SEC-01-01-G
State CIO Adopted: Dec. 10, 2024
TSB Approved: Dec. 10, 2024
Sunset Review: Dec. 10, 2027

Replaces:
N/A

WaTech
Washington Technology Solutions

SECURITY PRINCIPLES GUIDELINE

See Also:
RCW 43.105.054 WaTech Governance
RCW 43.105.205 (3) Higher Ed
RCW 43.105.020 (22) "State agency"
RCW 52.105.450 (6, 8) Office of Cybersecurity – Higher education, Judicial, and Legislative
RCW 52.105.450 (3j, 7a) Office of Cybersecurity – Agency IT Security Program
RCW 42.56.420 Security

The following principles are a framework for Washington State information security practices and platform implementations:

a. Accountability – Clearly define accountability and responsibility for information security within a structured cybersecurity management framework. Both management and staff should acknowledge and accept their roles to ensure compliance and oversight.

b. Risks – Risks to information systems and data should be assessed periodically and managed continuously as part of a robust state cybersecurity risk management strategy that addresses emerging threats, vulnerabilities, and risks to maintain a secure environment.

c. Awareness– Ensure all users with access to information systems or data are consistently aware of the importance of information security and their role in maintaining it.

d. Cost Effective – Information security controls should be cost-effective and proportionate to the identified risks. Resource allocation for security measures will be optimized to ensure maximum protection without unnecessary expenditure.

e. Ethical – Information systems and data will be used and operated in accordance with the state's ethics policies and practices, ensuring ethical conduct in all information security activities.

f. Defense-in-Depth – Select and architect information security controls with a "Defense-in-Depth" approach, employing multiple layers of protection to defend against potential security threats comprehensively.

g. Equitable – Information security policies should balance the rights of customers, users, and third parties with the state's operational needs. This balance is crucial to achieving the state's objectives while respecting individual rights.

h. Governance–Information security policies and standards should be developed based on industry-recognized security standards and best practices. These policies and standards will undergo periodic reviews, and corrective actions will be taken to promptly remediate identified deficiencies.

i. Integration – Information security is fundamental to sound business management. It should be integrated into the state's overall information management framework to support and enhance business operations.

j. Minimize Complexity – Information technology services and systems should be designed to minimize technological diversity and reduce complexity. Simplifying the technology landscape will enhance manageability and security.

k. Least Privilege – Grant only the minimum necessary privileges to users, systems, and processes required to perform their assigned functions, limiting potential damage from accidental or intentional misuse of access.

l. Separation of Duties – Responsibilities and privileges should be segregated to prevent any individual or small group from controlling multiple critical aspects of a process. This separation is vital to preventing inappropriate actions and mitigating potential harm or loss.

m. Timeliness – Agencies should act promptly and in a coordinated manner to prevent, detect, and respond to potential incidents affecting information systems or data. Timely action is essential to mitigate risks and maintain system integrity.

REFERENCES

1. Definition of Terms Used in WaTech Policies and Reports.

CONTACT INFORMATION

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

PROPOSED DEFINITIONS

Separation of Duties

The principle is that no single user should have sufficient privileges to misuse the system or process independently.