Washington State
Department of Social
& Health Services

Transforming lives

Administrative Policy No. 15.10

Subject: Information Security

Information Contact: DSHS Chief Information Security Officer
MS 45889 (360) 902-8443

Authorizing Source: RCW 42.56.420 - Security
RCW 70.02.150 - Security safeguards
RCW 71A.14.070 - Confidentiality of information--Oath
CJIS Security Policy, Chapter 5
IRS Publication 1075 - Tax Information Security Guidelines for Federal, State and Local Agencies
Governors Directive 16-01 - Providing Accountability for State Systems Responsible for Critical Functionality.
Governor's Executive Order 00-03 Public Records Privacy Protections
OCIO Policy 141 - Securing Information Technology Assets

Effective Date: October 30, 1990

Revised: September 14, 2020

Approved By: **Original signed by Lori Melchiori**
Senior Director, Office of Policy and Rules

Purpose

The DSHS Information Security Standards Manual contains department-wide standards for information security designed to protect department information and information technology resources. This policy establishes the requirement to comply with the standards and assigns responsibility for maintenance of the standards to the DSHS Information Security Office.

Scope

This policy applies to all DSHS organizational units and all DSHS employees, contractors, interns, vendors, volunteers, and business partners.

Definitions

Business continuity plan: A plan developed by an organizational unit describing how the unit will recover from and continue to provide mission critical services in the event of a disaster. In the context of the overall business workflow and priorities, the plan identifies critical IT systems and resources needed to restore or continue services. In addition, the plan defines how soon the IT systems and resources must be available after a disaster.

Chief information security officer (CISO): The information security authority for the department.

CXO: This includes various staff within the department holding the positions of chief information officer, chief administrative officer, chief risk officer, or chief financial officer.

Department information: All information in hard copy or electronic format that is available for use by staff, contractors, and partners to carry out the department's mission.

IT disaster recovery plan: A component of an organizational unit's business continuity plan that describes how they will identify and support recovery of IT functions following a disaster.

IT resources: Includes all computing, and telecommunications facilities, data, hardware, software and information technology staff.

Information security (InfoSec): The practice of preventing unauthorized access, use, disclosure, disruption, modification, inspection, recording or destruction of information regardless of the form the data may take (e.g., electronic, physical).

Information security office (ISO): The department-level information security team, comprised of the Chief Information Security Officer and their staff. Their primary focus is the balanced protection of the confidentiality, integrity and availability of data (also known as the CIA triad) while maintaining a focus on efficient implementation of the security policy and standards.

Information Security Standards Manual: The ISSM provides information to support the confidentiality, integrity, and availability of department information and information technology systems and resources through administrative, physical, and technical controls.

Information technology security administrator (ITSA): This is the senior information security authority within an administration or division.

Office of the Chief Information Officer (OCIO): The OCIO sets information technology policy and direction for the state of Washington. The State CIO is a member of the governor's executive cabinet and advisor to the governor on technology issues.

Organizational unit: An administration, division, or office within the department.

Security design review: The formal process whereby proposed new IT systems or upgrades are reviewed to identify and address potential security vulnerabilities. Administrations and the information security office work together to complete the review.

Policy Requirements

The information security office, under the direction of the DSHS chief information security officer, is responsible for developing and maintaining agency-level information security policies and standards. The security standards are maintained in the DSHS Information Security Standards Manual and include specific, detailed information including, but not limited to, security requirements, and roles and responsibilities. Administrations may develop additional policies and standards, as strict as or stricter than the department-level, as appropriate to their administration, divisions, and programs.

Roles and Responsibilities

A. The DSHS CISO, or their designee, is responsible for:

1. Administering the DSHS information security program;
2. Developing and maintaining department-level information security policies, standards, and procedures;
3. Developing and providing security awareness training and elevated privileges training;
4. Coordinating federal and state information security audits;
5. Conducting department information security audits;
6. Preparing and/or providing state and federal information security reports;
7. Coordinating response activities for department-level information security incidents;
8. Providing consultation to DSHS staff regarding information security;
9. Assisting the administrations' ITSAs in developing security design review and threat analysis documents for CISO approval, as required and defined in the DSHS Information Security Standards Manual - Chapter 6, prior to purchases, upgrades, implementations, and as required during implementation stages;
10. Conducting final security design reviews and threat analyses of submissions to the CISO and determine if a security design review and threat analysis requires referral to the WaTech Office of Cybersecurity;
11. Providing oversight, consultation, and guidance to department staff on IT disaster recovery planning and testing; and
12. Developing and approving contract security language, and review and approve any changes to contract security language.

B. DSHS assistant secretaries and CXOs, or their designees, are responsible for implementing the requirements of this policy for their respective organizational units by:

1. Complying with all policies, standards, and procedures in the DSHS Information Security Standards Manual, the DSHS IT Standards Manual, the OCIO policies and standards, and all applicable state and federal laws and regulations;;
2. Developing and maintaining business continuity plans;

3. Developing and maintaining IT disaster recovery plans based on the organizational unit's business continuity planning;
4. Updating and testing the IT disaster recovery plans annually; and
5. Updating and submitting IT disaster recovery plans annually to the CISO as specified in the DSHS Information Security Standards Manual.

C. DSHS information technology security administrators are responsible for implementing the requirements of this policy for their respective administration or division by:

1. Assisting their administrations in implementing and complying with department-level information security policies, standards, and procedures;
2. Developing and maintaining administration-level security policies, standards, and procedures as needed to meet the business needs of their administrations, while complying with department-level policies and standards, and all applicable state and federal laws and regulations;
3. Applying established security measures and rules to systems, applications, and information to ensure the confidentiality, integrity and availability of department data, and for safeguarding department information resources;
4. Performing initial troubleshooting before escalation of security issues to the ISO;
5. Working with the ISO to develop security design reviews and threat analyses for submission to the CISO or their designee, as required and defined in the DSHS Information Security Standards Manual - Chapter 6, prior to purchases, upgrades, implementations, and as required during implementation stages;
6. Coordinating with the ISO on the development of IT disaster recovery planning and testing; and
7. Providing oversight and consultation on threat modeling to application development staff.

D. All DSHS managers and supervisors are responsible for:

1. Ensuring that their staff follow applicable department and administration information security policies, standards, and procedures; and
2. Applying and documenting appropriate corrective actions and sanctions, as identified in the DSHS Information Security Standards Manual, when staff violate the department's information security policies and standards.

E. All DSHS employees, contractors, interns, vendors, volunteers, and business partners who have access to department information are responsible for the following:

1. Protecting information systems against theft, tampering, and loss from both insider and outsider threats by controlling physical and logical access to all department facilities, systems, and data;

2. Complying with all policies, standards, and procedures in the DSHS Information Security Standards Manual, the DSHS IT Standards Manual, the OCIO policies and standards, and all applicable state and federal laws and regulations;
3. Complying with their administration's information security policies, standards, and procedures;
4. Complying with software licensing provisions;
5. Completing annual DSHS information security awareness training in addition to appropriate role based security training;
6. Protecting department information according to its level of sensitivity, as identified in the DSHS Information Security Standards Manual; and
7. Understanding and meeting their organizational unit's business continuity and disaster recovery plan requirements, as defined for their position.