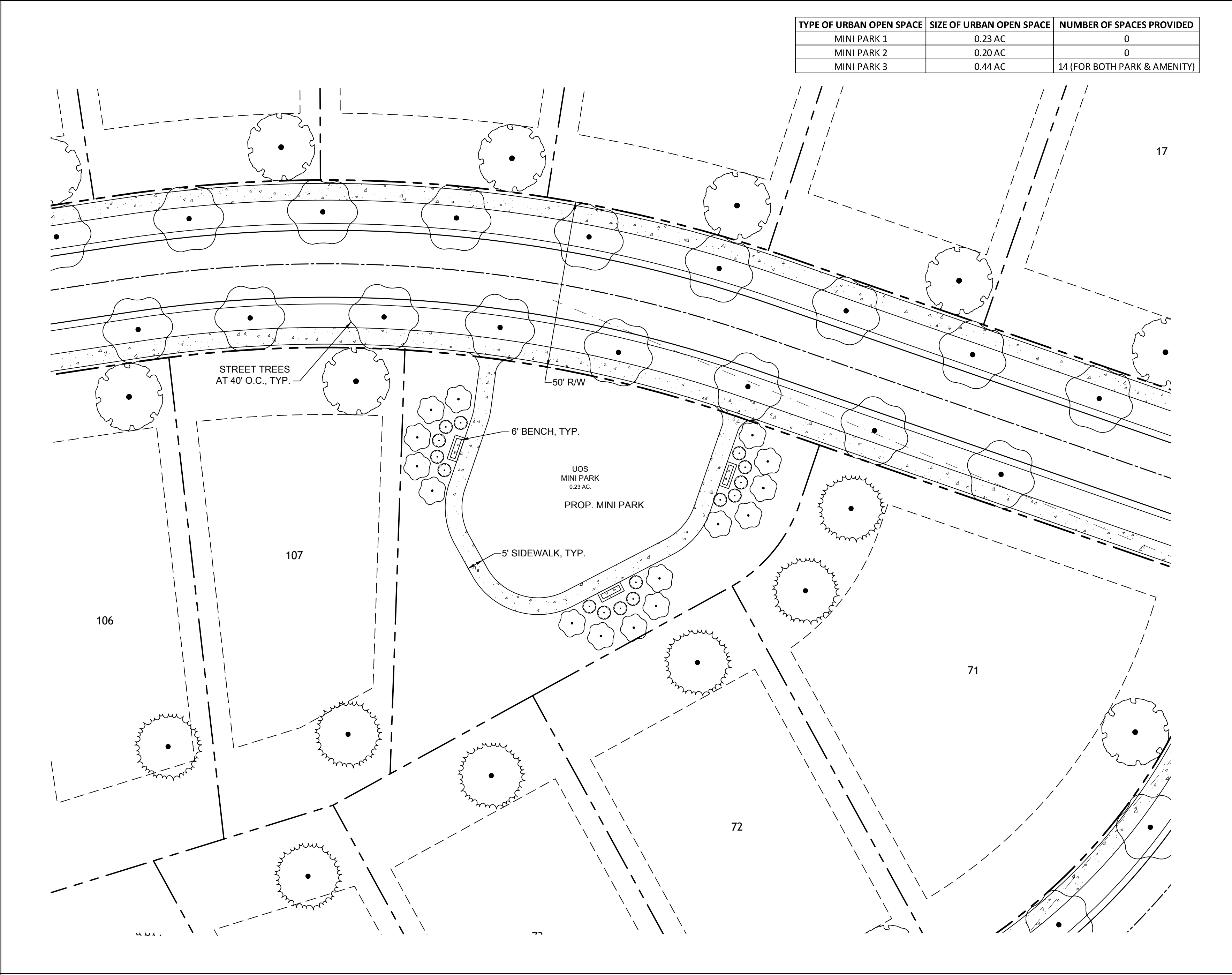


NOT USED



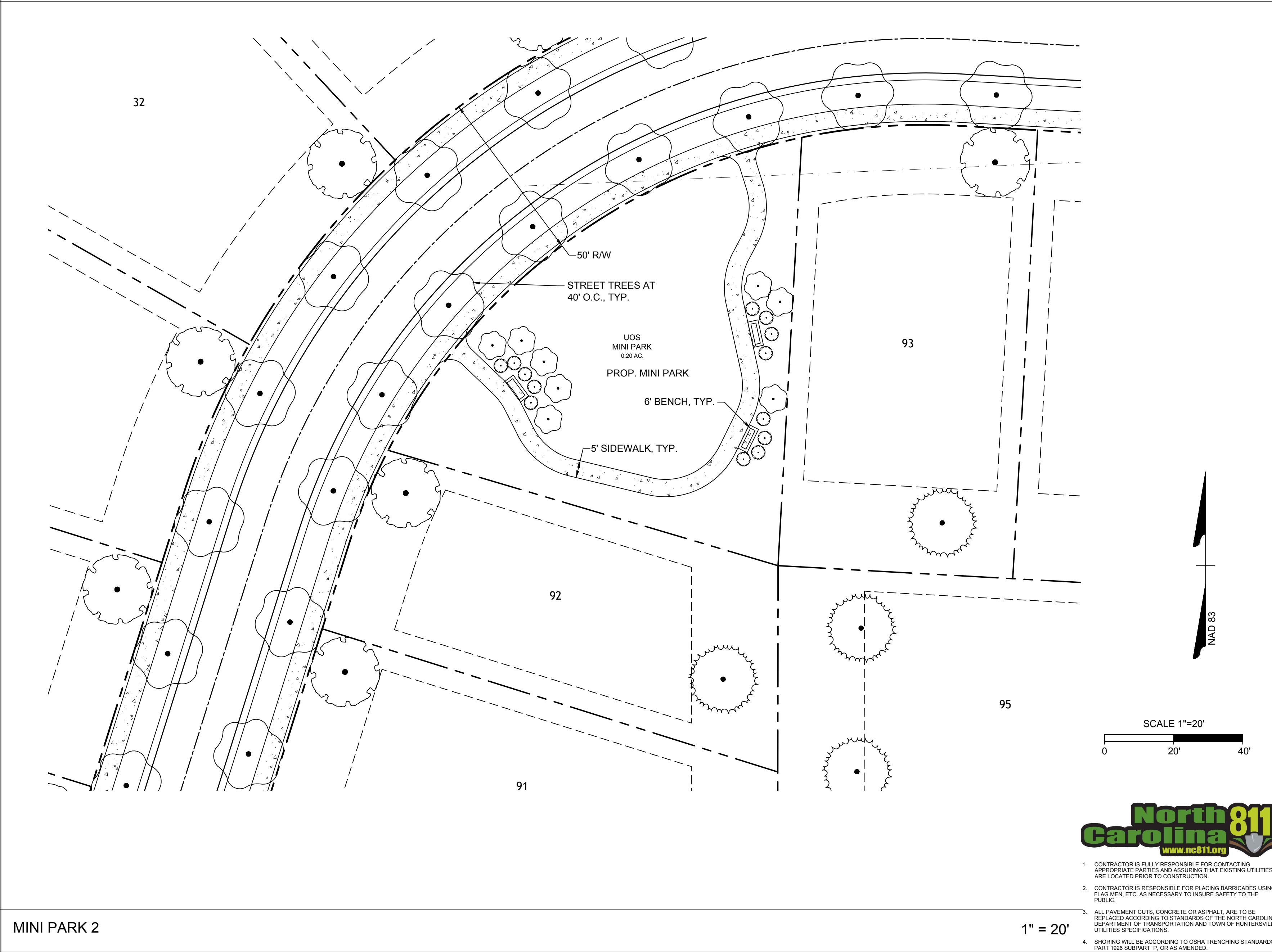
MINI PARK 3

1" = 30'



MINI PARK 1

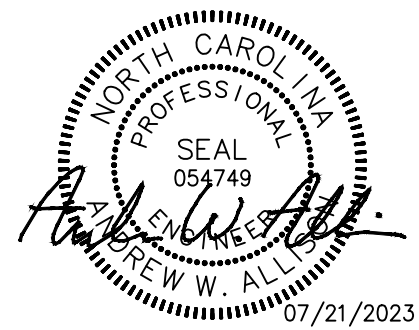
1" = 20'



MINI PARK 2

1" = 20'

TYPE OF URBAN OPEN SPACE	SIZE OF URBAN OPEN SPACE	NUMBER OF SPACES PROVIDED
MINI PARK 1	0.23 AC	0
MINI PARK 2	0.20 AC	0
MINI PARK 3	0.44 AC	14 (FOR BOTH PARK & AMENITY)



PRELIMINARY
FOR REVIEW
PURPOSES ONLY

THIS DRAWING PREPARED AT THE
CHARLOTTE OFFICE
610 E. Morehead Street, Suite 250 | Charlotte, NC 28202
TEL 704.602.8600 FAX 704.376.1076 www.timmons.com
North Carolina License No. C-1652



REVISION DESCRIPTION

REVISED PER TOWN COMMENTS

DATE

07/21/2023

DATE

07/21/2023

DRAWN BY

A. CLARK

DESIGNED BY

A. ALLISON

CHECKED BY

A. ALLISON

SCALE

AS SHOWN

TIMMONS GROUP
YOUR VISION ACHIEVED THROUGH OURS.

EPCON - COURTYARDS AT WALTERS FARM
HUNTERSVILLE, NORTH CAROLINA

CONCEPTUAL URBAN OPEN SPACE PLAN

JOB NO.

57770

SHEET NO.

RZ-500



- CONTRACTOR IS FULLY RESPONSIBLE FOR CONTACTING APPROPRIATE PARTIES AND ASSURING THAT EXISTING UTILITIES ARE LOCATED PRIOR TO CONSTRUCTION.
- CONTRACTOR IS RESPONSIBLE FOR PLACING BARRICADES USING FLAG MEN ETC. AS NECESSARY TO INSURE SAFETY TO THE PUBLIC.
- ALL FINISHMENT CURB, CONCRETES OR ASPHALT ARE TO BE INSTALLED ACCORDING TO STANDARDS OF THE NORTH CAROLINA DEPARTMENT OF TRANSPORTATION AND TOWN OF HUNTERSVILLE UTILITIES SPECIFICATIONS.
- SHOWING WILL BE ACCORDING TO OWN TRENCHING STANDARDS PART 108 SUBPART F, OR AS AMENDED.

Beatties Ford Road Subdivision – Neighborhood Meeting Summary

- Location Huntersville Arts and Cultural Center
- Scheduled for 6pm. David Peete requested to hold off meeting start to account for traffic (began 6:03pm)

Beginning of Meeting:

- Whitney started it off – introduced the EPCON team, engineering team
- John Shamp – brief overview on what EPCON does
 - 55+ communities – age restricted
 - Emphasized private courtyards – every project has ‘courtyards’ in the name
 - Emphasized open space behind the lots (no decks, trampolines, swings, etc.)
 - All manicured lawns, sprinkler systems, etc.
 - Front/rear of homes maintained by HOA
 - All open space
 - Referenced “courtyards at Huntersville” as an example – up the road from Beatties project
 - Went into the benefits
 - Generate 50% less traffic than traditional neighborhoods
 - Higher tax revenues – average price over 600,000
 - Lower services costs
 - Low school impacts
 - Less than 3% of homes have school age children
 - High quality architecture and landscaping – no vinyl
 - Local economy – residents have resources to support local businesses
- Whitney – describing project
 - 118 units, main road off Beatties
 - Left and right turn lane with appropriate storage
 - Providing stubs for potential future development
 - Also tying into Riverdale
 - Urban Open Space – (3) mini parks
 - Other open space to be left undisturbed
 - Tree buffers around most of the development

Questions/Responses

Unidentified Resident - Are you providing access to greenway?

Not currently

Mary Nicholson – Will the entrance on Beatties Ford Road be the main entrance?

Yes, that will be the main entrance.

Christine Summers – Will there be opportunity or be ability to access the neighborhood via the road connecting to the Riverdale subdivision to the south?

Yes, residents will be able to access development through Riverdale

Joe Sailors – What are the open areas along the tree line to the north? Is there going to be a walkway along creek and lake? Since these are all ‘old people’ – they like to walk.

No, not proposing walkway along creek currently.
Pond is not existing – but will be landscaped.

Joe Sailors - Is TR zoning okay with town?

David Peete – Beatties road doesn’t support TR but as a subdivision it meets the requirements.

Whitney – we are looking to feather-in some density; mix up the densities along Beatties Ford Road

Unidentified Resident – can you define a wetpond?

Pond to treat stormwater. We will be requesting a modification to the ordinance to propose a wetpond here.

Unidentified Resident – is access to pond restricted? Will there be a fence?

There will be an easement, no fence. Pond will be landscaped to provide a more “natural feel”.

Dan Boone –

When will the HOA take over?

At 75% occupancy, it will be turned over to HOA

Will property owners to the left be able to use the pond?

No, pond will not be engineered in a way that would allow others to use it

Are you looking for any relief on Buffers?

Yes, we are looking for relief on the 40' buffer along the southern portion of the property. We will hold 20' along Riverdale and will replant as required per the ordinance. Asking for modification to grade within 20' of the 40' buffer. 20' closest to the property line will not be touched.

Will car lights shine in the windows across from entrance?

No, there are no homes directly across from entrance.

Unidentified Resident – plans online show no buffer along right hand side.

Buffer will be held where required by the ordinance and replanted per the ordinance if disturbed for grading activities.

Unidentified Resident – is there a drawing of what the entrance looks like? How far down will these go? Can you tell me exactly where the turn lanes will be? Is there a stoplight?

Nothing will go past the church property. Entire frontage will have turn lanes. Whole frontage of pasture will have turn lane – will stop at property corner. No stop light at this intersection.

Unidentified Resident – lets say everything goes perfectly – what is estimated project start date? When does demo/grading start?

May of 2024. We will start earlier if possible, but need to follow Town process to get all permits.

Unidentified Resident - Will this be split into phases? Will you build roads first, in sections, certain homes?

We will do as much grading as possible to get the cut/fill ratio balanced all in one go. Pave enough to get a certain number of homes started. Then see how many homes we can accomplish. Start with around 30 homes.

Follow up question - how long do you hope it takes to get the first homes to sell?

May 2025, 17ish months

Unidentified Resident - Initially do you plan to do work Monday-Friday? When you start construction, is it a 7-day deal? Trying to get my head around the vehicles that will be in front of the farm.

7 days. We want that availability to account for weather.

Unidentified Resident - Who is responsible for maintaining Beatties Ford Road in regards to construction vehicles coming/going to development? Dirt/debris? Huge detriment on roads from construction equipment along Beatties. Sometimes cannot get out of driveway.

Anything that comes out of site, we are responsible for. Any damage done to road falls to DOT enforcement. Part of preliminary plan process is to work with DOT to make sure we follow their requirements.

Unidentified Resident - what are the benefits to the neighboring homes?

If not us, then who?

Eric Deitrich–

That 20' buffer line along, there is currently a power line running through site. What is this for and what will happen to the power line?

There is a mobile home in the back of the property. Power line is on our site of the buffer, so it will be removed.

Is power line within buffer?

Line will be abandoned. Will hold at least 40' from power line. Trees between power lines and property line will remain if possible. Whitney also mentioned 100' panting buffer at the front of the development

David Peete – Wanted to elaborate on lights/noise. Requirements do not go away during construction. Police make the call. M-S 7 to 8, Sunday - noon to 8. We do not usually see any major issues.

Unidentified Resident – are the houses all single story?

They are not all single story. Some have bonus room option.

Unidentified Resident – Will there be a privacy fence along rear of lots?

No, there will not be a solid privacy fence behind every home. Will install privacy fence as needed. Folks want both options – completely private and to enjoy the open space behind their home.

Frank Gammon -

Have you gotten the TIA done?

We do not meet the threshold – not required.

When in the process will lanes be installed? Beatties is busy at rush hour. Will help with traffic for both normal and construction traffic. Go out there at peak traffic hours and see for yourself.

Whitney asked David Peete if there will be a traffic light going in. Design is started.
Traffic at Gilead – 99% of traffic takes right turn

David Peete – DOT owns Beatties so they have deciding factor. Don't have firm date in mind on when traffic light is in. Looking at other parallel roads as well – we'd like to replicate Beatties Ford. Work is unknown and unfunded.

Whitney – last questions?

-no further questions

Meeting adjourned @ 6:45pm

**Town of Huntersville
Town Board
August 7, 2023**

To: Town Board

From: Lora Mastrofrancesco, Transportation Engineer/Project Manager

Date: August 7, 2023

Subject: Resolution - Abandon Portion of Mt. Holly-Huntersville Road

EXPLAIN REQUEST:

Resolution Order to Abandon and close a Portion of Mt Holly-Huntersville Rd.

ACTION RECOMMENDED:

Approval

FINANCIAL IMPLICATIONS:

None

ATTACHMENTS:

1. Resolution - Order to close ROW - Mt Holly Huntersville Section 2023.8.7

**Resolution Order to Abandon and
Close a Portion of Mt Holly-Huntersville Rd**

WHEREAS, Mr. Charles S. Guignard has filed a petition to close a part of Mt Holly-Huntersville Road, in the Town of Huntersville, as further described in Exhibit A – Legal Description; and

WHEREAS, N.C.G.S. § 160A-299 allows for a municipality to permanently close any street or public alley; and

WHEREAS, said resolution of intent to close the street was published for a period of once a week for four successive weeks; and

WHEREAS, said resolution of intent was sent by mail to all owners of property adjoining the streets, and a notice of closing and public hearing was prominently posted in at least two places along the streets; and

WHEREAS, a public hearing was held on the 17th day of July, 2023, where the Board of Commissioners determined that the closing of a portion of Mt. Holly-Huntersville Rd is not contrary to the public interest, that no individual, firm or corporation owning property in the vicinity thereof will be deprived of reasonable means of ingress and egress to his or its property, and is contrary to the adopted policy to preserve existing right of way for connectivity.

WHEREAS, the Board desires to, through this Order and pursuant to N.C.G.S. § 160A299, order the closing of a portion of Mt Holly-Huntersville Road, as further described in Exhibit A.

NOW THEREFORE, BE IT RESOLVED AS FOLLOWS:

1. The Board hereby, through this Order, orders the closure of a portion of Mt Holly-Huntersville Road, as further described in Exhibit A.
2. This Resolution shall be effective as of the date of its adoption.
3. This Order shall be recorded in the Mecklenburg County Register of Deeds.

Adopted this the 7th day of August 2023.

Attest:

Clerk to the Board

Mayor, Town of Huntersville

Approved as to Form:

Town Attorney



EXHIBIT A - LEGAL DESCRIPTION TO ABANDON A PORTION OF A STREET

The properties now or formerly belonging to Charles S Guignard as recorded in Deed Book 17489 Page 813 and Deed Book 28947 Page 581 of the Mecklenburg County Register of Deeds. Parcel address is 406 South Main Street, Huntersville, NC 28078.

Mt Holly-Huntersville Road Right of Way Area 1:

Beginning at a computed point in the center of the Right of Way of Mt Holly-Huntersville Road, said point being the following six calls from NGS Monument First, having NC Grid Coordinates of North: 607,581.34' and Easting: 1,451,923.55' S23°0'35"W 66.38' to a half inch rod in the centerline of the Norfolk Southern Railway, thence following the tracks S10°5'34"E 110.97' to a computed point, thence crossing South Main Street Right of Way S80°24'27"W 63.51' to a computed point, said point being in the common line of Don and Carol Darcy (Deed Book 04164 Page 467) and Charles Guignard (Deed Book 28947 Page 581), thence following the existing Right of Way of South Main Street N11°44'0"W 111.08' to a computed point, thence N68°2'23"W 17.78' to a computed point, thence N14°25'35"W 9.25' to a computed point in the centerline of the old Mt Holly-Huntersville Road the Point and Place of Beginning, thence along the west Right of Way of South Main Street and across the old road the following two calls N14°25'35"W 9.05' to a computed point, thence N18°52'42"E 7.78' to a computed point in the northern Right of Way of the old Mt Holly-Huntersville Road, thence with said right of way S69°21'36"W 215.87' to a computed point in the new Right of Way of Mt-Holly Huntersville road, thence with said Right of way S5°17'4"E 15.55' to a computed point in the centerline of the old Mt Holly-Huntersville Road, thence along the former road centerline N69°21'36"E 214.06' to the point and Place of Beginning, containing 3,205 square feet. All per a map dated May 23, 2023 prepared by Jay Decoursey, NC PLS # L-4156 and WSP USA. 128 Talbert Road, Suite A. Mooresville, NC 28117. Phone 704-662-0100.

Mt Holly-Huntersville Road Right of Way Area 2:

Beginning at a computed point in the southerly Right of Way of Mt Holly-Huntersville Road, said point being the following five calls from NGS Monument First, having NC Grid Coordinates of North: 607,581.34' and Easting: 1,451,923.55' S23°0'35"W 66.38' to a half inch rod in the centerline of the Norfolk Southern Railway, thence following the tracks S10°5'34"E 110.97' to a computed point, thence crossing South Main Street Right of Way S80°24'27"W 63.51' to a computed point, said point being in the common line of Don and Carol Darcy (Deed Book 04164 Page 467) and Charles Guignard (Deed Book 28947 Page 581), thence following the existing Right of Way of South Main Street N11°44'0"W 111.08' to a computed point, thence N68°2'23"W 9.21' to a computed point in the southern Right of Way of Mt Holly-Huntersville Road and the Point of Beginning, thence following said southern Right of Way line S69°21'36"W 223.48' to a computed point in the new Right of Way for Mt-Holly Huntersville Road (Deed Book 34950 Page 933), thence N5°17'4"W 15.55' to a computed point in the centerline of the old Mt Holly-Huntersville Road, thence along the former road centerline N69°21'36"E 214.06' to a computed point, thence across the old road and with the south Right of Way of South Main Street S14°25'35"E 9.25' to a computed point, thence S68°2'23"E 8.57' to the point and Place of Beginning, containing 3,250 square feet. All per a map dated May 23, 2023 prepared by Jay Decoursey, NC PLS # L-4156 and WSP USA. 128 Talbert Road, Suite A. Mooresville, NC 28117. Phone 704-662-0100.

Decoursey, Jay
B.
(USJD672823)

Digitally signed by Decoursey, Jay B.
(USJD672823)
DN: cn=Decoursey, Jay B.
(USJD672823), ou=Active,
email=Jay.Decoursey@wsp.com
Date: 2023.05.23 10:06:41 -04'00'



**Town of Huntersville
Town Board
August 7, 2023**

To: Town Board

From: David Lucore, Electric System Manager

Date: August 7, 2023

Subject: Purchase Agreement for Electric Distribution Substation Property

EXPLAIN REQUEST:

Electricities needs to purchase land for an electric distribution substation. Duke has offered to sell the Town 1.13 acres of a 3.60 acre tract for \$466,125.

ACTION RECOMMENDED:

Approve purchase agreement.

FINANCIAL IMPLICATIONS:

\$466,125

ATTACHMENTS:

1. Town of Huntersville - DEC Seller - Sam Furr Retail (EMD and Reserve ROW)
FINAL COPY 8-7-23
2. Sam Furr Road Property Exhibit Sketch Cut to HVL

STATE OF NORTH CAROLINA
COUNTY OF MECKLENBURG

Property No.: 003596
Land Unit: 0042043
Project No.: 003596-859797

CONTRACT TO SELL AND PURCHASE REAL ESTATE

This Contract (this "Contract"), is made as of _____, 2023 (the "Effective Date"), by and between **DUKE ENERGY CAROLINAS, LLC**, a North Carolina limited liability company, hereinafter referred to as "Seller", and **TOWN OF HUNTERSVILLE**, a North Carolina municipal corporation, hereinafter referred to as "Buyer";

WITNESSETH:

That for and in consideration of the mutual covenants, agreements and undertakings set forth herein, Seller agrees to sell to Buyer and Buyer agrees to purchase from Seller a fee simple interest in that certain real property, together with all the rights, easements, privileges, hereditaments and appurtenances pertaining thereto, hereinafter referred to as the "Property", located in Huntersville Township, Mecklenburg County, North Carolina, as more particularly described as follows:

An approximately 1.13 ± portion of Parcel ID Number 00911112 shown on **Exhibit A**, attached hereto and incorporated herein by reference, located in Huntersville Township, Mecklenburg County, North Carolina, and acquired by Seller in that deed recorded in Deed Book 3465, Page 195, in the Office of the Register of Deeds of Mecklenburg County.

- 1. PURCHASE PRICE:** The total purchase price for the Property (the "Purchase Price") is **Four Hundred Sixty-Six Thousand One Hundred Twenty-Five and No/100 Dollars (\$466,125.00)**, to be paid as follows:
 - A. Forty-Six Thousand and No/100 Dollars (\$46,000.00) in "Earnest Money" to be paid by Buyer to Seller's designated closing attorney or escrow agent within five (5) days of the latter of Buyer being notified of the recipient or the Effective Date as a partial payment of the Purchase Price as provided in Paragraph 1.B below.
 - B. Four Hundred Twenty Thousand One Hundred and Twenty-Five and No/100 Dollars (\$420,125.00) the balance of the Purchase Price, in cash, or its equivalent, at Closing (as defined in Paragraph 8) after title to the Property has been updated and reveals that title to the Property can be conveyed in accordance with this Contract and the Deed (as defined in Paragraph 7) has been recorded in the applicable public registry, or as otherwise provided herein.
- 2. POSSESSION:** Possession of the entire Property will be given to Buyer upon Seller's execution and delivery of the Deed to Buyer.
- 3. INVESTIGATION PERIOD AND BUYER'S ELECTION:** Buyer shall have a period of time (hereinafter referred to as "Investigation Period") beginning on the Effective Date and concluding at 5:00 PM on the date which is six (6) months after the Effective Date, to conduct all studies, surveys and investigations of the Property, including environmental audits and testing (subject to the terms and provisions hereof) (hereinafter collectively referred to as "Investigations") to determine in Buyer's sole judgment if it is feasible for Buyer to purchase the Property; provided, however, Buyer shall not be entitled to conduct any environmental Investigations on the Property beyond a Phase I environmental site assessment (i.e., no sampling, drilling, etc.) without the prior written consent of Seller, which may be granted, withheld or conditioned in Seller's sole discretion. Buyer shall not interfere with normal business operations of Seller on the Property during the Investigation Period. Immediately upon completing the Investigations, Buyer, at its sole cost and expense, shall restore the Property to substantially the same or better condition as same existed prior to such Investigations. Buyer shall indemnify, defend and hold Seller harmless from and against any and all costs, liabilities, and claims, including legal fees and court costs, arising from, caused by, or resulting from, the action or inaction of Buyer, any agent or contractor or other representative of Buyer. Buyer's obligations contained within the immediately preceding two (2) grammatical sentences (collectively being the "Survival Obligations") shall survive the termination of this Contract and the Closing indefinitely. Buyer shall promptly provide Seller with the results of any Investigations made hereunder upon the completion thereof. If such Investigations do not, in the sole discretion of Buyer, warrant the purchase of the Property, then Buyer may deliver written notice to Seller, prior to the expiration of the Investigation Period, that it is not feasible for Buyer to purchase the Property, whereupon this Contract shall terminate, and neither Buyer nor Seller will have any further rights or obligations under this Contract (except for the Survival Obligations). The failure of Buyer to provide such notice of termination prior to the expiration of the Investigation Period shall be deemed conclusively a waiver of Buyer's termination rights under this Paragraph 3.

IF BUYER DOES NOT EXERCISE ITS RIGHT TO TERMINATE THIS CONTRACT PRIOR TO THE EXPIRATION OF THE INVESTIGATION PERIOD AS PROVIDED IN THIS PARAGRAPH 3, BUYER SHALL BE DEEMED TO BE SATISFIED WITH ALL ASPECTS OF THE PROPERTY (INCLUDING, WITHOUT LIMITATION, THE ENVIRONMENTAL CONDITION) AND SHALL ACCEPT THE PROPERTY AT CLOSING “AS IS” AND WITH ALL FAULTS.

4. SELLER’S ENVIRONMENTAL INVESTIGATIONS: Seller may, during the Investigation Period, conduct its own environmental testing on the Property to determine if, in Seller’s sole discretion, the Property is environmentally acceptable for sale. Seller may disclose, **without warranty**, the results of any environmental testing conducted by Seller to Buyer. Any disclosure relating to environmental issues shall contain the following disclaimer:

Attached you will find environmental information on the above referenced Property. The scope of Duke Energy Carolinas, LLC’s environmental investigation does not include all possible contaminants. As a result, this report may not represent all the environmental considerations at the site. Duke Energy Carolinas, LLC encourages you to conduct your own environmental assessment of the Property to determine if the Property is suitable for your intended use.

*This information is provided to you for the purpose of assisting you in your own environmental assessment of the Property. **DUKE ENERGY CAROLINAS, LLC MAKES NO WARRANTY WHATSOEVER, EXPRESS OR IMPLIED, REGARDING THE ENVIRONMENTAL CONDITION OF THE PROPERTY, THE EXISTENCE OF ANY ENVIRONMENTAL CONTAMINATION UPON THE PROPERTY, THE ACCURACY OF THE INFORMATION SUPPLIED OR THE SUITABILITY OF THE PROPERTY FOR ANY SPECIFIC USE.***

5. SELLER’S ELECTION: Should environmental investigations conducted by either Buyer or Seller reveal the presence of hazardous materials on the Property, Seller may, at its sole option, elect to remediate said hazardous material in accordance with this Paragraph 5 or to terminate this Contract, and after such termination, neither party shall have any further rights or obligations hereunder, except for the Survival Obligations. Buyer agrees that if Seller elects to remediate said hazardous material, Seller shall have access to the Property subsequent to Closing to perform remediation operations. Buyer further acknowledges and agrees that upon completion of any remediation of hazardous material by Seller hereunder that certain hazardous materials may remain on the Property provided the levels of such remaining hazardous materials are deemed acceptable by state and federal guidelines. Subject to the foregoing, Seller agrees that if remediation operations are performed, the Property will be restored to a condition comparable to its condition on the date of commencement of remediation, except for the hazardous materials that are remediated.

6. SURVEY: Buyer shall cause a survey of the Property, at Buyer’s expense, to be performed by a North Carolina Registered Licensed Surveyor. The survey shall include any facilities, rights of way, and easements owned by Seller or to be reserved by Seller to be performed by a North Carolina Registered Licensed Surveyor. Said survey shall be provided to Seller at least thirty (30) days in advance of the end of the investigation period. Before the end of the Investigation period, Buyer may, at its sole discretion, determine that the property is not feasible based on the rights of way and easements shown on the survey, and may terminate this Contract, whereupon neither Buyer nor Seller will have any further rights or obligations under this Contract (except for the Survival Obligations) and the Earnest Money shall be disbursed as set forth in this Agreement.

7. CLOSING COSTS AND PRORATIONS: All due and payable City and County ad valorem taxes for the Property for the year in which the Closing occurs shall be prorated to the date of Closing and shall be paid by Buyer. Buyer shall pay any and all ad valorem taxes for the Property for all years preceding the year of Closing prior to Closing.

Buyer shall pay the cost of any documentary or revenue stamps required to be paid in connection with the recording of the Deed and for the costs of preparing and recording any instruments required by Seller, Seller’s attorney, or Seller’s lender.

Buyer shall be responsible for the recording of the Deed. Buyer shall pay for preparation and recording of any and all instruments required by Buyer, Buyer’s attorney or Buyer’s lender.

Should this Contract expire, terminate, or be terminated for any reason other than by Seller in its sole discretion then Seller shall be entitled to received reimbursement for any actual expenses incurred by it in relation to this Contract or the obligations imposed upon it by this Contract. Such reimbursement shall be paid form the Earnest Money. The holder of the Earnest money shall pay the reimbursement to Seller and then release any remaining Earnest Money to Buyer. Seller shall not be entitled to reimbursement for any amounts in excess of the Earnest Money.

8. DEED: The special warranty deed conveying the Property from Seller to Buyer (the “Deed”) shall be prepared by Seller and submitted to Buyer for review at least seven (7) business days in advance of the Closing. With regard to the legal description of the Property to be included in the Deed, Seller may, in its sole discretion, take such legal description from its acquisition deed, from existing property descriptions or surveys in Seller’s possession, or from Buyer’s survey of the Property (if any).

9. CLOSING: The closing of the transaction contemplated by this Contract (the “Closing”) shall take place on or before **ninety (90) days** from the end of the Investigation Period. Closing shall occur at the offices of Buyer’s closing attorney or at a location mutually acceptable to both Buyer and Seller.

10. CONDITION OF TITLE: The Deed shall contain the following exceptions (the “Permitted Exceptions”):

- (a) Rights of Way to be reserved by Seller over the Property for any existing or contemplated distribution and or transmission power lines as well as access easements for such power lines and other needs of Seller. Reservation of said rights of way shall be in form of Seller’s then-standard right-of-way reservation language, a copy of which is attached hereto as **Exhibit B**.
- (b) Public streets and roads, visual easements, restrictions, and recorded rights of way.
- (c) All matters of survey and recorded plats (including matters that would be revealed by a current, accurate physical survey of the Property).
- (d) All easements, restrictions, rights of way and all other matters of record and all matters that would be revealed by a physical inspection of the Property.
- (e) Lien of the First and Refunding Mortgage given to The Bank of New York Mellon Trust Company, N.A. (formerly known as JPMorgan Chase Bank, N.A.), successor Trustee to Morgan Guaranty Trust Company, dated December 1, 1927, recorded in Book 686 at Page 311 in the Office of the Register of Deeds for Mecklenburg County (as amended). Seller agrees to apply for, obtain and record a release of said lien of Mortgage within one (1) year from the date of Closing and shall indemnify and save harmless Buyer from any and all damages, costs and expenses relating to Seller’s failure to obtain the release of said Mortgage. In the event Buyer cannot reasonably obtain title insurance from Buyer’s title insurance company because of this Section 10(e), Buyer shall be entitled to terminate this Contract, and neither Buyer nor Seller will have any further rights or obligations under this Contract (except for the Survival Obligations).

Seller shall provide Buyer with such affidavits as may be reasonably required by Buyer’s title insurance company attesting to the absence of any unrecorded materialmen’s liens relating to the Property. Acceptance by Buyer at Closing of the Deed from Seller shall constitute full performance by Seller in accordance with this Contract, except for warranties specifically provided herein (if any) that expressly survive the Closing

If Buyer shall discover any matters affecting the Property, other than the Permitted Exceptions, Buyer shall advise Seller in writing of any such matters to which it objects prior to the expiration of the Investigation Period, and Seller shall have a period of twenty (20) days from the date Seller receives such notice of said objections in which to remedy said objections to the reasonable satisfaction of Buyer or to refuse to remedy any such objections. In the event said objections are not cured or remedied within such twenty (20) day period or Seller refuses to remedy any such objections, then Buyer shall be entitled to terminate this Contract by giving written notice of such election to Seller within ten (10) days following the earlier of (i) the date Seller notifies Buyer of its refusal to satisfy any such objection(s), or (ii) the end of such twenty (20) day period, in which event neither party shall thereafter have any obligations hereunder, except for the Survival Obligations.

11. ASSIGNMENT: Seller specifically reserves the right to assign this Contract in connection with a tax-free exchange. Buyer shall be entitled to assign this Contract, but not without the prior written consent of Seller (which may be withheld, conditioned or delayed in Seller’s sole discretion).

12. DEFAULT AND REMEDIES: In the event Seller fails to perform any of the conditions or obligations of Seller under this Contract and Seller does not commence to cure such failure within twenty (20) days after receiving written notice thereof from Buyer, Buyer, as its sole and exclusive remedy, shall be entitled to either (i) terminate this Contract, after which Buyer and Seller shall have no obligations to one another hereunder except for the Survival Obligations, or (ii) commence an action against Seller for specific

performance of this Contract. In the event Buyer defaults or fails to perform any of the covenants and conditions of this Contract, then Seller shall be entitled to terminate this Contract.

13. INTENTIONALLY DELETED.

14. NOTICES: Any notices, requests, or other communications required or permitted to be given hereunder shall be in writing and shall be either (i) delivered by hand, (ii) mailed by United States registered mail, return receipt requested, postage prepaid, (iii) sent by a reputable, national overnight delivery service (e.g., Federal Express, Airborne, etc.) or (iv) sent by facsimile (with the original being sent by one of the other permitted means provided in this grammatical paragraph) and addressed to each party at the applicable address set forth herein. Any such notice, request, or other communication shall be considered given or delivered, as the case may be, on the date of hand delivery (if delivered by hand), on the third (3rd) day following deposit in the United States mail (if sent by United States registered mail), on the next business day following deposit with an overnight delivery service with instructions to deliver on the next day or on the next business day (if sent by overnight delivery service), or on the day sent by facsimile (if sent by facsimile, provided the original is sent by one of the other permitted means as provided herein in this grammatical paragraph). However, the time period within which a response to any notice or request must be given, if any, shall commence to run from the date of actual receipt of such notice, request, or other communication by the addressee thereof. Rejection or other refusal to accept or inability to deliver because of a changed address of which no notice was given shall be deemed to be receipt of the notice, request, or other communication. By giving at least ten (10) days prior written notice thereof, any party hereto may, from time to time and at any time, change its mailing address hereunder.

NOTICE TO SELLER: Duke Energy Carolinas, LLC
Data & Document Management ECII-05
526 South Church Street
Charlotte, North Carolina 28202

NOTICE TO BUYER: Town of Huntersville
Attn: Anthony Roberts, Town Manager
PO Box 664
101 Huntersville-Concord Rd
Huntersville, North Carolina 28078

15. APPLICABLE LAW: This Contract shall be governed by and construed in accordance with the laws of the state in which the Property is located.

16. RISK OF LOSS, DAMAGE OR REPAIR: Until Closing, the risk of damage or loss to the Property, except as otherwise provided herein, shall be borne by Seller. In the event the Property is damaged between the Effective Date and Closing so that it cannot be conveyed in substantially the same condition as it was as of the Effective Date, Buyer may elect to terminate this Contract, and neither party shall thereafter have any rights or obligations hereunder, except for the Survival Obligations. Except for maintaining the Property as provided herein, Seller shall have no responsibility for the repair of the Property, including any improvements, unless both parties agree in writing.

17. AGENTS: Seller and Buyer represent and warrant to each other that there are no brokers, agents or other persons who are or will be entitled to a commission, fee or other similar compensation relating to this Contract or the transactions contemplated hereby other than the following:

For Buyer: _____ N/A _____
For Seller: _____ N/A _____

Each party agrees to defend and hold harmless the other in the event any claim for commission should be brought against either party for payment of any alleged commission allegedly due because of the acts or alleged acts of the other party.

18. SURVIVAL OF WARRANTIES AND CONDITIONS: Except as otherwise expressly provided herein, all conditions, warranties, representations and agreements made herein shall survive Closing and delivery of the Deed for a period of six (6) months.

19. ENTIRE AGREEMENT: This instrument (and any exhibits or addenda attached hereto) contains the entire understanding and agreement by and between the parties and all prior or contemporaneous oral or written agreement or instruments are merged herein. No amendment to this Contract shall be effective unless the same is in writing and signed by the parties hereto.

20. MISCELLANEOUS:

- a. The provisions of this Contract shall inure to the benefit of, and shall be binding upon, the parties hereto and their respective heirs and permitted successors and assigns, as may be applicable.
- b. TIME IS OF THE ESSENCE in this Contract. In addition, if the final day of any period of time set out in any provision of this Contract, falls on a Saturday, Sunday or holiday recognized by Bank of America, N.A., or any successor thereto ("Bank of America"), in Charlotte, North Carolina, then in such case, such period shall be deemed extended to the next day which is not a Saturday, Sunday or holiday recognized by Bank of America in Charlotte, North Carolina.
- c. No presumption shall be created in favor of or against Seller or Buyer with respect to the interpretation of any term or provision of this Contract due to the fact that this Contract was prepared by or on behalf of one of said parties.
- d. The captions used in connection with the paragraphs of this Contract are for reference and convenience only and shall not be deemed to construe or limit the meaning of the language contained in this Contract or be used in interpreting the terms and provisions of this Contract.
- e. This Contract may be executed in two or more counterparts and shall be deemed to have become effective when and only when one or more of such counterparts shall have been signed by or on behalf of each of the parties hereto (although it shall not be necessary that any single counterpart be signed by or on behalf of each of the parties hereto, and all such counterparts shall be deemed to constitute but one and the same instrument), and shall have been delivered by each of the parties to the other.
- f. If any provision of this Contract is held to be illegal, invalid or unenforceable under present or future laws, such provision shall be fully severable; this Contract shall be construed and enforced as if such illegal, invalid or unenforceable provision had never comprised a part of this Contract; and the remaining provisions of this Contract shall remain in full force and effect and shall not be affected by the illegal, invalid or unenforceable provision or by its severance from this Contract. Furthermore, in lieu of such illegal, invalid or unenforceable provision, there shall be added automatically as a part of this Contract a provision as similar in terms to such illegal, invalid or unenforceable provision as may be possible and be legal, valid or enforceable.
- g. Each party hereto represents and warrants to the other party that the execution of this Contract and any other documents required or necessary to be executed pursuant to the provisions hereof are valid, binding obligations and are enforceable in accordance with their terms.
- h. Should any distribution line or lines currently located on or in the vicinity of the Property need to be relocated to accommodate Buyer's use of the Property post-closing, then Buyer shall reimburse Seller for those projected costs up to One Hundred Thousand and no/100 Dollars (\$100,000.000), prior to or at Closing.
- i. Buyer shall be responsible for all costs associated with the Huntersville Zoning Ordinance Article 7.4, and related or successor provisions, relating to saving a percentage of the mature specimen trees currently existing on or in the vicinity of the Property and/or the requirement for additional landscaping for buffer or screening purposes.

IN WITNESS WHEREOF, Seller and Buyer have caused this Contract to be executed, this the _____ day of _____, 2023.

SELLER:

DUKE ENERGY CAROLINAS, LLC

BUYER:

TOWN OF HUNTERSVILLE

By: _____

Name: _____

Title: _____

By: _____

Name: _____

Title: _____

Exhibit B

DISTRIBUTION LINE RIGHT OF WAY

Grantor for itself, its successors and assigns, reserves over and across the land conveyed in fee above, a perpetual easement and right of way for the purposes hereinbelow set out, and consisting of the following rights, privileges and easements to wit

OVERHEAD DISTRIBUTION LINE RIGHT OF WAY

Grantor reserves for itself, its successors and assigns, a perpetual easement and right of way for the purposes hereinbelow set out, over and across the portion of the Property more particularly shown on the Plat labeled "D.E.C. OVHD Distribution Line 30' R/W To Be Retained" (the "Overhead Distribution Strip"). Within the Overhead Distribution Strip above referred, Grantor shall have the right to construct, maintain and operate with poles, lighting fixtures, crossarms, wires, guys, anchors, cables, transformers and other apparatus and appliances, overhead lines for the purpose of transporting electricity and/or providing lighting services and for the communications purposes of the Grantor and regulated telephone utilities. The following rights are also reserved by Grantor: to enter said Overhead Distribution Strip to inspect said lines, equipment and facilities; to perform maintenance and repairs, and to make alterations and additions thereto; to remove from the Overhead Distribution Strip, now or at any time in the future, trees, structures or other obstructions that may endanger the proper maintenance and operation of said lines or other facilities or equipment and trees of any species that Grantor determines will grow at maturity to a height that will endanger the proper maintenance and operation of said lines or facilities or equipment; to trim or remove and to keep trimmed or removed dead, diseased, weak or leaning trees or limbs outside of the Overhead Distribution Strip which, in the opinion of Grantor, might interfere with or fall upon the electric, lighting, telecommunications, or other communications facilities within the Overhead Distribution Strip; and to install guy wires and anchors extending beyond the limits of the Overhead Distribution Strip.

Grantor further reserves the right to relocate its facilities and Overhead Distribution Strip over the Property to conform to any future highway or street relocation, widening or improvement.

UNDERGROUND DISTRIBUTION LINE RIGHT OF WAY

Grantor reserves for itself, its successors and assigns, a perpetual easement and right of way for the purposes hereinbelow set out, over and across the portion of the Property to be agreed upon by Grantor and Grantee, (the "Underground Distribution Strip"). Within the Underground Distribution Strip above referred, Grantor shall have the right to construct, maintain and operate with poles, lighting fixtures, crossarms, wires, guys, anchors, cables, transformers and other apparatus and appliances, either above ground or below ground, to include transformers and service connections, for the purpose of transporting electricity, providing lighting services and for the communications purposes of Grantor. The following rights are also granted to Grantor: to enter said premises to inspect said lines, equipment and facilities, to perform maintenance and repairs, and to make alterations and additions thereto; and to clear the land within the Underground Distribution Strip and to keep it clear of trees, structures or other obstructions; and to clear that land outside the right-of-way strip within ten feet of the service door of any transformer or cabinet located within the Underground Distribution Strip and to keep the area within ten feet of said door clear of trees, structures or other obstructions.

TRANSMISSION LINE RIGHT OF WAY

Grantor, for itself, its successors and assigns, reserves over and across the land conveyed in fee above, a perpetual easement and right of way for the purposes hereinbelow set out, and consisting of the following rights, privileges and easements, to wit:

- (a) Grantor's Use of Right of Way Strip. Grantor reserves for itself and its successors and assigns, a perpetual easement within the Right of Way Strip (as defined herein) to construct, reconstruct, replace, rebuild, enlarge, modify, remove, inspect, repair, maintain, operate and use within the Right of Way Strip multiple lines for transporting electrical energy and for telecommunications and/or data uses of Grantor, its successors and assigns. As used herein, the "Right of Way Strip" shall refer to those areas or parcels of land containing ± acres, all as shown on a plat of survey entitled " ", dated , marked Map: , said Plat attached hereto as **Exhibit A** and incorporated herein by reference. Which lines may consist of single or multiple rows of poles, towers, or other structures (at appropriate intervals and without limitation as to number) and related footings and foundations; crossarms; insulators; aboveground and/or underground conductors, static wires, grounds, cables, conduits, electronic equipment, and other appurtenant apparatus, fixtures, hardware, and appliances; and guy wires and anchors inside and/or outside the Right of Way Strip to support Grantor's overhead facilities at angle points. Grantor shall have the right to: (i) clear and keep the Right of Way Strip free of all trees and other vegetation (except as provided in subsection (b) below), structures, and other objects of any nature including, without limitation, satellite signal receiver systems, billboards, signs, buildings, manufactured homes, mobile homes and trailers, graves, wells, retaining walls, racking, dumpsters, sheds, fire pits or barbecues, swimming pools and any associated decking, septic systems or storage tanks and systems (whether aboveground or belowground), flammable materials, building materials, wrecked or disabled vehicles or equipment, refuse of any type and all other objects (whether aboveground or belowground); and (ii) install and maintain roads within the Right of Way Strip and install gates in any fences located within the Right of Way Strip, to afford Grantor access to the Right of Way Strip.
- (b) Grantee's Use of Right of Way Strip. Grantee shall be entitled to use the Right of Way Strip for all purposes not inconsistent with the rights and easements herein reserved by Grantor, including the right to: (i) cultivate and harvest annual seasonal crops (not including orchards or timber); (ii) pave, improve and use the Right of Way Strip for vehicular parking, provided that such vehicles are operable and readily moveable under their own power and further provided that Grantee installs protective barriers satisfactory to Grantor for the protection of Grantor's facilities; (iii) use the Right of Way Strip for recreation, provided no structures or objects (aboveground or belowground) are erected or placed therein without the prior written approval of Grantor (which Grantor may withhold in its sole discretion); (iv) use and maintain existing roads and drives and sewer, water and other utility lines within the Right of Way Strip at their existing locations as of the date of this instrument; (v) construct, use, and maintain new paved or unpaved roads, streets and driveways and new water, sewer, drainage, and other utility lines or pipes crossing the Right of Way Strip, provided such facilities conform to the following requirements: (A) such facilities cross the Right of Way Strip from one side of the Right of Way Strip to the other side at an angle of not less than thirty (30) degrees between the center line of said facilities and the center line of the Right of Way Strip, (B) no road, street, or driveway shall intersect with any other road, street or driveway, in whole or in part, within the Right of Way Strip, (C) no portion of such facilities and their associated easement area, if any, is located within twenty-five (25) feet of any of Grantor's poles, towers, structures, guy wires, or guy anchors, (D) such facilities are constructed in such a manner as to withstand the weight of Grantor's heavy equipment, and (E) such facilities are constructed in strict compliance with all clearance requirements of Grantor and all other regulations and ordinances then applicable to electrical facilities; (vi) maintain existing fences, provided that Grantor may add gates to allow it access as set forth in subsection (a)(ii) above; (vii) build new fences on the Right of Way Strip with the prior written approval of Grantor (which Grantor may withhold in its sole discretion), provided any such new fences conform to the following requirements: (A) such fences shall not be attached to Grantor's poles, towers or structures, (B) such fences shall be installed at least twenty-five (25) feet from Grantor's poles, towers, structures, guy wires, and guy anchors, (C) such fences shall not exceed ten (10) feet in height (D) such fences shall cross the Right of Way Strip from one side of the Right of Way Strip to the other side at an angle of not less than thirty (30) degrees between the centerline of the fence and the center line of the Right of Way Strip, and (E) if a fence crosses the Right of Way Strip or makes part of it inaccessible to Grantor, Grantee shall install a gate pursuant to Grantor's specifications to allow free access required by Grantor's vehicles and equipment; and (viii) excavate, grade and fill, provided Grantee receives Grantor's prior written approval (which Grantor may withhold in its sole discretion), which approval may contain conditions including, without limitation, the allowable grade and distances from Grantor's facilities that cannot be excavated.
- (c) Grantor's Use of Property Outside of the Right of Way Strip. Grantor further reserves for itself, its successors and assigns, the right to enter upon the Property for the following purposes and uses:

- (1) to cut, fell and remove any and all trees on the Property that are or may become tall enough, in Grantor's opinion, to fall on or otherwise endanger a line or other facility or structure within the Right of Way Strip ("***Danger Trees***").
- (2) to gain access to the Right of Way Strip and Danger Trees at any time and from time to time by vehicles, equipment and pedestrians, provided that Grantor's use of the Property outside of the Right of Way Strip shall be confined to then-existing streets, roads, and driveways to the extent they provide sufficient access to the Right of Way Strip and/or Danger Trees by vehicles, equipment and pedestrians. If then-existing streets, roads and driveways do not provide sufficient access, then Grantor shall be entitled to use a reasonably convenient and feasible access route or routes over the Property to access the Right of Way Strip and/or Danger Trees and shall be entitled to construct and maintain a roadway or driveway for such purposes.

(d) Antennas and Related Equipment. Grantor reserves for itself and its successors and assigns, the following rights:

- (1) to attach antenna or other equipment or devices for wireless or other telecommunications or data transmission ("***Communications Equipment***") to poles, towers, or other support structures within the Right of Way Strip, including the right to add, modify, enlarge, and/or extend any poles, towers, or other support structures for such purposes.
- (2) to use one or more portions of the Right of Way Strip, having dimensions not exceeding twenty-five (25) feet by twenty-five (25) feet and located adjacent to or at the base of each such pole, tower or other support structure to which Communications Equipment is attached (each a "***Communications Area***") to construct, reconstruct, replace, rebuild, enlarge, modify, remove, inspect, maintain and use electronic equipment and other equipment necessary or desirable in connection with wireless or other communications from and to the Communications Equipment installed upon such pole, tower or other support structure. Grantor shall be entitled to designate the location of the Communications Areas and may relocate such Communications Areas within the Right of Way Strip if such pole, tower or other support structure to which Communications Equipment is attached is relocated.
- (3) to enter upon the Property at any time and from time to time to gain access to the Communications Areas and Communications Equipment by vehicles, equipment and pedestrians, provided that Grantor's use of the Property outside of the Right of Way Strip shall be confined to then-existing streets, roads, and driveways to the extent they provide sufficient access to the Communications Areas and/or Communications Equipment by vehicles, equipment and pedestrians. If then-existing streets, roads and driveways do not provide sufficient access, then Grantor shall be entitled to use a reasonably convenient and feasible access route or routes over the Property to access the Communications Areas and/or Communications Equipment and shall be entitled to construct and maintain a roadway or driveway for such purposes, provided that Grantee shall be entitled to relocate any such roadway or driveway constructed by Grantor for such purposes, at Grantee's sole cost and expense and after obtaining Grantor's prior written approval, elsewhere on the Property, but in such case, Grantee also must construct and install a comparable replacement roadway or driveway, at Grantee's sole cost and expense and without interrupting access to the Communications Areas and/or Communications Equipment. Grantor shall not unreasonably withhold written approval of Grantee's request to relocate such roadway or driveway hereunder; provided, however, that Grantor's failure to approve shall be deemed reasonable if reasonably convenient and feasible access to and from the Communications Areas and/or Communications Equipment is not afforded by the proposed replacement access route or routes.
- (4) to construct, reconstruct, replace, rebuild, inspect, maintain and use underground telephone and electrical lines to serve the Communications Equipment and Communications Areas, which underground lines may be installed along and generally parallel to the access route or routes established pursuant to subpart (d)(3) above. Provided, however, that if Grantee relocates a roadway or driveway pursuant to subpart (d)(3) above and within which Grantor has installed underground lines pursuant to this subpart (d)(4), then Grantee also must relocate such underground lines, at Grantee's sole cost and expense and without interrupting service to the Communications Areas and/or Communications Equipment along or in the vicinity of the access route or routes as relocated by Grantee.

(e) Grantor's Repair Obligation. Grantor shall repair damage to the Property, including roads, driveways and fences, resulting directly from Grantor's exercise of its rights granted herein. Provided, however, for purposes of the initial clearing of all trees which Grantor is entitled to cut and remove from the Property pursuant to Paragraphs (a) and (c) herein, said trees shall, upon

such cutting, become the property of Grantor. Nothing in this instrument shall impose upon Grantor any duty to repair or warn of any condition or any type of injury or damage to the Property existing prior to the date of this instrument nor shall Grantor have any duty to repair or warn of any condition or any type of injury or damage upon the Property caused by the Grantee, any third party, any Act of God, or any natural process, including, without limitation, erosion or conditions caused by vegetation.

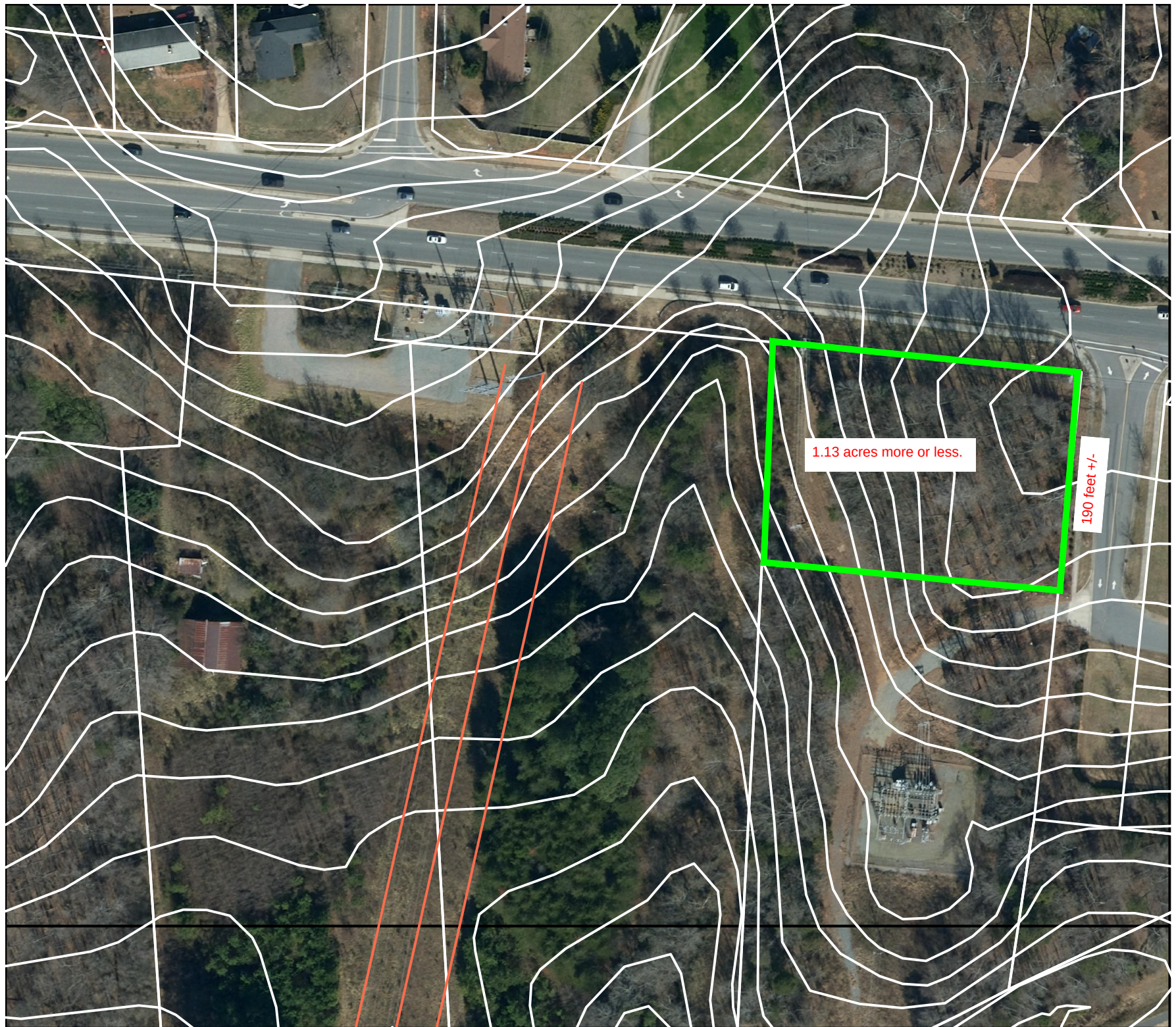
Grantor shall provide reasonable notice to Grantee prior to entering the property for any use associated with this agreement.

The failure of Grantor to exercise any of the rights herein granted shall not be construed as a waiver or abandonment of the right thereafter of at any time or from time to time to exercise any and all of such rights.

ACCESS ROAD RIGHT OF WAY

Seller reserves for itself and its successors and assigns a perpetual easement and right of way for ingress and egress for pedestrian and vehicular traffic over the Access Strip (as defined herein), together with the right to grade, level, fill, pave, build, maintain, repair and use a road on, over and across said Access Strip. As used herein, the "Access Strip" is described as follows:

That strip of land containing acres labeled " ," as shown on a plat of survey entitled " ", dated , marked Map: , and recorded in Book at Page in the Office of the Register of Deeds of Mecklenburg County, North Carolina.



1.13 acres more or less.

190 feet +/-

**Town of Huntersville
Town Board
August 7, 2023**

To: Town Board

From: Dan Boone, Commissioner
Amber Kovacs, Commissioner

Date: August 7, 2023

Subject: Downtown Social District Discussion

EXPLAIN REQUEST:
Downtown Social District Discussion.

ACTION RECOMMENDED:

FINANCIAL IMPLICATIONS:
N/A

ATTACHMENTS:
None