SEC-06-01-S
State CIO Adopted: September 12, 2024
TSB Approved: September 12, 2024
Sunset Review: September 12, 2027

WaTech
Washington Technology Solutions

Replaces:
IT Security Standard 141.10 (6.2, 6.3)
December 11, 2017

IDENTIFICATION AND AUTHENTICATION SECURITY STANDARD

See Also:
RCW 43.105.054 WaTech Governance
RCW 43.105.052 Powers and duties of agency—Application to higher education, legislature, and judiciary.
RCW 43.105.020 (22) "State agency"
RCW 43.105.450 Office of Cybersecurity
NIST 800-63B Digital Identity Guidelines – Authentication and Lifecycle Management.
NIST 800-63-3 Digital Identity Guidelines.
NIST 800-53 Security and Privacy Controls for Information Systems and Organizations.
NIST 800-63A Enrollment and Identity Proofing.
NIST 800-63C Federation and Assertions.

1. **Agencies will establish and implement administrative procedures for issuing, replacing, and revoking credentials. Agencies are required to safeguard credentials by:**

    a. Prohibiting the sharing of user authentication credentials, such as usernames, passwords, or any other form of identification, to access systems.

    b. Utilizing a secure password, passphrase or secrets management methodology for credentials not managed using agency directory services and documenting the method in the agency's security program, including but not limited to:

        i. Directory Services Root credentials.

        ii. API Keys.

        iii. Built-in account, root, and system passwords/passphrases.

        iv. Database root passwords.

        v. Password manager/password vault master passwords.

        vi. Encryption keys. See section 7 of SEC-08-02-S Encryption Standard.

2. **Agencies must manage identifiers for users, groups, roles, services, and devices by:**

    a. Requiring approval from designated agency staff to assign user, group, role, service, or device identifiers.

    b. Assigning a unique identifier to each user, group, role, service, or device.

    c. Preventing the reuse of identifiers for different users, groups, roles, services, and devices for a minimum of two years or longer as needed by agency compliance requirements. If a previously enrolled user, group, role, service, or device is re-enrolled, the same identifier should be reused to maintain continuity and avoid duplication.

3. **Agencies must manage the identity of users in the following manner:**

    a. Agencies must verify the identity of organizational IT system users before issuing credentials.

    b. Agencies must perform a risk assessment to determine the impact of a non-organizational user's fraudulent or compromised identity accessing data on internet-facing systems.

        i. Agencies must establish and implement the necessary actions based on the risk assessment.

        ii. Agencies must establish and implement processes to support objective measures for assessing the impact levels identified in the risk assessment.

4. **State IT systems must authenticate an identity prior to:**

    a. Permitting access to modify any data regardless of category.

    b. Providing access to category 2 data or higher. See SEC-08-01-S Data Classification Standard.

    c. Except, agencies may allow users to submit data without authentication regardless of category classification if there is a business need. Documented processes for evaluating associated risk and validating and categorizing the data upon submission are required.

5. **Agencies must manage information system authenticators by:**

a. Documenting the authentication methods for each system in the annual application inventory. See MGMT-01-01-S Application Inventory.

b. Requiring unique authenticators for all system access.

c. Requiring unique temporary authenticators and requiring them to be changed immediately after first use to establish initial access.

d. Changing the manufacturer's default authenticator before implementing an information system or component (e.g., routers, switches, firewalls, printers, etc.).

e. Only storing or transmitting encrypted representations of authenticators. See the SEC-08-02-S Encryption Standard.

    i. System administrators may transmit initial account authenticators and/or resets.

    ii. If encrypted transmission is unavailable, helpdesks must use a documented alternate communication method, such as phone, text, or voice communications, to transmit authenticators to users.

f. For self-service password/passphrase reset systems, requiring users to validate their identity through designated, previously established verification methods, such as multi-factor authentication, to ensure secure access to systems and data, where technically possible.

    i. When not technologically possible within a self-service password/passphrase reset system (i.e., helpdesk password resets, etc.), the agency must establish and implement alternate identity verification methods strong enough to prevent account compromise, identity theft and other fraudulent activities.

g. Expiring unused temporary authenticators within 14 days.

h. As soon as a password/passphrase is suspected to have been compromised, requiring a password reset.

i. Enforcing minimum password/passphrase complexity of:

    i. A minimum of eight (8) characters.

    ii. A minimum of one (1) numeric and one (1) special character.

    iii. Contain a mixture of at least one (1) uppercase and one (1) lowercase letter.

j. Setting the password history to disallow the reuse of the last nine (9) passwords/passphrases.

k. Enforcing a minimum password lifetime restriction of one (1) day, except for temporary passwords.

l. Educating users to use significantly different passwords/passphrases at reset and enforcing best practices through technical controls where available.

m. Establishing a maximum of five (5) incorrect login attempts and locking the account for a minimum of fifteen (15) minutes or until reset by an administrator.

    i. Prior to unlocking an account, the user must be identified with the same assurance method used when performing a password reset referenced in 5.f.i. above.

n. Implementing session and token expiration as required by SEC-02-01-S Application Security Standard and documenting the process.

o. Utilizing authentication certificates issued by a WaTech-approved Certificate Authority (CA) for all website security purposes. The use of self-signed certificates is not permitted without waiver.

p. Disabling and de-provisioning inactive accounts following the SEC-06 Access Control Policy requirements.

6. Access to state IT resources or the State Government Network (SGN) requires authentication via the applicable enterprise solution and must employ the following minimum controls.

a. Authenticated access for organizational users requires authentication via the enterprise solution according to the Identity Management User Authentication Standard (183.20.10 section 4.1.1) with the following minimum controls:

    i. Password/passphrase expiration requirements must not exceed 120 days and must be documented in the agency security program; OR password length must be a minimum of 15 characters with a maximum 365-day expiration.

    ii. Multi-factor Authentication (MFA) is recommended for all organizational user access. Verified authentication using MFA is required for high-risk scenarios as determined by the agency's risk assessment process.

1. The outcomes of these evaluations and the final decision must be thoroughly documented.

2. MFA is required for remote access. See the SEC-06-02-S Remote Access Standard.

iii. System administrator accounts must be discrete and used only for administrative functions and must be managed with the following controls:

1. Passwords/passphrases must have a minimum length of 20 characters. Password/passphrase expiration must be every 60 days and meet standard complexity requirements.

2. MFA is required for all system administrator accounts where technically possible. Compensating controls must be documented and implemented in the agency security program when not technically possible.

3. Built-in hosted or cloud service provider accounts may be used to establish and configure services, administrator accounts, and single sign-on (SSO) configurations.

4. Time-bound access and least-privileged authorization based on the duration needed to complete necessary activities are recommended to secure system administrator accounts.

iv. Service accounts must employ the following controls:

1. A discrete account used only for the defined privileges and functions. These accounts must never be used for interactive login. If an individual performs the set up and configuration of service accounts, the password must be reset whenever possible.

2. Passwords should be as long as possible ideally at least 20 characters balancing security with manageability. Complexity requirements should be adjusted to ensure they can be managed efficiently, especially for devices like desk phones. Password expiration policies must be documented in the agency's security program. Provisions must be made for non-expiring passwords when necessary, such as for desk phones to ensure reachability by emergency responders.

3. Authenticators and account secrets must be rotated whenever employees change roles and no longer require access, as feasible. In cases where physical changes are impractical, alternative security measures must be considered and documented.

4. Service accounts must be limited to access only the systems and applications necessary for their functions, adhering to the principle of least privilege.

5. Service accounts do not require MFA.

b. Authenticated access for non-organizational users requires authentication via the enterprise service according to the Identity Management User Authentication Standard (183.20.10 4.2) with the following minimum controls:

i. Password expiration is not to exceed 13 months.

ii. MFA is required for:

1. Access to all category 4 data.

2. Access to Category 3 data that is not the authenticated user's own personal information.

iii. MFA is recommended for access to category 3 data that is the authenticated user's own personal information.

7. **When applicable, WaTech's Office of Cybersecurity will support agencies in determining secure configuration requirements for federated single sign-on integrations as part of the security design review process. See the SEC-02 Security Assessment and Authorization Policy.**

8. **Agencies unable to utilize the designated enterprise service as described by 183.20.10 Identity Management User Authentication Standard must file a waiver request and implement security controls designated in this standard in section 6.a. and 6.b. or equivalent WaTech-approved controls. See POL-01-02-S Technology Policies and Standards Waiver Request Standard.**

9. **Agencies must consider events that may cause a failure of established identification and authentication mechanisms.**

a. As part of SEC-12 IT Disaster Recovery Planning and/or Continuity of Operations Planning (COOP), agencies must identify and document possible scenarios and procedures for modified identification and

authentication mechanisms to facilitate operations in emergency situations.

10. **Beginning January 1, 2026, password length and expiration requirements discussed in 6.a. above will increase.**

    a. Password length will increase to a minimum of 15 characters.

    b. Password expiration will increase to a maximum of 365 days.

    c. All other requirements will remain in effect.

REFERENCES

1. Definition of Terms Used in WaTech Policies and Reports.
2. SEC-08-02-S Encryption Standard.
3. SEC-08-01-S Data Classification Standard.
4. MGMT-01-01-S Application Inventory.
5. SEC-02-01-S Application Security Standard.
6. SEC-06 Access Control Policy.
7. Organizational User Identity Management & User Authentication Enterprise Service Standard (183.20.10 4.1).
8. SEC-06-02-S Remote Access Standard.
9. Non-Organizational User Identity Management & User Authentication Enterprise Service Standard (183.20.10 4.2).
10. SEC-02 Security Assessment and Authorization Policy.
11. POL-01-02-S Technology Policies and Standards Waiver Request Standard.
12. SEC-12 IT Disaster Recovery Planning
13. NIST Cybersecurity Framework Mapping:
    - PROTECT.ACCESS CONTROL-6: Identities are proofed and bound to credentials and asserted in interactions.
    - PROTECT.ACCESS CONTROL-7: Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks)

CONTACT INFORMATION

- For questions about this policy, please email the WaTech Policy Mailbox.