SEC-02-01-S
State CIO Adopted: April 1, 2024
TSB Approved: Pending
Sunset Review: Pending

Replaces:
IT Security Standard 141.10 (7.1-7.5)
November 13, 2017

WaTech
Washington Technology Solutions

APPLICATION SECURITY STANDARD

See Also:
RCW 43.105.054 OCIO Governance
RCW 43.105.205 (3) Higher Ed
RCW 43.105.020 (23) "State agency"
141.10 (1.2.1) Security Assessment and Authorization Standard

1. **Agencies must document application data protection requirements based on the classification of data that applications are processing, storing, and reporting on. See the Data Classification Standard.**

2. **Agencies must perform application risk assessments consistent with the Information Security Risk Assessment Standard.**

3. **Agencies must use secure coding practices which support security requirements, whether for outsourced, low-code/no-code or in-house projects. These include, but are not limited to the following:**

    a. Ensure that the application only accepts correct inputs.

    b. Ensure that the application responds as expected and that the output does not reveal information about the application functionality.

    c. Whenever possible, use tested and approved code for common tasks rather than creating new, untested code.

    d. Leverage the identification and authentication controls. See Identity Management/User Authentication and Identification and Authentication.

    e. Follow CIS controls required by the Configuration Management Standard.

    f. Limit connectors to an approved services list.

    g. Monitor platforms for data flow outside of the organizational boundary, including multi-hop paths.

    h. Follow the Asset Management Policy to maintain an inventory.

    i. Remove or disable unused dependencies, unnecessary features, components, files, and documentation.

j. Configure security logs according to the Security Logging Standard.

k. Use WaTech-approved authentication methods and services to validate users accessing the application and all resources within the application. See the 141.10 (6.3) - Identification and Authentication Standard for more details.

l. The application must recognize only session identifiers issued by the server or application framework as valid.

m. Agencies must document and implement authenticated session expiration.

n. Restrict access to files and other resources to only authorized users.

o. All cryptographic modules used by the application must comply with the Encryption Standard.

p. Ensure user-facing error handling does not provide details on how the application works or about the system on which it resides.

q. Implement application logging controls on the server.

r. Implement least privilege to restrict users to the functionality, data and application information required to perform their tasks.

s. Agencies may use Software Quality Best Practices Guidelines or Open Web Application Security Project's (OWASP) The Ten Most Critical Web Application Security Vulnerabilities.

4. Agencies must develop software applications based on industry best practices and include information security throughout the software development life cycle, including the following:

a. Separate development, test, and production environments, where possible.

b. Production data used for development testing must not compromise privacy or confidentiality.

   i. Prohibit the use of category 3 data or higher in development environments unless specifically authorized by the agency's information technology (IT) security program.

   ii. Production data in any environment must meet or exceed the level of protection required by its data classification. See the Data Classification Standard.

c. Removal of test data and accounts before production applications become

live.

d. Review of code prior to moving between environments and production deployment to identify potential coding vulnerabilities as described in the Vulnerability Management Standard.

    i. Where possible, agencies must scan the source code according to the Vulnerability Management Standard.

e. Appropriate placement of data and applications in the IT infrastructure based on their risk and complexity.

5. **Agencies must review and test application changes to ensure there are no adverse impacts on agency operations or security according to the Change Management Policy.**

REFERENCES

1. Definition of Terms Used in WaTech Policies and Reports.
2. SEC-11-01-S Risk Assessment Standard.
3. SEC-05 Change Management Policy.
4. 141.10 (6.3) - SEC-05-01-S Identification and Authorization Standard.
5. SEC-04-03-S Configuration Management Standard.
6. SEC-08-01-S Data Classification Standard.
7. SEC-11-02-S Vulnerability Management Standard.
8. The Open Worldwide Application Security Project (OWASP) Top Ten Web Application Security Risks.
9. NIST Cybersecurity Framework Mapping:
    - Identify.Asset Management-2 (ID.AM-2): Software platforms and applications within the organization are inventoried.
    - Identify.Asset Management-5 (ID.AM-5): Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value.
    - Identify.Risk Assessment-5 (ID.RA-5): Threats, vulnerabilities, likelihoods, and impacts are used to determine risk.
    - Identify.Supply Chain-3 (ID.SC-3): Contracts with suppliers and third-party partners are used to implement appropriate measures designed to meet the objectives of an organization's cybersecurity program and Cyber Supply Chain Risk Management Plan.
    - Protect.Data Security (PR.DS-7): The development and testing environment(s) are separate from the production environment.
    - Protect.Information Protection Processes and Procedures-2 (PR.IP-2): A System Development Life Cycle to manage systems is implemented.
    - Protect.Information Protection Processes and Procedures-3 (PR.IP-3):

Configuration change control processes are in place.

- Protect.Protective Technology-3 (PR.PT-3): The principle of least functionality is incorporated by configuring systems to provide only essential capabilities.
- Detect.Security Continuous Monitoring-4 (DE.CM-4): Malicious code is detected.
- Detect.Security Continuous Monitoring-5 (DE.CM-5): Unauthorized mobile code is detected.
  Detect.Security Continuous Monitoring-8 (DE.CM-8): Vulnerability scans are performed.

CONTACT INFORMATION

- For questions about this policy, please email the WaTech Policy Mailbox.
- For technical assistance, please email WaTech's Risk Management Mailbox.