TETON COUNTY ADMINISTRATIVE POLICIES

Password Management

See also "Computers, Technology & Information Security Policy"

Revision:	
Date:	11/23/15
Original Issue Date:	11/23/15
Number of Pages:	2
Approved:	BOCC

Employee passwords are the first line of defense in securing the county from inappropriate or malicious access to data and services. Compromised user accounts can become "stepping stones" for administrator-level penetration by unauthorized individuals, resulting in catastrophic data breaches. This policy provides guidelines for consistent and secure password management and includes mandates on how passwords should be generated, used, stored and changed, as well as instructions for handling password compromises. Every county employee, contract worker, consultant, and elected official must adhere to this policy.

General Requirements. The following guidelines should always be followed when creating, managing and storing passwords:

1. Blank or easily-guessed passwords such as "password" or "12345" are prohibited.
2. Passwords should not contain dictionary words such as "kitchen" or "automotive."
3. Passwords must be complex, containing at least 8 characters and a mixture of lower case, upper case, numbers and punctuation characters. For example, "B3llt0Wer!" should be used in place of "Belltower" as it is considerably more secure.
4. Passwords should never contain security-sensitive information such as social security numbers or date of birth. Passwords should also not include public information related to an employee's personal life, such as the names of their children, hobbies, favorite sports team, etc.
5. Use different passwords on different systems. A Windows account password should not be the same as a Quickbooks password. It is especially critical that passwords used to log on to "external accounts" (such as third-party websites like Facebook) are not the same passwords used to log on to "internal accounts" (such your County computer or email). Using different passwords protects internal accounts from data breaches that may occur on external accounts.
6. Passwords should not be sent through email, texting or instant messaging services.
7. Ideally, passwords should not be written down. However, if a password is written down, the password must be kept in a secure location not visible to others. Never put user names and passwords on notes stuck to monitors or other visible locations
8. The IT department will never ask you for passwords, but will, instead, set temporary passwords for employees who cannot log into their accounts.
9. When configuring security questions designed to protect against lost passwords, always choose fact-based questions such as, "What street did you grow up on?" rather than opinion-based questions such as, "What is your favorite food?" (Opinion-based questions are more difficult to remember since opinions change over time.) Never pick security questions with answers that could be easily researched such as, "Where did you go to high school?"

Device Management Strategies. Any device on which County information is stored must be secured with a password. Always lock screens/devices when away or not in use. Pressing "Windows-L" will immediately lock a Windows screen with the logged-on user's password. Screen savers that auto log users out after a certain time are another good option. Employees should avoid using public systems or un-trusted devices to access County resources since these may have been configured to steal passwords or log keystrokes.

Passwords must not be stored on insecure devices (hereby defined as smartphones/tablets/computers) which do not have password protection and do not utilize encrypted storage. Biometrics may be used for authentication to County systems but must not replace the use of passwords. Keep in mind that the best security model is "two-factor authentication," something you have (a door card) and something you know (a password).

Password Changes. All employee account passwords must change at least annually following the guidelines listed below:

1. No reuse of expired passwords is permitted. Passwords must be unique at every change.
2. It is recommended that employees with multiple accounts change all passwords at the same time, especially if the expiration dates are similar.
3. Notify the IT Department immediately of any passwords thought to be compromised. For example, if someone else views passwords being typed on a keyboard or accidentally displayed on a screen.
4. When employees leave employment with the County, even under voluntary circumstances, any passwords that they had access to must be changed.

Password Usage/Management Guidelines for the IT Department. The County's IT department and contracted technicians should adhere to the following guidelines:

1. Authentication systems such as Active Directory should be configured to warn users of expiring passwords within at least 7 days.
2. Document all system account passwords in an encrypted system. The master password must be shared only with appropriate individuals and must be memorized, not documented.
3. System/service account passwords should be changed at least annually.
4. Because expired system accounts can cause numerous technical problems, always use alerts to notify personnel of impending system account password expirations (within 7 days). Plan out password change steps (updating scheduled tasks, restarting services for the change to take effect, etc.) to ensure a seamless transition.
5. Don't embed passwords in scripts, programs or any file which could be read by unauthorized users.
6. When possible, set accounts to lock for 15 minutes after five failed login attempts. This will reduce the possibility of guessing account passwords using "brute force" strategies.
7. Never ask a user for their password. If users cannot log into their account assign them a temporary password and configure the account to require a password change upon the next logon.
8. Do not reset passwords upon request until you have confirmed the identity of the user(s) involved. Provide the password in person or over the phone.
9. Don't use a generic password such as "password".
10. If a user reports that their password has been compromised, lock their account immediately, then set a new password.
11. All administrative passwords should be changed if there is an actual or suspected security breach.
12. The IT department should maintain a "termination checklist" to document the steps involved with disabling accounts/changing passwords for ex-employees. The HR department must immediately notify the IT department whenever an employee termination or resignation occurs in order that the IT department may disable accounts for those employees.

Monitoring. Adherence to many of these password requirements, such as those requiring periodic password changes or enforcing password complexity, will be mandated by system controls. Monitoring of password usage to ensure compliance with these guidelines will be conducted by the IT department with assistance from each agency or department head.

Violations and Penalties. Any violation of the Password Management Policy must be immediately reported to the employee's supervisor and the IT department. Such violations could result in disciplinary action leading up to, and including, termination of employment and legal action where applicable.