CHARLOTTE.

STATE OF NORTH CAROLINA
COUNTY OF MECKLENBURG

FIRST AMENDMENT TO AGREEMENT TO PROVIDE COMMUNICATION AND RECORD MANAGEMENT SERVICES

This First Amendment to the Agreement to Provide Communication and Record Management Services (the "Agreement") is entered into and made effective as of the ___ day of April, 2016 (the "Effective Date"), by and between the Town of Huntersville, a North Carolina municipal corporation (the "Town"), specifically the Huntersville Police Department (the "HPD"), and the City of Charlotte, a North Carolina municipal corporation (the "City"), specifically the Charlotte Mecklenburg Police Department (the "CMPD").

RECITALS

WHEREAS, the parties previously entered into the Agreement for the CMPD to provide communication and record management services to the HPD;

WHEREAS, the parities now wish to amend the Agreement to address electronic data storage; and,

WHEREAS, the parties desire to reduce the terms and conditions of electronic data storage to this written form.

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. Defined terms used in this First Amendment shall have the same meaning as are assigned to such terms in the Agreement.
2. The Agreement is hereby amended to add the following Section:

10. ELECTRONIC DATA STORAGE

10.1 Data Ownership

All HPD data submitted by HPD to the CMPD RMS program (KBCOPS) will remain the property of HPD to the fullest extent provided by law. The RMS program will retain HPD data indefinitely.

10.2 Data Sharing, Access and Security

HPD will have sole responsibility for the accuracy, quality, integrity, legality, reliability and appropriateness of all HPD data. CMPD will not share HPD data for any purpose unless agreed to in writing by HPD.

HPD is responsible for all activities that occur under HPD's User accounts. HPD is responsible for maintaining the security and confidentiality of all usernames and passwords. HPD agrees to notify CMPD immediately of any unauthorized use of the RMS program.

CMPD will use security measures to protect HPD data against unauthorized disclosure or use. This includes:

- Using database authentication with secure passwords;
- Locating the database behind a firewall;
- Implementing SSL;
- Requiring use of a Virtual Private Network for access from outside the network;
- Securing a duplicate copy of all HPD RMS data via Data Guard; and,
- Generating audit records for event logging of access to HPD RMS data.

10.3 Loss of Data, Irregularities and Recovery

CMPD conducts automatic backups of its systems, to include HPD data stored therein, pursuant to CMPD's internal backup policies, which may be modified in CMPD's sole discretion at any time without notice. If the RMS program is impacted by any failure or other incident resulting in data loss on CMPD's primary system, CMPD will take reasonable steps to restore the RMS program and HPD data from the most recent existing, unaffected backup available to it. CMPD makes no representations or warranties regarding its ability to recover any HPD data lost.

10.4 Data Retention and Redundancy

During the term of this Agreement, HPD, in compliance with applicable law, may extract and/or purge data at any time by accessing its data in the RMS program. HPD may extract all HPD data through written request to CMPD. At any time during the term of this Agreement, HPD may also make a written request to CMPD to purge all of the HPD data in compliance with applicable law. Upon termination of this Agreement, CMPD shall retain all HPD data for a minimum of ninety (90) days, and HPD may continue to submit to CMPD written requests to purge or retrieve HPD data. All Customer Data is returned to Customer in its native format or within a common computer delineated file. Thereafter, CMPD shall have no obligation to continue to hold, export or return HPD data, and HPD

acknowledges CMPD has no liability whatsoever for deletion of HPD data which may occur ninety (90) days after termination of this Agreement.

3. Except to the extent specifically provided herein, this First Amendment shall not be interpreted or construed as waiving any rights, obligations, remedies or claims the parties may otherwise have under the Agreement.

4. In all other respects and except as modified herein, the terms of the Agreement shall remain in full force and effect.

IN WITNESS WHEREOF, and in acknowledgment that the parties hereto have read and understood each and every provision hereof, the parties have caused this First Amendment to be executed on the date first written above.

ATTESTED:

CITY OF CHARLOTTE

BY: _____
ASSISTANT CITY MANAGER

TOWN OF HUNTERSVILLE

BY: _____
TOWN MANAGER

ATTESTED:

BY: _____
CITY CLERK

"This instrument has been preaudited in the manner required by the Local Government Budget Fiscal Control Act."

_____
Finance Officer **Date**

17.5.4

(M M M M) Electronic Data Storage

If the agency uses a service provider for electronic data storage, a written agreement is established addressing:

a. data ownership;

b. data sharing, access and security;

c. loss of data, irregularities and recovery;

d. data retention and redundancy;

e. required reports, if any; and

f. special logistical requirements and financial arrangements.

Commentary

Electronic data storage is an ever-evolving technology that can improve the administrative and operational efficiencies of public safety agencies. However, there are a number of issues that must be addressed when agencies elect to contract these services. Proper contractual agreements provide assurances that services will be provided in a manner that supports organizational needs in a manner that complements existing network infrastructures.

Agreements for contracted electronic data storage must address legal ownership of data and which entity retains ownership in the event the applicable contracts are terminated. It is also important to address the transfer of data and how much data will be stored by the vendor. Agencies may wish to specifically ensure sufficient data is retained to allow complete database reconstruction.

Security issues to address include defining the physical environment in which the data will reside and protections against natural and man-made disasters. Redundancy is a primary strategy to control for these issues and should be included in any data storage agreement. The loss of data occurring from criminal actions should be considered, as well as other issues that impact data integrity, such as unauthorized data access by contract personnel. Effective agreements for data storage should include protocol on the length of time data will be stored, as well as provisions for the destruction of data in accordance with applicable records retention laws.

Because expenditures associated with data storage can vacillate significantly over time with the introduction of new technologies, agency representatives should consider the development of agreements that allow for market pricing adjustments. Additionally, scheduled reviews of data storage contracts or agreements ensure the most appropriate mediums are used to support business needs.

An executed contract for services with a service vendor can be used to address the requirements of this standard. (M M M M)