Password Protection
HIPAA Policy: Security 08

Summary: Provides rules for password management in HIPAA covered entities

Affected Individuals: Employees in HIPAA covered entities; IT staff

Purpose of Policy

The purpose of this policy is to protect University of Mississippi (UM) information assets by managing and enforcing password requirements.

Definitions

For a complete list of definitions, refer to the *Glossary*.

Scope

This policy applies only to covered entities as defined in the University of Mississippi (UM) HIPAA hybrid policy.

This policy applies to all workforce members, users, and all personnel affiliated with third parties who use the UM's information assets and related resources.
This policy applies to centrally-administered and managed information asset technologies, personally-owned computing devices connected by wire or wireless to UM's network, and to off-site computing devices that connect remotely to UM's network.
This policy applies to system administrators and developers who manage or design systems that require passwords for authentication.

Policy

A. Password Requirements

1. Passwords selected for accounts on systems, databases and applications align with the following, where technically feasible:

    a. Passwords require at least eight (8) characters which are:

        - Not easy to remember;
        - Not based on anything easily guessable or obtained using personal related information (e.g. Names, telephone numbers, and dates of birth etc.);

- Not vulnerable to dictionary attack (do not consist of words included in dictionaries);
- Free of consecutive identical characters; and
- A combination of alphabetic, upper and lower case characters, numbers, and special characters (combination of any three (3) of the above four (4) listed is acceptable).

b. Passwords are prohibited from being reused for at least six (6) generations

B. Password Creation

1. All user-level and system-level passwords conform to the *Password Requirements.*

2. New account and temporary passwords are created in accordance with the password complexity requirements outlined in this policy.

3. Users do not use the same password for UM accounts as for other non-UM access (e.g., personal ISP account, option trading, benefits, etc.).

4. Where possible, users do not use the same password for various UM access needs (e.g., email, laptop encryption, windows, etc.).

5. When users are required to maintain their own passwords they are initially provided with a secure temporary password, which they must immediately change.

6. Temporary passwords are not created using a predictable pattern or convention.

7. Temporary passwords are changed at the first log-on.

8. Temporary passwords are given to users in a secure manner, which includes communication in person or over the phone, after user identity has been validated.

C. Password Change

1. Default vendor passwords are changed following installation of systems or software in accordance with Password Requirements.
2. All system-level passwords (e.g., root, enable, administrator, application administration accounts, etc...) are changed at least every 60 days.
3. All user-level passwords (e.g., email, web, desktop computer, and so on) must be changed at least every 90 days or based on the number of accesses.
4. Password cracking or guessing may be performed on a periodic or random basis by the CISO (or delegates). If a password is guessed or cracked during one of these scans, the user is required to change it to be in compliance with the *Password Requirements*.
5. In the instance that a user forgot their password, the user may change their password by going through the appropriate reset process within the reset system in place.
6. User identities are verified prior to performing password resets.

D. Password Protection

1. Users are responsible for keeping account passwords secure and confidential. A password is private information and users do not reveal their account passwords to any other person.
2. Users are prohibited from sharing internal UM passwords with other UM employees, clients, or third-parties.
3. Systems and applications encrypt passwords in storage and during transmission. The use of third parties or unprotected (clear text) electronic mail messages is prohibited.
4. Passwords are never written down or stored on paper.
5. Systems and applications prohibit passwords from being displayed when entered.

6. Users change passwords whenever there is any indication of possible system or password compromise.
7. Any user suspecting that his/her password may have been compromised reports the incident and changes all passwords.
8. Users do not use the "Remember Password" feature of applications (e.g., web browsers).
9. Approved, secure password repositories (where passwords remain encrypted) are permitted for business use.

E. Application Development

1. Applications do not store passwords in clear text or in any easily reversible form.
2. Applications do not transmit passwords in clear text over the network.
3. Applications provide role management, such that one user cannot take over the functions of another without having to know the other's password.

Policy Compliance

Enforcement

The Chief Information Security Officer (CISO), or designee, has general responsibility for the implementation and enforcement of this policy.

Future Revisions

UM reserves the right to add, delete, or revise any provision of this Policy (approval by committee) at any time without prior notice to users.

Sanctions

Any user violating these policies or applicable local, state, or federal laws while using UM's computing environment is subject to loss of network privileges and any other disciplinary actions deemed

appropriate, up to and including termination and criminal and/or civil prosecution in accordance with policy.

Exceptions

Exceptions to this policy must follow the approved exception process as outlined in the *Information Security Waiver Policy*. All approved policy exceptions will be reviewed periodically for appropriateness by the CISO and may be revoked at any time with or without notice.

Regulatory and Standards References

The following regulations and standards are applicable to this policy:

- **HIPAA Regulatory Reference**: HIPAA § 164.308(a)(5)(ii)(D)
- **HITRUST References**: 01.d User Password Management, 01.r Password Management System
- **PCI References**: PCI DSS v3 2.1, PCI DSS v3 8.2.2, PCI DSS v3 8.2.3, PCI DSS v3 8.2.5, PCI DSS v3 8.2.6

Related Documents:

- Glossary

Approval

Chief Information Security Officer

<date>