WaTech
Washington Technology Solutions

Access Control Policy Background

New, Update or Sunset Review? Sunset Review. Replaces 141.10 6.1,6.2

What due diligence was conducted to determine the content of this policy/standard? If this is an update or sunset review, provide information as to what changes were made, if any, as well as reasons behind the policy/standard content.

Changes were made based on workgroup and community feedback to improve clarity for agency adoption and accountability.

Updates to this policy draw from NIST 800-53r5 and CIS controls.

What is the business case for the policy/standard?

Controls are necessary to ensure that only authorized individuals can access information systems and data assets.

What are the key objectives of the policy/standard?

- Requires agencies to exercise principles of least privilege when providing system access.
- Requires management of user accounts on system components.

How does policy/standard promote or support alignment with strategies?

Access control strengthens IT security and by aligning the business need with the technical privileges given, minimizing impacts of any security breaches.

What are the implementation considerations?

<What are the business & technical implementation impacts on agencies & staff, OCM, communications strategies, etc.>

There were not substantial changes that would require major changes, but agencies may need guidance and support to ensure they are applying the policy as intended.

How will we know if the policy is successful?

Specific: Agencies will use principles of least privilege when assigning permissions.
Measurable: Agencies will monitor access and keep records of changes.
Achievable: Agencies have tools available to support these standards but may need additional training.
Relevant: Access control is a tool to limit damage if a threat actor gets credentials.
Timely: The policy is effective when adopted by the state CIO.
Equitable: Agencies of all sizes are at risk for cybersecurity attacks, and all agencies can limit the risk through appropriate access controls.

SEC-06
State CIO Adopted: Month 1 2023
TSB Approved: Month 1 2023
Sunset Review: Month 1 2023

Replaces:
Securing IT Assets Standard 141.10 (6.1,6.2)
Month 1, 2023

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.
- For technical assistance, please email confirmemail@watech.wa.gov

Commented [ZS(1]: @Johnson, Ralph (WaTech) is there a technical contact we should list for this?

PROPOSED DEFINITIONS

Privileged Account (Access): Accounts with permissions to change system configurations, or create, modify, or delete users.

Non-Repudiation:

Current definition: Assurance that the sender of information is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the information.

Recommended Change: Repudiation refers to the ability of a user or system to deny having performed a particular action or transaction.

Non-repudiation is the assurance that a user cannot deny (repudiate) having performed a transaction. Non-repudiation combines authentication and integrity:

non-repudiation authenticates the identity of a user who performs a transaction and ensures the integrity of that transaction.

Context-restricted least privilege: requiring just-in-time identity verification, authentication or authorization when attempting to create, modify, or delete user accounts or system configurations with any account not primarily and extensively used for such purposes on a daily basis.

mandatory justification of privileged access: as a condition of employment or contract, require users to document immutably their purpose for accessing privileged account credentials, or for elevating to or exercising technical or administrative permissions to create, modify, or delete user accounts or system configurations.

Least Privilege Principle

The principle that a security architecture should be designed so that each entity is granted the minimum system resources and authorizations that the entity needs to perform its function.

User
Employees, volunteers, and other persons whose conduct, in the performance of work for an agency, is under the direct control of the agency, whether or not they are paid by the agency. This includes, but may not be limited to, full and part time elected or appointed officials, employees, contractors, affiliates, associates, students, volunteers, and staff from third party entities who provide service to the agency.