SEC-06
State CIO Adopted: May 28, 2024
TSB Approved: June 24, 2024
Sunset Review: June 24, 2027

Replaces:
Securing IT Assets Standard 141.10 (6.1)
November 17, 2017

WaTech
Washington Technology Solutions

ACCESS CONTROL POLICY

See Also:
RCW 43.105.054 OCIO Governance
RCW 43.105.205 (3) Higher Ed
RCW 43.105.020 (22) "State agency"

1. **Agencies must manage user or system access throughout the account life cycle from the identification of a user to the granting, modification or revocation of a user's access privileges following the principle of least privileges.**

    a. Agencies must document a procedure or procedures that address the following events:

        i. User account issuance, management, maintenance, and revocation.

        ii. Recording of all user access requests and their subsequent approval status.

        iii. Recording of all changes in user access privileges.

        iv. Unauthenticated access requests.

            1. Unauthenticated access may only be granted to category 1 public data, forms submission, FTP file uploads, etc.

    b. Agencies must define and document approved access levels.

    c. Agencies must maintain and review account access logs in accordance with the SEC-09-01-S Security Logging Standard to verify that only authorized user accounts have access privileges.

    d. Agencies must revoke access for any user no longer employed or under contract within one (1) business day of termination.

        i. Agencies must develop a procedure to notify IT of employment status changes, including termination.

    e. Agencies must perform a user access review, at a minimum, semiannually. Review of privileged accounts must occur at least quarterly.

        i. Agencies must remove all unauthorized accounts and access

discovered during the user access review procedure.

ii. Agencies must disable accounts after 90 days of inactivity.

f. Agencies must establish procedures for obtaining necessary access to information systems during an emergency. See the SEC-12 IT Disaster Recovery Planning Policy and Incident Response Policy (SEC-0-141.10, section 11).

g. Display banner text conveying the ownership and appropriate system use before the user logs into an agency-owned computer or network device. See NIST 800-53 (AC-8: System Use Notification).

i. Display banners are used only for access via login interfaces with human users and are not required when such human interfaces do not exist.

ii. Specific language for banner text may be required based on federal or other requirements.

2. **Agencies must separate conflicting access privileges so that no one person can perform any tasks that lead to fraudulent activity.**

3. **Agencies must determine the access levels of a user in the system based on the user's role in the organization.**

a. Whenever technically and administratively feasible, separate user functions from administrative (management) functions.

i. Standard user accounts must not include elevated permissions.

ii. Administrative roles requiring privileged or elevated access should be performed using separate authentication credentials.

b. Whenever technically and administratively feasible, the access level must be based on:

i. The user's level of identity assurance and the risk associated with the access permission and;

ii. The apparent immediate business need to obtain or exercise that level of access permissions.

c. Access controls must be appropriately robust for the risk of the application or systems to prevent unauthorized access to IT assets. See the Risk Assessment Standard.

d. Manage and group systems, data, and users into security domains and establish appropriate access requirements within and between each security domain.

e. Limit access to and use of programs or utilities capable of overriding system and application controls to system administrators.

4. **To ensure appropriate management of user accounts on system components, agencies must:**

a. As described in the Identification and Authentication Standard (SEC-0-141.10 6.3, 6.4), identify users with a unique identifier, for their individual use only, before allowing them to access components, systems, networks, or data.

b. Ensure that accounts are assigned access only to the services that they have been specifically authorized to use.

c. Ensure the access rights of users to information and information processing facilities are removed upon suspected compromise, termination of their employment or contract, or are adjusted upon change in status.

d. Implement mechanisms to restrict and control the use of privileges.

i. Whenever technically and administratively feasible, require users to document their use and/or elevation of privileged account credentials.

e. Enable accounts used by vendors for remote maintenance only during the time needed.

f. Always ensure and enforce non-repudiation of all account use, such as through technical and administrative controls prohibiting the use of group, shared, or generic accounts.

g. Establish a maximum of five failed login attempts and lock the account for a minimum of 15 minutes or until reset by an administrator.

h. Agencies must remove all unauthorized accounts and access discovered during the user access review procedure.

i. Agencies must revoke access for any user no longer employed or under contract within one (1) business day of termination.

i. Agencies must disable accounts after 90 days of inactivity.

REFERENCES

1. SEC-09-01-S Security Logging Standard.
2. SEC-12 Disaster Recovery Policy.
3. Incident Response Policy (SEC-0-141.10, section 11).
4. Risk Assessment Standard.
5. Identification and Authentication Standard (SEC-0-141.10 6.3, 6.4).
6. Definition of Terms Used in WaTech Policies and Reports.
7. NIST Cybersecurity Framework Mapping
    - Protect.Identity Management, Authentication and Access Control-1 (PR.AC-1): Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users, and processes.
    - Protect.Identity Management, Authentication and Access Control-2 (PR.AC-2): Physical access to assets Is managed and protected.
    - Protect.Identity Management, Authentication and Access Control-3 (PR.AC-3): Remote access is managed.
    - Protect.Identity Management, Authentication and Access Control-4 (PR.AC-4): Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties.

CONTACT INFORMATION

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