Washington State Department of Social & Health Services

Transforming lives

Administrative Policy No. 5.08

Subject:	DSHS Minimum Physical Security Standards for Confidential Information and Financial Instruments
Information Contact:	Security Rule Program Manager Office of Information Governance Phone: (360) 902-7756, MS: 45135
Authorizing Source:	HIPAA Security and Privacy Rules – 45 CFR Part 164 IRS Publication 1075 Social Security Administration EIES OCIO 141.10 Standards
Effective Date:	November 9, 2015
Revised:	April 6, 2022
Approved By:	Original signed by Dana Phelps Senior Director, Office of Policy and Rules

Purpose

This policy establishes the Department of Social and Health Services (DSHS) minimum physical security standards necessary to safeguard confidential information and financial Instruments located within DSHS offices and facilities as required by law.

Background

The National Institute of Standards and Technology (NIST) Special Publication 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations,* identifies the minimum standards necessary for DSHS to appropriately manage the physical security of its confidential information and financial instruments. The adoption of these standards is necessary to ensure the safeguarding of confidential information and financial instruments for which DSHS is fully responsible. These standards are applicable to every DSHS-owned and leased office and facility.

DSHS routinely undertakes a diverse range of business. As a result, unique program work may require additional security measures beyond the minimum standards at some DSHS locations. Administration leadership must work closely with their staff to assess and analyze those circumstances that may require additional security standards and apply them as necessary.

This policy provides links to procedural templates, which have been included to assist DSHS administrations with creating and implementing a basic framework of minimum physical security standards at their offices and Facilities. These templates will still allow programs considerable flexibility to manage general and unique conditions at locations within their area of responsibility.

Scope

This policy applies to all DSHS facilities where either confidential information, financial instruments, or both are stored.

Additional Guidance

For related, useful information see:

- DSHS Information Security Standards Manual:
  - Information Security Standard 3.1, *Classify Information According to Level of Protection Needed*
  - Information Security Standard 3.2, *General Protection Requirements*
  - Information Security Standard 3.3, *Protecting Information in Computers, Hard Copy Documents and Removable Media*
  - Information Security Standard 3.10, *Work Areas*
  - Information Security Standard 11.2, *Requirements for Safeguarding IRS Information*
- DSHS Administrative Policy 5.01, *Privacy Policy – Safeguarding Confidential Information*
- DSHS Administration Policy 14.15, *Building Management of DSHS Leased Facilities*
- DSHS Administration Policy 15.10, *Information Security*
- OCIO Policy 141.10 , *Securing Information Technology Assets Standards*
- NIST Special Publication 800-53 Revision 5, *Security and Privacy Controls for Federal Information Systems and Organizations*
- National Fire Prevention Association (NFPA) Code 730, *Guide for Premises Security*

Definitions

Building management committee: A standing committee formed at each facility that houses two or more DSHS tenants to coordinate on site facility maintenance and operations. The committee must consist of one representative from each DSHS tenant program occupying space in the facility. The building management committee representatives have delegated authority from their respective program to:

- Participate in and make building management decisions and coordinate funding approval from their chain of command as needed.
- Define rules for the facility to include, but not limited to security procedures.

Building manager: The primary building contact for a facility/campus to the lessor, other

building tenants, and leased facilities unit (LFU) staff for day-to-day and on-going issues. This position may have other responsibilities outside of these functions and may have responsibilities for multiple facilities.

Data classifications: The classification of data into categories based on the sensitivity of the data. For example, the Office of the Chief Information Officer (OCIO) Standard 141.10, Section 4.1, requires state agencies to follow these designated classification categories:

1) Category 1 – Public information
   Public information is information that can be or currently is released to the public. It does not need protection from unauthorized disclosure, but does need integrity and availability protection controls.

2) Category 2 – Sensitive Information
   Sensitive information may not be specifically protected from disclosure by law and is for official use only. Sensitive information is generally not released to the public unless specifically requested.

3) Category 3 – Confidential information
   Confidential information is information that is specifically protected from either release or disclosure by law. This includes, but is not limited to:
   a. Personal information as defined in RCW 42.56.590 and RCW 19.255.10.
   b. Information about public employees as defined in RCW 42.56.250.
   c. Lists of individuals for commercial purposes as defined in RCW 42.56.070.
   d. Information about the infrastructure and security of computer and telecommunication networks as defined in RCW 42.56.420.

4) Category 4 – Confidential Information Requiring Special Handling
   Confidential information requiring special handling is information that is specifically protected from disclosure by law and for which:
   a. Especially strict handling requirements are dictated, such as by statutes, regulations, or agreements.
   b. Serious consequences could arise from unauthorized disclosure, such as threats to health and safety, or legal sanctions.

Enterprise Technology Division: Provides department-wide information technology services.

Facilities: Means physical spaces such as offices and buildings owned by DSHS or leased on its behalf to meet the space requirements of one or more programs.

Financial instruments: A tradable asset such as cash, evidence of ownership, or a contractual right to receive or deliver another Financial Instrument.

HIPAA: The Health Insurance Portability and Accountability Act of 1996, 42 USC 1320d et seq. To implement HIPAA, the U.S. Department of Health and Human Services Office for Civil Rights (OCR) has adopted the HIPAA Privacy Rule, Security Rule and Breach Notification Rules.

HIPAA Rules: References to the "HIPAA Rules" apply to the following rules that OCR enforces; the HIPAA Privacy Rule, which protects the privacy of Individually Identifiable Health Information; the HIPAA Security Rule, which sets national standards for the security of electronic Protected Health Information; the HIPAA Breach Notification Rule, which requires Covered Entities and Business Associates to provide notification following a breach of unsecured PHI; and the Enforcement Rule which provides authority and procedures for OCR investigations, imposition of penalties, and administrative hearings.

Output devices: An output device is a piece of computer hardware that receives data from a computer and then translates that data into another form. That form may be audio, visual, textual, or hard copy such as a printed document.

Physical access control: A manual process or automated system that manages the passage of people or assets through an opening in a secure perimeter based on a set of authorization rules.

Physical security: The part of the DSHS security controls concerned with physical measures designed to safeguard people; to prevent unauthorized access to equipment, facilities, material, and documents; and to safeguard them against a security incident.

Public access areas: The spaces at a DSHS location designated as unrestricted to the public and includes such areas as foyers, hallways, and lobbies.

Restricted access areas: DSH areas within its facilities that contain either confidential information, financial instruments, or both, such as, but not limited to server rooms, telecommunication rooms, IT equipment rooms, and storage rooms.

Safeguard: A protective measure prescribed to meet the security requirements (i.e., confidentiality, integrity, and availability) specified for an information system. Safeguards may include security features, management constraints, personnel security, and security of physical structures, areas, and devices. Synonymous with security controls and countermeasures.

Security incident: An occurrence that jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.

Standards: Items that are mandatory and required as part of this document. They typically refer to equipment specification, performance requirements and functional requirements.

Policy

A. DSHS must ensure that Confidential Information and Financial Instruments are physically secure within its Facilities as required by law and applicable regulations, such as:
   - The HIPAA Security Rule: Sets federal standards for the security of electronic Protected Health Information;
   - Internal Revenue Service (IRS) Publication 1075: The Tax Information Security Guideline for Federal, State and Local Agencies;
   - The Social Security Administration (SSA) Electronic Information Exchange System (EIES) Security Requirements and Procedures for State and Local Agencies Exchanging Electronic Information with the Social Security Administration: Requires formal data exchange agreements between the SSA and DSHS;
   - Office of the Chief Information Officer (OCIO) Policy 141.10: The statewide policy for maintaining system and network security, data integrity, and confidentiality at state agencies.
   - The National Institute of Standards and Technology (NIST) Special Publication 800-53 Revision 5, Security and Privacy Controls for Federal Information Systems and Organizations.

B. Each individual facility building management committee or building manager, or their designee(s) must establish, document, implement, and maintain minimum physical security standards to help safeguard confidential information and financial instruments located in DSHS offices and facilities within their area of the responsibility. These physical security standards include:
   1. Physical access authorization;
   2. Physical access control;
   3. Access control for output devices;
   4. Monitoring physical access; and
   5. Maintain physical access audit logs.
   6. Escort visitors and control visitor activity.

C. Each administration's IT staff must establish, implement, document, and maintain minimum physical security standards to safeguard Restricted Access Areas they are responsible for such as server rooms, telecommunication rooms, and IT equipment rooms within DSHS offices and facilities. These physical security standards include:
   1. Physical access authorization;
   2. Physical access control;
   3. Access control for output devices;
   4. Monitoring physical access; and
   5. Maintain physical access audit logs.

D. Assignment of administrative responsibilities

1. Each individual facility building committee or building manager, or their designee(s) must:
   a) Oversee and approve the documentation and implementation of DSHS's minimum Physical Security Standards.
   b) Ensure their Facilities continue to maintain compliance with DSHS's minimum Physical Security Standards.

2. DSHS's Enterprise Technology Division must oversee and approve each DSHS administration's documentation and implementation of minimum physical security standards for restricted access areas that contain information technology assets, such as server rooms, telecommunication rooms, and information technology equipment rooms.

3. All personnel must:
   a) Comply with DSHS's minimum Physical Security Standards as set by their programs;
   b) Protect Confidential Information and Financial Instruments;
   c) Sign DSHS's Nondisclosure of Confidential Information attestation in the Learning Center.

E. Physical access authorizations

Each individual facility building committee, building manager, or their designee(s) must:
1. Develop, approve, and maintain a list of DSHS positions and individuals assigned to them that have authorized access to DSHS offices, facilities and their restricted access areas where confidential information or financial instruments reside;
2. Issue authorization credentials for office, facility and restricted area access;
3. Review the access list (i.e. card-keys) detailing authorized office, facility and restricted area access by DSHS position and the individuals assigned access as needed; and
4. Remove DSHS positions and individuals from the office facility and restricted area access list when access is no longer required.

F. Physical access control

Each individual facility building committee, building manager, or their designee(s) must:
1. Establish and enforce physical access authorizations at entry/exit points to the office, facility and restricted access areas where confidential Information or financial instruments reside by:
   a) Verifying individual access authorizations before granting access to the office, facility, and restricted access areas; and
   b) Controlling ingress/egress to the office, facility and restricted access areas using physical access controls.
2. Maintain physical access logs (i.e. card-keys) for office, facility, and restricted access area entry/exit points in a secure location for the required document retention period;

3. Provide physical security safeguards to control access to officially designated public access areas within offices and facilities;
4. Require visitors to be escorted and their activity monitored while having access to offices, facilities, and their restricted access areas where confidential information or financial instruments reside. If visitor(s) are DSHS employees determine what measures are appropriate to monitor staff while visiting;
5. Provide physical security safeguards to control access to restricted access areas located within the office or facility;
6. Coordinate physical security of the restricted access areas with the information technology staff and co-located business units at the facility and other state entities as needed;
7. Safeguard keys, card-keys, combinations, and other physical access devices;
8. Inventory keys, card-keys, combinations and other physical access devices;
9. Change combinations and keys when keys are lost, combinations are compromised, or individuals are transferred or terminated as soon as is reasonably possible (e.g., the same day);
10. Deactivate card-keys when lost or stolen, or when individuals are transferred or terminated as soon as is reasonably possible (e.g., the same day);
11. Maintain physical security access control during periods of disruption due to any emergency, disaster, or human caused incidents as appropriate.

G. Access control for output devices

Each individual facility building committee, building manager, or their designee(s) must control the physical access to information system output devices to prevent unauthorized individuals from obtaining confidential information and financial instruments.

H. Monitoring Physical Access

Each individual facility building committee, building manager must coordinate the monitoring of physical access to restricted access areas with the information technology staff and co-located business units at the facility and other state entities as needed.

I. Visitor Access Records

Each individual facility building committee or building manager must maintain visitor access records to the office, facility and restricted access areas where confidential information and financial instruments reside for the required document retention period.