STOREY COUNTY ADMINISTRATIVE POLICIES AND PROCEDURES

NUMBER 031
EFFECTIVE DATE: 01/13/2020
REVISED:
AUTHORITY: BOC
COUNTY MANAGER: AO

SUBJECT: PASSWORD PROTECTION POLICY

I. PURPOSE/POLICY:

The purpose of this policy is to establish a standard for creation of strong passwords and the protection of those passwords.

This policy contains the procedures and requirements needed for the safeguarding of county system access. Passwords are an important aspect of computer security. A poorly chosen password may result in unauthorized access and/or exploitation of county resources. All employees are responsible for safeguarding Storey County system access login information and password credentials and must comply with the password parameters and standards as further defined in this policy. Passwords must not be shared with or made accessible to anyone in any manner that is not consistent with this policy and procedure.

Assigning unique user logins and requiring password protection is one of the primary safeguards employed to restrict access to the Storey County network and the data stored to authorized users only. If a password is compromised, access to information systems can be obtained by an unauthorized individual, either inadvertently or maliciously. Individuals with Storey County network access are responsible for safeguarding against unauthorized access to their account, and as such, must conform to this policy in order to ensure passwords are kept confidential and are designed to be complex and difficult to breach.

II. SCOPE:

The scope of this policy includes all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any Storey County facility, has access to the county-maintained network, or stores any nonpublic County information.

Individuals are responsible for keeping passwords secure and confidential. As such, the following must be adhered to for creating and safeguarding passwords:

III. PROCEDURES:

User passwords must be changed immediately upon issuance for the first-use. Initial passwords will be securely transmitted to the individual, either via the Department Head or Human Resources/Administrative Officer.

A. Password Creation:

1. All user-level and system-level passwords must conform to the Password Construction Guidelines:
    - Minimum of 8 characters
    - Must have at least one uppercase or lowercase letter or number
    - Must have at least one special character
    - Not consist of any portion of first or last name
    - Must not include any portion of UserID (or Login Alias)
2. Employees must use a separate, unique password for each of their work-related accounts. Employees should not use the same passwords for work as they do for personal use.
3. Accounts that have system-level privileges granted through group memberships or Active Directory settings must have a unique password from all other accounts held by the employee to access system-level privileges. It is highly recommended that some form of multi-factor authentication is used for any account.

B. Password Change:

1. The Storey County IT Department is authorized to reset passwords only. There is no password recovery for existing passwords.
2. User passwords must meet the complexity requirements outlined in this policy.
3. User passwords must be changed on an annual basis or sooner upon suspicion of a breach or compromise. In the event a breach or compromise is suspected, the incident must be reported to the direct supervisor, Department Head, the IT Department or Administration.
4. The IT Department and Administrative Officer/HR Director or County Manager reserves the right to reset or request a reset of an employee's password.
5. In order to limit attempts at password cracking or compromising accounts, an account lockout policy is in effect for all systems. Account lockout thresholds are currently set to 3 attempts. Once locked the account will have to be re-enabled by the IT Department and the password will be required to change.

C. Password Protection:

1. Passwords are not to be shared with anyone, including supervisors and coworkers. All passwords are to be treated as sensitive and confidential information.
2. Passwords must not be inserted into email messages, text messages or other forms of electronic communication, nor revealed over the phone to anyone.
3. A shared or compromised user password is a reportable IT security incident.
4. Employees—including administrators, elected officials and supervisors, are unauthorized to use or obtain passwords of another employee. In the event an employee is requested to provide password information to an individual or sign into a system and provide access to someone else under his/her login, s/he is obligated to report this to the direct supervisor, Department Head, the IT Department or Administration as soon as possible.

5. User passwords must never be written down and left in a location easily accessible or visible to others.
6. Do not use the "Remember Password" feature of applications (for example, web browsers).
7. Passwords must not be stored electronically in any web browser's password manager, a text file or office file.
8. Passwords may be stored electronically through the use of a secure and encrypted password manager, installed locally on the user's desktop, subject to approval and installation of the application by the IT Department. Cloud-based password managers may not be accepted if they do not meet IT security policy requirements.
9. Multi-factor authentication is highly encouraged and should be used whenever possible.

D. Compliance

Storey County Information Technology will verify compliance to this policy through various methods, including but not limited to, periodic walk-throughs, internal and external audits, and feedback to the policy owner.

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

IV. EXCEPTIONS

Any exception to the policy must be approved by the Information Technology Director and HR Director/Administrative Officer or County Manager in advance.

Nothing in this policy shall be construed to limit or effect the rights and responsibilities of the County Manager, IT Director or Administrative Officer/HR Director in the access and protection of county resources.

V. RESPONSIBILITY FOR REVIEW:

The IT Director and Administrative Officer/ HR Director will review this policy every 5 years or sooner as necessary.