State of Iowa Enterprise Authentication
Security Standard
May 28, 2013

Purpose
This Standard establishes the minimum requirements for authentication to state IT systems and applications.

Overview
The State of Iowa maintains a variety of data in its IT systems, including confidential information, personally identifiable information, and other protected information. In order to protect data and systems it is necessary to authenticate accounts prior to granting them access to the systems and applications.

Scope
This standard applies to all agencies as defined by Iowa Code Chapter 8A, Section 101. Non-participating agencies are encouraged to follow the guidelines in this and other enterprise standards.

This standard applies to user accounts, administrator accounts and system accounts where applicable.

Definitions
Selected terms used in the Enterprise Authentication Security Standard are defined below:

- **Administrator Account**: An account with full\elevated privileges on a computer\device or application.
- **Authentication**: The process of establishing confidence in the identity of users of information systems.
- **Digital Certificate**: A software token containing the user's private key.
- **Multi-factor Authentication**: Authentication using two, or more, methods (something the user knows, something the user has, or something the user is) to verify the user.
- **Remote**: An information exchange between network-connected devices where the information cannot be reliably protected end-to-end by a single organization's security controls. Any exchange across the internet is considered remote.
- **System Account**: An account that allows the direct connection of two or more IT systems for the purpose of sharing data and other information resources.
- **User Account**: An account with limited privileges to a computer\device or application.

Elements
The following are the elements of the Enterprise Authentication Security Standard.

1. **Sharing:**
    a. User accounts shall be assigned to a single individual, not a group or entity. Exceptions require approval by the agency CIO and shall be documented by the agency.
    b. User passwords shall not be shared with co-workers, managers, help desk staff or others.

2. **Passwords:** The following requirements apply to passwords.
    a. Default administrative and initial user passwords shall be changed after initial use.
    b. Passwords shall be:
        i. At least eight characters for user passwords (except mobile device passwords see Enterprise Mobile Device Security Standard).
        ii. At least 10 characters for accounts with elevated privileges such as administrator accounts or system accounts.
        iii. A mixture of numbers, upper and lower case letters, with at least one special character.
        iv. Changed at least every 90 days.
    c. Social security numbers shall not be used as a user ID or password.
    d. Passwords shall not be displayed when entered.

3. **Multi-factor Authentication**: Multi-factor authentication shall be used for remote network connections (ex. VPN or remote desktop) and remote administrator tasks. Multi-factor authentication shall include a user ID and password\PIN plus one, or more, of the following:
    a. Digital certificate,
    b. Token\Smart card, or
    c. Biometrics.

4. **Encryption:** Passwords and password recovery information shall be encrypted in storage and transmission outside of the agency.

5. **Unsuccessful Login Attempts:** Accounts shall be set to lock after five consecutive unsuccessful password attempts. Accounts shall remain locked until the account is reset by an account administrator.

6. **Account Reset\Recovery:** Users and administrators shall be verified before passwords are reset\recovered.
    a. Account administrators shall NOT request the following as verification information:
        i. Social security number.
        ii. Mother's maiden name.
        iii. Employee ID number.

7. **Training:** State employees, interns, contractors shall receive security awareness training covering passwords, social engineering\phishing, malware threats and reporting incidents.

8. **Storage**:
    a. Written passwords, smart cards, and tokens shall not be stored with the computer\mobile device.
    b. Tokens\smart cards shall be secured when not in use.
    c. Hard copy emergency administrator passwords shall be stored in a secure area and restricted to authorized individuals.

9. **Cookies**: Cookies shall be set to expire.

10. **Disabling Accounts**: State employee, including intern and contractor, accounts shall be disabled when:
    a. The account credentials have been compromised.
    b. The user leaves employment or has been placed on administrative leave.
    c. The accounts are inactive for more than 90 days.

Accounts shall require agency director or designee approval before re-activation. Account passwords shall be changed before the account is re-activated.

11. **Inactivity Timeout**:
    a. User accounts shall timeout after 15 minutes of inactivity requiring the user to re-enter their password to access the account.
    b. Administrator accounts shall timeout after five minutes of inactivity requiring the user to re-enter their password to access the account.

Updates This document shall be reviewed at least every two years and updated as needed.

Effective Date This standard shall be effective May 28, 2013.

Enforcement This standard shall be enforced pursuant to Iowa Administrative Code 11—25.11(8A).

Variance Iowa Administrative Code 11 - 25.11(2) provides for variances from security standards. Requests for a variance from any of the requirements of this policy will be submitted in writing to the Chief Information Security Officer prior to implementation. http://das.ite.iowa.gov/standards/waiver.html