NEW BERN
CITY OF NEW BERN

300 Pollock Street, P.O. Box 1129
New Bern, NC 28563-1129
(252) 636-4000

MEMORANDUM

TO: Tony Gatlin, IT Manager

FROM: Mark Stephens, City Manager 9/30/19

DATE: September 30, 2019

SUBJECT: Backup Retention Policy Waiver

Administrative Order 1.11, Data Backup and Retention Policy, specifies the required retention times for backups of data stored in the City's on-site backup system. As authorized in section 3.2 of that administrative order, I am issuing a waiver to reduce the maximum required data retention time on local backup devices to thirty (30) days. This waiver does not apply to required retention times for replicated copies of backups in the cloud.

This waiver is effective immediately and will remain in force until Administrative Order 1.11 is revised to modify required on-site backup retention times to a maximum of 30 days.

CITY OF NEW BERN
ADMINISTRATIVE ORDERS
OF THE CITY MANAGER

ADMISTRATIVE ORDER 1.11
To: All City Employees
From: Mark Stephens, City Manager 9/7/18
Maintained By: Information Technology
Subject: DATA BACKUP AND RETENTION POLICY
Date: September 5, 2018
Update to N/A

1. Introduction

Data is critical to both the daily operation of the City of New Bern's municipal government and to maintaining a historical record of those operations. The ability to backup and recover this data is vital to ensuring continuity of operations for the City government.

The intent of this policy is to establish governance to ensure that backups of the City's data are taken at appropriate frequencies, stored in a secure and accessible manner, maintained for the required retention times, and are periodically tested to verify that they can be restored as necessary.

2. Scope

This policy applies to all digital data owned by the City of New Bern. This includes data contained in City-owned computing infrastructure, personally owned devices such as smartphones and tablets used by City personnel in conjunction with the performance of their official duties, and in cloud services utilized by the City. Although this policy addresses some capabilities critical to disaster recovery and business continuity, it is not a comprehensive disaster recovery and business continuity plan.

3. Data Backup and Recovery Policy

3.1Application

Compliance with this policy is mandatory for all city personnel.

3.2 Procedural Waivers

The procedures defined in this document may be waived in part or in whole at the discretion of the City Manager, Assistant City Manager, or IT Manager as appropriate in a given circumstance. An official memorandum to all relevant parties shall document waivers. In a time-critical situation, the waiver may be issued verbally or via email, and the memorandum issued after the fact.

3.3 Definitions

Table 1 documents the definitions that are applicable to this document.

Backup	A copy of electronic data made for recovery purposes if the primary copy is corrupted or deleted.
City Personnel	Any elected official, employee, contractor, or volunteer who uses creates, modifies or otherwise utilizes electronic data and/or documents in the conduct of City business.
Cloud	A data center or group of data centers geographically separate from the City and accessible via the internet. Typically, a cloud data center will lease data storage and compute capabilities to provide for the recovery of data and/or execution of computer workloads when the customer's data and/or facilities have been destroyed or otherwise incapacitated. Cloud data centers may also act as the primary facility for their customers' data storage and workload execution. For the purposes of this document the term 'cloud' will be used generically to refer to any lease or subscription service which stores and/or processes City-owned data on infrastructure that is not owned or managed by the City, its officials or employees.
Data	Information in digital form that can be stored and processed electronically. Examples are word processor files, spreadsheets, photographs, video, and the contents of databases.
Data Owner	City personnel directly responsible for the management of a specific subset of the City's electronic data.
Data Set	Electronic information that can be treated as a uniform group with respect to determining frequency, retention and other factors related to its backup and recovery.
Personally Owned Device	An electronic device such as a smartphone or tablet owned by a City official, employee or contractor which has been authorized for use by that individual in the conduct of City business. The authorization process for personally owned devices is outside the scope of this document.
Restoration Priority	The relative priorities that are to be followed when determining the order of restoration for multiple data sets.

Restoration Time	The amount of time required to restore a backup copy of a data set to its normal location and make it available for use by City personnel.
Retention	The minimum amount of time that a backup must be kept before being discarded.
User	Person who operates a City computer.
Windows Workstation	A City desktop, laptop or tablet that runs the Windows operating system.

Table 1. Definitions

3.4 Data Owner Responsibilities

Data owners are responsible for identifying specific data sets that require backup, and for communicating that information to the IT Division.

Data owners are also responsible for developing and executing test plans to verify the accuracy and integrity of data restored from backups as part of a periodic quality assurance test or in response to actual data loss or corruption, and for providing the results of those tests to the IT Division for the purpose of process verification and improvement.

3.5 IT Division Responsibilities

The IT Division shall specify, budget for, acquire, configure and operate the infrastructure and services necessary to meet the requirements of this document.

The IT Division shall develop and execute a procedure for periodic data restorations in a test environment. The IT Division shall analyze the outcome of these restorations, including data owner test results, to verify that the backup and recovery infrastructure and processes meet design specifications.

The IT Division shall proactively help data owners understand and execute the responsibilities assigned to them in this document. Typically, this will include performing the business process and technical analysis necessary to ensure that backup infrastructure, processes and services acceptably mitigate the risk of data loss due to human error, malicious action, system malfunction, or natural disaster.

3.6 Cloud Services Data

Cloud data center vendors normally provide backup and restoration as a part of their service offerings. Ideally, a cloud service vendor's backup and restoration policy will mirror that of the City. In instances where this is not the case, the IT Division will work with the data owners to coordinate an acceptable backup, retention and restoration policy with the cloud vendor.

3.7 Windows Workstation Data

City personnel shall ensure that data stored on Windows workstations assigned to or used by them is available for backup. In practice, this means that all data stored on end-user workstations must be located under the Documents folder, or a sub-folder thereof.

3.8 Non-Windows Device Data

The IT Division is responsible for the development and implementation of backup capability for non-Windows devices where such capability is required. Backups of these devices shall comply with the policies defined in this document except in cases where a procedural waiver or technical limitations exist.

City personnel who are issued non-windows devices shall contact the IT Division for an analysis of their data backup requirements. The IT Division will determine the feasibility and cost of backing up data from these devices.

3.9 Personally Owned Devices

In general, personally owned devices should not be used to store the copy of record of City data. If circumstances require the copy of record to be stored on a personally owned device the owner of the device shall consult with the IT Division to determine a suitable process for making a periodic backup of the data.

3.10 Backup Retention[1]

Table 2 documents the standard frequency and retention times for backups.

Hourly[2]	7 Days	N/A
Daily	3 weeks	Once Daily[3]
Weekly	1 Month	N/A
Monthly	3 Months	N/A
Daily	7 days	N/A
Weekly	1 Month	N/A
Monthly	12 Months	N/A

Table 2. Backup Frequency and Retention Times

[1] Backup systems are intended solely to protect against data loss, and their design is fundamentally different from systems intended to meet legal record retention requirements. Consequently, backup retention times bear no relation to the record retention times dictated by law, statute, ordinance, or policy.

[2] Some intra-daily backups may be taken at frequencies other than hourly, depending on individual system requirements. The retention time will still be the same as for hourly backups.

[3] Only daily backups are replicated to the cloud. By contract, the cloud retention period is one year.

3.11 Backup Restoration Priority

To the extent possible, senior management shall determine and document restoration priorities in advance. In some cases, technical dependencies will dictate some or all restoration priorities. When multiple restorations are required, IT will first perform the restorations required by technical dependencies, and follow senior management's priority list for any remaining restorations.

If an approved priority list does not exist, the remaining restoration order will be determined by mutual agreement of the data owners. If mutual agreement cannot be reached, the lowest level manager having direct authority over all affected data shall determine the restoration priority.

3.12 Backup Restoration Times

The IT Division shall make every attempt to meet the backup restoration time requirements communicated by the owners of the data, subject to the technical capabilities of the backup and recovery system and to the relative restoration priorities assigned to competing restoration requirements.

3.13 Data Migration

Regular backups alone do not ensure that archived data remains usable. Data that is stored to meet record retention requirements is subject to becoming unusable over time if the software used to generate and read the data is no longer available or loses the ability to read data stored in older formats. It is the responsibility of data owners to budget for and initiate the remedial actions necessary to keep archived data usable. This includes, but is not necessarily limited to, periodically updating the format of the data so it is readable by currently available software and housing the data on a server with a fully supportable (i.e. not end of life) operating system.

4. Contact Information

Questions regarding this policy and procedure may be directed to the Information Technology Manager at 252-639-2782 or gatlint@newbern-nc.org.