

Administrative Policy No. 15.10

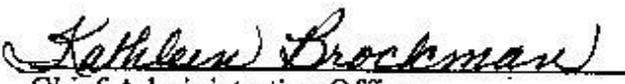
Subject: Information and Technology Security

Information Contact: DSHS IT Security Administrator
MS 45889 (360) 902-7615

Authorizing Source: CFR 45 Public Welfare, [Part 95](#) and [Chapter III](#)
CFR 7 Agriculture, [Part 227](#) (Food Stamps)
[CFR 40](#), Public Documents, Records, and Publications
[Chapter 13.50 RCW](#), Keeping and Releasing Juvenile
Records
[Chapter 42.17 RCW](#), Disclosure - Public Records Section
[Chapter 70.02 RCW](#), Medical Records - Disclosure
[RCW 70.96A.150](#), Alcohol and Drug Abuse, Records
[RCW 71A.14.070](#), Developmental Disabilities, Records
[Chapter 71.05 RCW](#), Mental Illness,
Sections 390, 395, 420, 620, 630 - 690
[Title 74 RCW](#), Public Assistance
[RCW 74.04.060](#), Records – Confidential
[RCW 74.09.290](#), Patient Records – Confidential
[RCW 74.09A.020](#), Computerized Information
[Chapter 74.13 RCW](#), Child Welfare Services
Sections 133, 500 - 525

Effective Date: October 30, 1990

Revised: December 21, 2007

Approved By: 
Chief Administrative Officer

Sunset Review Date: December 21, 2011

Purpose

This policy identifies the roles and responsibilities for the department's Information and Technology Security Program designed to protect department information and information technology (IT) resources.

Scope

This policy applies to all organizational units of the department.

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. The plan identifies critical IT systems and IT resources needed to restore or continue services and defines how soon the IT resources must be available after a disaster.

CXO: Staff in DSHS who hold the position 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 and/or contractors/partners to carry out the mission of the department.

Organizational Unit: An administration, division, or office that functions at a headquarters, regional or local office level within DSHS.

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.

DIS Data Center: Primary computer operations center, operated and maintained by the Department of Information Services (DIS).

Information Technology Security Section: This is a unit within the Information System Services Division (ISSD). This unit is managed by the Information Technology Security Administrator (ITSA) and helps accomplish the responsibilities of the ITSA.

IT Resources: All computing and telecommunications facilities, hardware, and software.

Policy

- A. The DSHS ITSA is responsible for administering the department's Information Technology Security Program. The ITSA:
1. Develops and maintains DSHS IT security policies, standards, procedures, and training.
 2. Coordinates federal and state IT security audits.
 3. Conducts agency IT security audits.
 4. Prepares state and federal IT security reports.
 5. Coordinates activities for agency-level IT security incidents.

6. Provides consultation to DSHS staff regarding IT security.
 7. Develops and maintains the DSHS IT Disaster Recovery Manual.
 8. Provides consultation to DSHS staff on IT disaster recovery planning.
 9. Coordinates testing of the agency Disaster Recovery Plan for DSHS mainframe applications at the DIS Data Center.
- 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 applicable state and federal policies on IT security and the policies and standards outlined in the [DSHS IT Security Policy Manual](#) and the [DSHS IT Security Procedures Manual](#).
 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. Testing the IT disaster recovery plans annually.
 5. Updating and electronically submitting IT disaster recovery plans annually to the ITSA as specified in the DSHS IT Security Manual.
- C. DSHS employees are responsible for:
1. Complying with applicable state and federal policies on IT security.
 2. Complying with the requirements of the [DSHS IT Security Policy Manual](#) and the [DSHS IT Security Procedures Manual](#).
 3. Understanding any requirements their organizational unit's business continuity and disaster recovery plans may define for their position.