CITY OF NEW BERN
ADMINISTRATIVE ORDERS
OF THE CITY MANAGER

INFORMATION TECHNOLOGY SECURITY POLICY
ADMISTRATIVE ORDER 1.9
To: All City Employees
From: Mark Stephens, City Manager 9/7/18
Maintained By: Information Technology
Subject: INFORMATION TECHNOLOGY SECURITY POLICY
Date: September 4, 2018
Update to N/A

1. Introduction

The City of New Bern's information technology (IT) systems contain a vast array of information and capabilities that are critical to the operation of the municipal government. The compromise of these systems can result in unacceptable disruptions to the City's ability to provide critical services, such as fire, police and utilities, to its citizens. A compromise can also result in the unauthorized modification, destruction or disclosure of information contained in those systems.

An effective IT security program is multifaceted. Its design is based upon the premise of "defense in depth", meaning that the systems and data are protected with multiple layers of technical, procedural and policy defenses. The theoretical objective of an IT security program is to prevent a system compromise from happening. While that is a worthy goal, in actual practice it is no more practical or achievable than setting a police department goal of zero crime or a fire department goal of zero fires. Consequently, the IT security program must be designed limit the impact to the overall system of a compromise of any part, and to provide recovery mechanisms to restore normal operations as quickly as practical after a compromise. A final complication is that every security measure applied to an IT system comes with a financial cost and some degree of increased complexity for the end users. Therefore, the true objective for an IT security program is to strike the right balance between acceptable risk, the cost of the security measures applied to the systems, and the impact to the usability of those systems for City personnel.

One of the primary keys to the successful implementation of an IT security program is ensuring that personnel who are granted access to the system understand their role in maintaining the integrity of the system and the information it contains. The purpose of this document is to establish mandatory security policies and best practice guidelines, which define the roles and responsibilities in protecting the City's computer systems against unauthorized access and the malicious, inadvertent, or improper disclosure, modification or destruction of information.

2. Scope

The policies and guidelines in this document apply to permanent and temporary employees, contractors, consultants, and any other personnel who are granted access to City IT systems.

3. Policy Directives

This document contains both policies and guidelines. Compliance with policies is mandatory unless a written waiver has been issued by the City Manager in accordance with section 3.1 of this document. Guidelines describe generally accepted industry best practices, and while compliance is not mandatory, it is strongly recommended.

3.1 Policy Waivers

The policies defined in this document may be waivered in part or in whole at the discretion of the City Manager. Waivers shall be communicated to the IT Division and all other relevant parties via an official memorandum describing the purpose, specifics and scope of the waiver.

3.2 Password Policy

The intent of the following policy and guidelines is to ensure the creation and protection of strong passwords, in accordance with generally accepted industry standards as well as the Police Department's requirement for compliance with Federal Bureau of Investigation (FBI) Criminal Justice Information System (CJIS) policy.

3.2.1 Password Construction Policy

Passwords shall comply with the requirements listed in Table 3.1. Some IT systems used by the City may not offer the capability for passwords to fully comply with these requirements. If this is believed to be the case, the IT Division shall be contacted to verify that the system cannot support the requirements in Table 3.1. Upon such verification, system users shall select passwords that comply as closely as the system will allow with the Table 3.1 requirements.

<table>
<tr><td colspan="2">A minimum of 8 characters in length</td></tr>
<tr><td colspan="2">Cannot be the same as any of the 10 previous passwords</td></tr>
<tr><td colspan="2">Cannot be a dictionary word or proper name</td></tr>
<tr><td colspan="2">Cannot be the same as the logon name or user ID</td></tr>
<tr><td colspan="2">Cannot contain more than two consecutive letters from the user's proper name</td></tr>
<tr><td rowspan="4">Must contain elements from at least 3 of these categories</td><td>Uppercase letters (A through Z)</td></tr>
<tr><td>Lowercase letters (a through z)</td></tr>
<tr><td>Base 10 digits (0 through 9)</td></tr>
<tr><td>Non-alphanumeric characters: ~!@#$%^&*()_-=+'\|[]{}<>.,?/</td></tr>
</table>

	Any Unicode character that is categorized as an alphabetic character but is not uppercase or lowercase, including characters from Asian languages

Table 3.1 – Password Construction Requirements

3.2.2 Password Expiration Policy

Passwords shall expire and be changed every 90 calendar days.

3.2.3 Password Usage and Protection Guidelines

System users should take all reasonable measures to protect the confidentiality of their passwords. Examples of this are:

- Do not share your password with anyone. If it is necessary for someone else to access a system with your password the preferred procedure is for you to log in to the system without disclosing the password and then turn the keyboard over to the other individual. It would also be a good idea to monitor what the individual is doing since any actions they take (emails sent, data accessed or modified, etc.) will be associated with your user account in the system security logs.
- If it is necessary to give your password to someone else, it should be changed immediately once the other person is finished using it. It is strongly recommended that you monitor what the other person does while logged into your account for the reasons listed in the previous bullet.
- It is best not to write your password down either on paper or in an electronic document. Since many employees have multiple passwords, it is recognized that it is not practical to expect that they all be committed to memory. If you must write passwords down in order to remember them, keep the document in a secure location that you have control of at all times.

3.2.4 Password Policy Enforcement

Where possible, IT personnel shall enforce password policy by technical means at the system level. Where technical enforcement capabilities do not exist, it is the responsibility of each system user to select and manage their passwords in compliance with this policy.

3.3 Automatic Console Lock Policy

The following policy and guidelines describe the standard automatic console lock configuration to be implemented on City computers. This policy is designed to improve the security of the City's computer systems while minimizing the impact on employee productivity. It is based on generally accepted industry standards as well as the Police Department's requirement for compliance with Federal Bureau of Investigation (FBI) Criminal Justice Information System (CJIS) policy.

3.3.1 Automatic Console Lock Policy

City computers shall be configured to automatically engage a console lock after a period of 30 minutes of user inactivity. Once the console lock is engaged all access to data, applications and other online resources shall be blocked until the user's password is entered to disengage the console lock.

3.3.2 Policy Exceptions

The following computers are exempted from the automatic console lock policy:

- Computers performing a monitoring or control function requiring information to be constantly displayed and/or the ability to input data or commands to be available at all times. Physical access to these computers shall be restricted to prevent unauthorized personnel from accessing sensitive data or critical control functions.
- Computers performing a public kiosk function allowing unauthenticated access to non-sensitive information by the media or citizens. The kiosk user account shall be restricted from access to sensitive information, which is not appropriate for public release.
- Computers located in the Police Department 911 Center. These machines are in a secure, restricted access area, which is staffed 24 x 7 x 365. Any benefit gained by the implementation of an automatic console lock policy is negated by the impact of the delayed ability to dispatch, support, and document the activities of police and fire assets.
- Mobile Data Computers (MDC) used by the Police and Fire Departments. The requirement for immediate access to data and applications needed by Police and Fire personnel supersedes the requirement for the additional security provided by enabling an automatic screen lock. To mitigate the additional risk of exempting these machines from the automatic console-lock policy MDC users shall be responsible for taking all reasonable precautions to safeguard these machines against access by unauthorized persons.

3.3.3 Console Lock Guidelines

Leaving a logged-in computer unattended increases the risk of unauthorized access. An automatic console lock policy mitigates this risk to a degree, but still leaves a period of up to 30 minutes in which an unattended machine can be easily compromised. To further reduce this window of vulnerability, City computers should be secured by taking one of the following actions prior to relinquishing direct observational or physical control of the machine.

- Shut down the computer.
- Log out of the computer.
- Manually engage the console lock.

The console lock may be manually engaged by pressing and holding the Windows key (located near the lower left corner of the keyboard, see figure 3.1 below) and then pressing the "L" key.

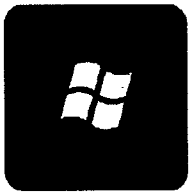


Figure 3.1 – Windows Key

3.3.4 Screen Lock Policy Enforcement

Where possible, IT personnel shall enforce the automatic console lock policy by technical means at the system level. Where technical enforcement capabilities do not exist or whenever a computer is going to be left unattended it is the responsibility of the user to secure the system as described in paragraph 3.3.3.

3.4 User Account Management

3.4.1 Separation From City Employment

Immediate action with respect to logon accounts to information systems shall be taken when an employee separates from City employment. The specific actions and timing are dependent upon the circumstances surrounding the separation. For the purposes of the User Account Management section of this document, the term "employee" will be used to refer to any official, employee, contractor, volunteer, intern or other person who has been given credentials to access any City IT system.

3.4.1.1Involuntary Separations

In the event of an involuntary separation, IT shall be directed by the employee's management or by Human Resources to disable all access to City IT systems prior to the employee being informed of the action in order to minimize any opportunity for the employee to take malicious retaliatory actions involving the IT systems.

3.4.1.2 Voluntary Separations

Human Resources shall provide advance notice to the IT Division of all retirements, resignations or other planned employee separations for which there are no reasonable grounds to assume any hostile intent towards the City on the part of the employee. The advance notice shall include a date and time at which the employee's access to City IT resources shall be disabled.

3.4.1.3 Hostile Intent

If management has reasonable grounds to believe that any employee bears malicious intent towards the City that might be manifested by an attempt to use their IT system access to inappropriately access, modify, disclose or otherwise damage the City data or computer systems the IT Division shall be directed to immediately disable that individual's access to City IT systems. The employee's access may be restored at the further direction of management if it is determined that there are no longer any grounds to suspect hostile intent towards the City on the part of the employee.

3.4.1.4 Preservation of Data

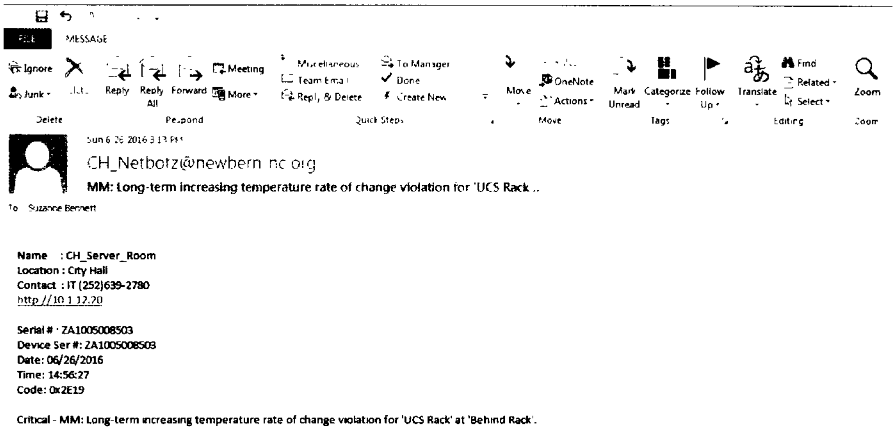
In all cases in which the IT Division is directed to disable an employee's account action shall be taken to preserve and protect all data contained within the account pending further direction on the disposition of the data from management.

4. Computer Room Temperature Management

Maintaining temperatures within design limits is crucial to the proper operation of computer equipment. Allowing temperatures to rise above these limits will cause malfunctions and if left unchecked will result in loss of data and physical damage to the systems. The policies and procedures documented in this section apply to both the City Hall and Police Department computer rooms.

4.4 Automatic Notification Emails

The City's computer rooms are equipped with a temperature monitoring system that will automatically generate an email if the temperature rises above the maximum safe operating level. The email will be sent to a distribution group maintained by IT, which includes personnel from IT and Control. Figure 4.1 illustrates the format of the email.



Sun 6/26/2016 3:13 PM
CH_Netbotz@newbern.nc.org
MM: Long-term increasing temperature rate of change violation for 'UCS Rack ..
To Suzanne Bennett

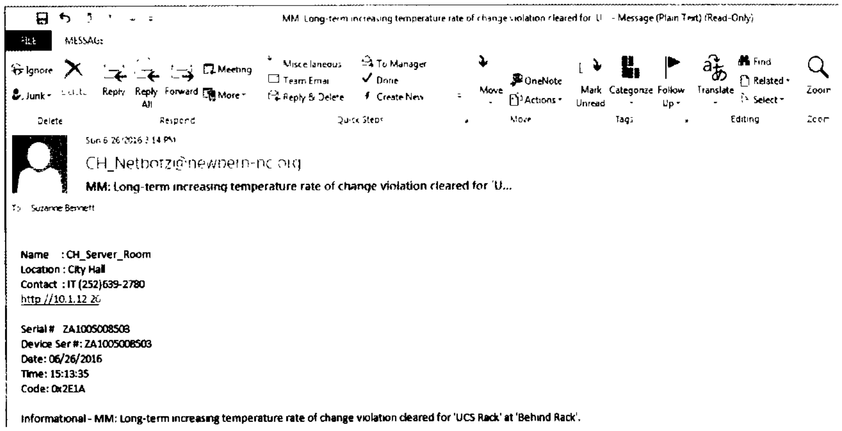
Name : CH_Server_Room
Location : City Hall
Contact : IT (252)639-2780
http://10.1.12.20

Serial # : ZA1005008503
Device Ser #: ZA1005008503
Date: 06/26/2016
Time: 14:56:27
Code: 0x2E19

Critical - MM: Long-term increasing temperature rate of change violation for 'UCS Rack' at 'Behind Rack'.

Figure 4.1 – Unsafe Computer Room Temperature Notification Email

The system will also generate a notification email once the temperature drops back to a safe operating level. Figure 4.2 illustrates the format of this email.



Sun 6/26/2016 3:14 PM

CH_Netbotz@newbern-nc.org

MM: Long-term increasing temperature rate of change violation cleared for 'U...

To Suzanne Bennett

Name : CH_Server_Room
Location : City Hall
Contact : IT (252)639-2780
http //10.1.12 26

Serial # ZA1005008503
Device Ser #: ZA1005008503
Date: 06/26/2016
Time: 15:13:35
Code: 0x2E1A

Informational - MM: Long-term increasing temperature rate of change violation cleared for 'UCS Rack' at 'Behind Rack'.

Figure 4.2 – Safe Computer room Temperature Notification Email

4.5 Required Actions – Control

4.5.1 Coverage Times

Control will provide monitoring and response support during the following days and times. Over-temperature notification emails may be ignored by Control at all other times.

- Regular Business Days: (Monday – Friday) 1700 through 0800
- Weekends: 1700 on Friday through 0800 on Monday
- Holidays: 1700 on the last regular business day prior to the holiday through 0800 on the first regular business day after the holiday
- During other times as agreed upon between the IT Manager and the Director of the Electric Utility due to special circumstances

4.5.2 Response to Over Temperature Notification Emails

Due to normal cycling of the HVAC system and other factors, it is not unusual for the temperature in the computer room to briefly spike above the maximum safe operating level. In order to ensure that intervention is actually required, Control personnel shall take no action unless more than 10 email alerts are received in a 30-minute period. If this alert threshold is met, Control shall take the following actions:

- Contact the on-call IT technician at extension 2780. If the on-call technician does not answer, leave a voicemail stating that a computer room over temperature alert email has been received and then call the IT Manager at 252-670-3889.
- Once the alert has been confirmed to have been received by IT (i.e. by directly speaking to a member of the IT Division), Control may disregard any further over temperature alert emails.
- When notified by IT that the HVAC system is working properly and computer room temperatures have stabilized resume monitoring for over temperature alert emails.

4.6 Required Actions – IT

4.6.1 Coverage Times

IT has primary responsibility for monitoring computer room temperatures at all times other than those specified in paragraph 4.2.1 of this document.

4.6.2 Response to an Over-Temperature Condition

If notified of an over-temperature condition either by a call from Control or through direct monitoring, the following actions shall be taken:

- Immediately notify the Building and Grounds Maintenance Superintendent at 252-639-7504 or 252-665-0021.
- If after hours, call in additional IT personnel as required.
- Take all necessary actions to protect the equipment in the computer room from damage.
    - Utilize portable air conditioning units, fans, open doors and windows, etc.
    - Selectively shut down systems in reverse order of priority to City operations to reduce the heat load in the computer room.
        - This action should be taken only if necessary to prevent equipment damage
        - Contact the IT Manager, Acting IT Manager, or Senior IT Analyst if possible prior to initiating system shutdowns.
- Disable the generation of over temperature alert emails.
- Once the HVAC problems have been corrected and computer room temperatures have returned to normal take the following actions:
    - Re-enable the generation of over temperature alert emails.
    - Notify Control to resume their regular alert email monitoring schedule.

5. Contact Information

Direct questions regarding this policy to the Information Technology Manager at 252-639-2782 or gatlint@newbern-nc.org.