Password & Workstation Security Policy

Policy No. D-05[1]

The Scope of this policy includes the following individuals:[2]

- ✓ Employees (including Appointed Officials, Probationary Employees, Full-Time At-Will Employees, Part-Time Employees, Temporary Employees, Civil Service Employees, Teamsters Employees, HPOA, HPSA, and IAFF Employees)
- ✓ Full-Time Elected Officials
- ✓ Volunteers

I. PURPOSE

To protect and provide for the security of the City's computer systems.

II. POLICY APPLICATION

A. Password Security

All passwords must be treated as sensitive, confidential City data. Employees may not share City passwords with anyone, including administrative assistants or employees of the Department of Information Technology (DoIT). Employees may not use the "Remember Password" feature of any application except a DoIT-approved password manager. Employees may not re-use the same password for City accounts that are used for other non-City access (i.e., personal accounts, option trading, and benefits).

If an account or password is suspected to have been compromised, employees must report the incident to the Help Desk and change their password in all systems.

[1] This policy is not to be construed as a contract or an implied contract concerning any employment-related decision or term or condition of employment. The City reserves the right to revise, delete or add to any and all policies, procedures, work rules or benefits stated in this policy at its sole discretion. See Introduction, Administrative Policy No. A-01.

[2] The relevant definitions for the individuals identified in the Scope of this policy are defined in Introduction, Administrative Policy No. A-01.

Employees are required to enter passwords in order to access the City's computer equipment and databases. All user-level passwords (i.e., email, web, and desktop computers) must be changed at least every ninety (90) days. For those applications that do not utilize the network's primary password management tool, a password change is recommended every ninety (90) days.

The City enforces policies and standards relating to the storage of account information and password details. The exclusive repositories authorized for storing information related to City-specific accounts are the City-approved password vault and the privileged access management system.

Server administrative account information, domain administrative account information, and service account information must only be kept in the privileged access management system.

Storing City account credentials within non-City provided password vaults, personal browsers, or any third-party password vaults is prohibited (i.e – Passwords stored in scripts/encoded in script). The City disables the password saving feature within the City-provided Google Chrome and Microsoft Edge browsers.

The storage of personal account information within the City-approved password manager is prohibited.

All passwords must be at least twelve (12) alphanumeric characters long and the last ten (10) passwords shall not be reused. Additionally, all passwords must contain at least two (2) of the following criteria:

1. Both upper and lower case characters (i.e., a-z, A-Z);
2. Digits (0-9); and
3. Punctuation characters (i.e., !@#$%^&*()_+|~-).

To make a password more secure, it is required that employees use a password that is ***not***:

1. A word found in a dictionary (English or foreign)
2. A common usage word such as the names of immediate family members or pets
3. The words "City of Henderson, Henderson, COH," or any similar common usage words

4. Sport Team Names such as GoldenKnights, SilverKnights, Raiders

5. Job titles such as Engineer, Firefighter, Police Officer

6. Department names such as Information Technology, Fire

7. Seasons such as Spring, Summer, Fall, Winter

8. Birthdays and other personal information such as addresses and telephone numbers

9. Word or number patterns such as aaabbb, qwerty, zyxwvuts, and 123321

10. Any of the above examples spelled backwards

11. Any of the above examples preceded or followed by a digit (i.e., secret1, 1secret) and/or special character.

The DoIT will perform random security assessments to determine adherence to this policy. Notification of these scans may or may not be given. If a password is guessed or cracked during one of these assessments, the user will be notified and required to change their password. The City may override any applicable passwords or codes to perform any authorized inspections, investigations, or searches of an employee's files and messages.

B. Workstation Security

Workstations are an important part of overall cybersecurity. Workstation security involves protecting the City's workstations from tampering, which could result in intentional or accidental damage. Workstations used for sensitive or critical tasks must have adequate physical and electronic controls to provide continued confidentiality, integrity, and availability of data stored on the system.

All City data must be maintained on DoIT-managed systems and storage so that the data can be backed up and recovered if needed. Approved locations include the desktop on City owned workstations, My Documents folders, and Mapped drives, and City SharePoint and OneDrive Libraries. If an employee is using a City-owned laptop, the employee must transfer or copy new and updated City data from the local drives on the laptop to DoIT-managed systems and storage at the earliest opportunity in order to insure that the data is not lost or destroyed.

Employees must use the "Lock Workstation" function any time they leave their immediate work area. After fifteen (15) minutes of inactivity, the workstation screen saver will automatically be activated and lock the workstation or automatically log off. Public Safety laptops docked in a vehicle mount are exempt from the workstation screen saver lock. Any monitor in public view used to view confidential data[3] must have a privacy filter installed.

C. Removable Electronic Media

Removable electronic media includes USB storage devices (e.g., flash drives, portable hard drives, smartphones, mp3 players, etc.) and any other form of writeable media including but not limited to CDs, DVDs, and SD cards. Removable electronic media presents a risk to the security of sensitive data as it can be easily lost, stolen, or transported without adequate security protections.

Confidential City data may only be transferred to DoIT-approved, encrypted removable electronic media, and only for pre-approved business purposes. Removable electronic media containing confidential City data must always be physically secured. If the responsible employee is not in the immediate work area, the removable electronic media must be removed from the computer and kept on their person or in a locked drawer, cabinet, or other secure repository. If confidential City data is found on unencrypted media, it must be delivered to the DoIT Help Desk for appropriate sanitization or disposal.

III. APPROVAL

APPROVED BY:
Jim McIntosh, Asst City Manager/CFO on behalf of
Richard Derrick, City Manager/CEO

REVIEWED BY:
Nicholas Vaskov, City Attorney
Brooke Stream, Director of Human Resources

Record of approved document can be obtained through the Human Resources Department.

ORIGINAL EFFECTIVE DATE: 2/16/2016
REVISION DATE(S): 8/28/2023

[3] Confidential data may include, but is not limited to, documents/information containing personal information; records of recreational facility/activity registration where the name, address, telephone number of the applicant are collected; employee medical records; employee personnel records; attorney/client privileged information; and information that is subject to the deliberative process privilege. If an employee is unsure as to whether a document/information is confidential, it is the employee's responsibility to inquire with their supervisor and/or department director to confirm the nature of the document/information.