SEC-05
State CIO Adopted: August 11, 2023
TSB Approved: September 14, 2023
Sunset Review: September 14, 2026

WaTech
Washington Technology Solutions

Replaces:
IT Security Standard 141.10 (8.1)
December 11, 2017

CHANGE MANAGEMENT POLICY

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"
SEC-11 Risk Management Policy

1. **Agencies must document change management roles and responsibilities to reduce opportunities for unauthorized changes.**

Role	Responsibilities
Requestor	The requestor submits the change request.
Implementer	The implementer deploys the change into production. The implementer is the person or team that records the implementation results.
Approver	The approver is responsible for deciding whether a change is fit to proceed to implementation by examining the evidence in the change request.
Change Advisory Board (CAB)	The group who assesses, prioritizes, and authorizes changes as part of the agency's change control process.

2. **Agencies must identify and document how they will ensure implementation of approved changes only.**

3. **Agencies must designate a change approver separate and distinct from the individuals authorized to request and implement changes. Agencies must implement and document compensating controls if separation of duties is not possible between the Requestor and Implementor due to resource constraints.**

4. **Agencies must document acceptance criteria for all changes to minimally include:**

a. A description of the change.
b. The impact of the change.
c. The justification for the change.
d. The implementation and communication plan.
e. A risk and impact analysis of the change. See SEC-11-01-S Risk Assessment Standard.
f. A plan to test the change.
g. A back out plan to roll back changes if something goes wrong.
h. The planned start date and planned end date of the change.

5. **Agencies must classify requested changes consistent with the change types in the table below:**

Change Type	Description
Normal	• A normal change must be evaluated, authorized, and scheduled according to a standardized change management process.
Standard	• Low risk, low impact, highly repeatable change with very little possibility of adversely impacting the production environment.
Emergency	• Not able to meet the minimum lead-time requirements for normal change request. Service Owner/Configuration Item (CI) Manager will approve instead of Change Advisory Board (CAB) due to time constraints. Separation of Duties (SOD) may be deferred. Approvals that do not violate SOD should be provided as a follow-up to any emergency change. • Urgent changes must satisfy two criteria for auto-approval: 1. The change is related to a high or critical priority incident. 2. The incident is in a non-closed status.

6. **Agencies must independently meet change management requirements from third-party regulatory authorities, such as CJIS or HIPAA.**

REFERENCES

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

2. SEC-11-01-S Risk Assessment Standard.
3. NIST Cybersecurity Framework Mapping:
    - Identify.Governance (ID.GV-2): Cybersecurity roles and responsibilities are coordinated and aligned with internal roles and external partners
    - Protect.Information Protection Processes and Procedures (PR.IP-3): Configuration change control processes are in place.

CONTACT INFORMATION

- For questions about this policy, please contact the WaTech Policy Mailbox.
- For technical security questions and risk management document submissions, contact the WaTech's Risk Management Mailbox.