POLICY AND PROCEDURE MEMO

NO. 5.006
DATE:
10/15/2015 App

SUBJECT:
PASSWORD POLICY
COMPUTER SOFTWARE APPLICATIONS and
CITY OWNED ELECTRONIC DEVICES

CITY MANAGER

I. STATEMENT:

This policy is intended to provide guidelines pertaining to the use of City owned accounts used to access software applications as well as the use of City owned electronic devices such as, but not limited to, cell phones, smart phones, computers, tablets or other electronic devices provided by the City and used by employees in the performance of their duties in the employ of the City.

There are two main objectives of this policy: (1) to protect the security of sensitive data and information and (2) to clearly inform employees of the limits upon the expectation of privacy.

With regard to protecting the security of sensitive data and information, the proliferation of electronic data creates a number of risks – access to sensitive and confidential data by unauthorized persons (loss of which may never be known or not known until it is misused), non-compliance with regulatory requirements pertaining to health, financial or other sectors subject to specific privacy and security regulations (for example the Health Insurance Portability and Accountability Act or HIPAA), general liability to citizens and taxpayers as well as public relations harm, and risk of failing to properly comply with obligations to maintain information subject to legal discovery.

With regard to an expectation of privacy, the City seeks to take a measured approach in recognition of the blending of work and personal lives with the ubiquitous use of electronic communications such as text messaging and social media. However, at the same time employees must recognize the City has the responsibility and authority to monitor the use of City owned systems and devices.

II. DEFINITIONS

A. Computer Software Applications – These include, but are not limited to, financial data systems such MUNIS, email systems such MS Exchange, technical systems such as Patriot Properties and ViewPermit.

B. Electronic Devices – These include cellular telephones, smartphones and other devices that in addition to making telephone calls, adds features that you might find on a personal digital assistant or a computer (such as the ability to send and receive text messages, e-mail and edit documents. Electronic devices usually have a computerized Operating System.

1

POLICY AND PROCEDURE MEMO

NO. 5.006

DATE:

10/15/2015 App

SUBJECT: **PASSWORD POLICY**
COMPUTER SOFTWARE APPLICATIONS and
CITY OWNED ELECTRONIC DEVICES

CITY MANAGER

C. Credentials – As used herein, pertains to the username and password that grants access and specific levels of authority to electronic systems and data.

III. PROCEDURE

A. Computer software applications purchased by the City that contain sensitive and often confidential data is provided to designated employees to carry out their job related functions.

B. An electronic device that is the property of the City of Rochester is entrusted in the appropriate care of a designated employee for the performance of their duties.

C. Employees are required to set up and maintain credentials (usernames and passwords) at all times to prevent unauthorized access to City owned computer applications and electronic devices. Employees are expected to take reasonable steps to safeguard against access to these credentials by unauthorized persons.

D. The use of software applications and electronic devices is intended for City business use and not for conducting personal business. As such, employees shall have no expectation of privacy in any communications originating on, or received by, a City owned electronic device or through City owned and maintained software applications. To this end, any supervisor may search any city owned device or software applications to determine compliance with this policy or to gather information relative to other suspected incidents of employee misconduct.

E.

User name and password requirements may vary for different systems. For most City of Rochester systems there will be in force a required password change every 180 days and meeting the following complexity standards:
1 - Not contain the user's account name or parts of the user's full name that exceed two consecutive characters
2 - Be at least six characters in length
3 - Contain characters from three of the following four categories:
English uppercase characters (A through Z)
English lowercase characters (a through z)
Base 10 digits (0 through 9)
Non-alphabetic characters (for example, !, $, #, %)

F. Electronic devices must be returned to the City Business Office or appropriate supervisor when the device is no longer necessary for the performance of their City duties or upon separation from employment.

2

POLICY AND PROCEDURE MEMO

NO.   5.006
DATE:

10/15/2015 App

SUBJECT:

PASSWORD POLICY
COMPUTER SOFTWARE APPLICATIONS and
CITY OWNED ELECTRONIC DEVICES

CITY MANAGER

G. Loss of an electronic device must be reported to the Business Office and the employee's supervisor immediately. The proper safeguarding of access to accounts will be handled through the Business Office. A temporary device if available may be issued until a permanent replacement is secured. Loss due to negligence may result in disciplinary actions.

H. The City will not use any credentials to access an employee's personal email, social media accounts or any other personal information. The City will adhere to the provisions of RSA 275:74 as well as the federal Electronic Communications Privacy Act of 1986.

I. All City owned mobile devices will have Mobile Device Management (MDM) software installed by MIS. This includes but is not limited to smart-phones, tablets and laptops used outside of the City network. Security for mobile devices will be enforced by MDM. The installation of MDM on all devices will be phased in with a completion date of July 1, 2016.

IV.   EXCEPTIONS

A. The City Manager may agree, in writing, to exceptions to this policy depending on specific circumstances.

- END OF PROCEDURE -