Wyoming Department of Health

Commit to your health.
visit www.health.wyo.gov

Thomas O. Forslund, Director

Governor Matthew H. Mead

Policy Title:	Password Use and Management
Policy Number:	S-005d
Effective Date:	July 1, 2013
Approval:	Thomas O Forslund 4/18/13 Thomas O. Forslund, Director Date

Purpose:

This policy establishes standards for creating, changing, and safeguarding passwords that are used to access Wyoming Department of Health (WDH) systems.

Scope:

This policy applies to all WDH workforce.

Definitions:

Authentication means the corroboration that a person is the one claimed.

Password means confidential authentication information composed of a string of characters.

User means a person or entity with authorized access.

Policy:

1. All passwords shall meet the "strong password" criteria listed below.
   - a. Strong passwords are:
     - i. At least nine (9) characters in length.
     - ii. Comprised of at least one character from each of the following four sets:
       - A. Upper case letters;
       - B. Lower case letters;
       - C. Numbers; and
       - D. Punctuation and other special characters (e.g., &, $).
   - b. Strong passwords are not:
     - i. Common dictionary terms.
     - ii. Personal information (e.g., names of pets or family members).
     - iii. Workplace names, titles, or terminology.
     - iv. Items visible in the immediate work area.
2. All passwords shall be changed at regular intervals based upon system risk and safeguards specified within this policy. Passwords shall be changed as soon as reasonably practicable if an account is suspected to have been compromised.
3. Each high-risk account shall have a password unique from all other accounts held by that user.
4. Passwords shall be safeguarded accordingly.

   a. All passwords shall be regarded as sensitive and confidential.
   b. Generally, passwords should not be revealed to anyone. However, if a user reveals a password to resolve an operating issue, such password shall be changed upon resolution of the issue.
   c. Any written record of passwords shall be retained in a secure environment (e.g., on the user's person or in a locked file cabinet).
   d. Any suspected compromise of a user's accounts or passwords shall be reported to the user's immediate supervisor and the WDH Compliance Office.

5. Users shall not share accounts or passwords.
6. Users shall not utilize "remember my password" features.
7. Password strength shall be evaluated on a periodic basis. WDH shall request that the user change any passwords that are assessed as "weak to moderate."

Contacts:

De Anna Greene, CIPP/G, CIPP/IT, WDH Privacy/Compliance Officer, (307) 777-8664
Tate Nuckols, JD, WDH Security Officer, (307) 777-2438

Reference:

45 CFR § 164.304
45 CFR § 164.308(a)(5)(ii)(D)
45 CFR § 164.530(c)
0400-P170, User Access Management; Department of Enterprise Technology Services, Policies and Standards
NIST SP-800-12
NIST SP-800-14

Training: