Washington State Human Rights Commission

Policy No. 2025-07

Business Application & System Governance

Applies to: Applies to all business-critical applications/systems owned, procured, or maintained by WSHRC, including those shared with external entities.

Governance: Listed below are some, but not all, applicable governing requirements. (*Note: Laws and rules may change over time, and such changes may take precedence over this policy.*)

Authority: WaTech State Office of Cybersecurity

WaTech Cybersecurity policies

Executive Sponsor (Business Owner – Executive Director)

- WSHRC leader accountable for application performance, business value, and strategic alignment.
- Qualifications include understanding business goals, decision-making authority, and resource ownership.

Technical Owner (IT Manager)

- IT representative responsible for technical integrity, security posture, and maintenance.
- Responsible for compliance with enterprise architecture and OCS security standards .

Governance Committee

- Includes Executive Sponsor, Technical Owner, and potentially other stakeholders (finance, security, users).
- Meets quarterly to review:
    1. Defect logs and defect remediation progress
    2. Enhancement requests and prioritization
    3. Security & risk assessment outcomes
    4. Inventory status and maintenance costs
    5. Strategic lifecycle decisions (update, enhance, replace, or retire)
        - WaTech Business Application/System Governance Policy
        - WA State Auditor Controls to Manage Outdated Computer Applications

Approved by: _____ **Effective Date:** 07.18.2025

Andreta Armstrong, Executive Director

Purpose & Definition

To establish a governance framework for business applications/systems that ensures alignment with WSHRC's business objectives, promotes accountability, supports risk management, and complies with OCS standards watech.wa.gov.

Policy Statement

Inventory Management

- Maintain a centralized register of all business applications.
- Include details: owner, steward, vendor, version, risk/security ratings, maintenance costs, lifecycle stage.

Requests & Defect Management

- Implement formal logging for defects and enhancements.
- Categorizations: (a) Business-critical defects, (b) Minor enhancements, (c) Major enhancements.
- Governance Committee reviews submissions, categorizations, and action plans.

Risk & Security Assessments

- Perform periodic (at least annual) formal risk and security assessments, including vulnerability scans and remediation tracking.
- Technical Owner ensures compliance with OCS mandates watech.wa.gov & Washington State Auditor.

Lifecycle Strategy

- At defined intervals (every 6 months) or upon end-of-life notification, evaluate one of the four OCS-defined options :
    1. Accept the risk
    2. Update the system
    3. Enhance the system
    4. Replace/retire the system
- Use documented, balanced cost–risk–benefit analyses to inform decisions.

Cost Monitoring

- Track total lifecycle cost: licensing, support, maintenance, enhancements, upgrades.
- Incorporate cost trends into governance reviews and risk analyses

Responsibilities

Role	Responsibilities
Executive Sponsor	Accountability, resource approval, lifecycle decisions
Technical Owner	Technical oversight, security/risk compliance, defect/enhancement processing
Governance Committee	Oversight, prioritization, policy compliance
IT & Security Staff	Support assessments, remediation, documentation

Reporting & Documentation

- Produce quarterly governance reports summarizing items in Governance Committee section
- Keep records of meetings, decisions, assessments, and remediation outcomes.

- Report key performance indicators (KPIs): open defects, resolution time, assessment findings, maintenance cost trends.
- IT Manager will create a tracking log and track incidents reported by staff and external parties relating to disruptions in accessing the CMDb or incidents and disruption relating to use of the CMDb

How to Report an Incident or Disruption

- **HUM staff are to alert your Manager and the IT Manager directly by email and cc the Assistant Director**
- **Report what the specific incident or disruption event was.**
- **Provide the date and time of the event**

Policy Review & Updates

- Annual policy review by Governance Committee to integrate OCS updates, accelerate modernization, or update governance practices.

Compliance & Consequences

- All staff must adhere to this policy.
- Non-compliance may lead to executive escalations, suspension of system changes, or funding reallocation.

Resources

- Chief Information Officer Policy Statement
- WaTech DL OCS Security Design Review: **sdr@watech.wa.gov**
- WaTech OCS Security Operations Center: **SOC@watech.wa.gov**
- WaTech Risk Management: **RiskManagement@watech.wa.gov**
- WaTech mi Security: **security@watech.wa.gov**
- WaTech Business Application/System Governance Policy
- WA State Auditor Controls to Manage Outdated Computer Applications

---

History

First Effective: 07/21/2025

Review Cycle: Annually or upon Office of Cybersecurity (OCS) update

Amended: