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 Policy & External Relations Phone: (360) 902-7804, MS: 45115
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:	New
Approved By:	**Original signed by Dana Phelps** Senior Director, Policy & External Relations

Purpose

This policy establishes the Department of Social and Health Services (DSHS, or Department) minimum Physical Security Standards necessary to safeguard Confidential Information and Financial Instruments located within Department 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 Systems and Organizations* identifies the minimum standards necessary for the Department to appropriately manage the physical security of its Confidential Information and Financial Instruments. The adaptation 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 Department-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 Department locations. Administration leadership must work closely with their staff to assess and analyze those

circumstances that may require heightened security standards and apply them as necessary.

This policy provides links to procedural templates which have been included to assist Department Administrations with creating and implementing a basic framework of minimum Physical Security Standards at their offices and Facilities. These 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 Confidential Information and/or Financial Instruments are stored.

Additional Guidance

For related, useful information see:

- DSHS Information Security Policy Manual:
  - Information Security Policy 3.2.1, *Classify Data According to Level of Protection Needed*
  - Information Security Policy 3.2.2, *General Protection Requirements*
  - Information Security Policy 3.2.3, *Protecting Data in Hard Copy Documents and Removable Media*
  - Information Security Policy 3.2.10, *Work Areas*
  - Information Security Policy 11.21, *Requirements for Safeguarding Confidential Information*
  - Information Security Policy 11.3.1, *IRS Physical Security Requirements*
- 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 and Technology Security*
- OCIO Policy 141.10 , *Securing Information Technology Assets Standards*
- NIST Special Publication 800-53 Revision 4, *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: Means a standing committee formed at each Facility that houses two or more DSHS tenants to coordinate on site facility maintenance and operations. The committee shall 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: Means 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) Policy Section 4.1 requires state agencies to follow the designated classification categories:

Category 1 – Public Information
Public information is information that can be released to the public. It does not need protection from unauthorized disclosure, but does need protection from unauthorized change that may mislead the public or embarrass DSHS.

Category 2 – Sensitive Information
Sensitive information is not specifically protected by law, but should be limited to official use only, and protected against unauthorized access. Computer system documentation that is not classified as Confidential (see below) should be classified as Sensitive.

Category 3 – Confidential Information
Confidential Information is information that is specifically protected by law. It generally includes:

a. Personal information about individual clients, regardless of how that information is obtained;
b. Information concerning employee payroll and personnel records;
c. Source code of certain applications programs that could jeopardize the integrity of department data or result in fraud or unauthorized disclosure of information if unauthorized modification occurred.

Category 4 – Confidential Information Requiring Special Handling
Confidential information requiring special handling is information for which:

a. Especially strict handling requirements are dictated, e.g. by statutes, regulations, or agreements; or
b. Serious consequences could arise from unauthorized disclosure, ranging from life threatening to legal sanctions.
c. Examples of Confidential Information requiring special handling include:
d. Protected Health Information (PHI), as defined in Administrative Policy 5.01 Privacy Policy -- Safeguarding Confidential Information, and by the HIPAA Security Rule;
e. Information that identifies a person as being or ever having been a client of an alcohol or substance abuse treatment, or mental health program;
f. Federal wage data;
g. Location of an abused spouse.

Enterprise Technology Division: Provides agency-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" includes the rules that OCR enforces which include the HIPAA Privacy Rule, which protects the privacy of Individually Identifiable Health Information; the HIPAA Security Rule, which sets federal 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 confidentiality provisions of the Patient Safety Rule, which protect identifiable information being used to analyze patient safety events and improve patient safety.

Output Devices: Equipment which produces information in a usable form such as monitors, printers, copiers, scanners, facsimile machines, tablet computers, cellular phones, cameras and voice recorders are examples of output devices.

Physical Access Control: A manual process, or automated system that manages the passage of people or assets through an opening(s) in a secure perimeter(s) based on a set of authorization rules.

Physical Security: The part of the Department's 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: Department areas within its Facilities that contain Confidential Information and/or Financial Instruments 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.

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

Policy

A. The Department shall 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 the Department;
   - 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.

B. Each individual Facility Building Management Committee and/or Building Manager, or their designee(s) must establish, document and implement and maintain minimum Physical Security Standards to help safeguard Confidential Information and Financial Instruments located in Department 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. Maintaining Visitor Access Records.

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 Department 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. Maintaining Visitor Access Records.

D. Assignment of Administrative Responsibilities

   1. Each individual Facility Building Committee and/or Building Manager, or their designee(s) shall:
      a) Oversee and approve the documentation and implementation of the Department's minimum Physical Security Standards.
      b) Ensure their Facilities continue to maintain compliance with the Department's minimum Physical Security Standards.

2. The Department's Enterprise Technology Division shall oversee and approve each Department Administration's documentation and implementation of the Department's minimum Physical Security Standards for Restricted Access Areas that contain that contain information technology assets, such as server rooms, telecommunication rooms, and information technology equipment rooms.

3. All personnel shall:
   a) Comply with the Department's minimum Physical Security Standards as set by their programs;
   b) Protect Confidential Information and Financial Instruments;
   c) Sign the Department's Nondisclosure of Confidential Information Form.

E. Physical Access Authorizations

Each individual Facility Building Committee and/or Building Manager, or their designee(s) shall:

1. Develop, approve, and maintain a list of Department positions and individuals assigned to them that have authorized access to Department offices, Facilities and their Restricted Access Areas where Confidential Information and/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 Department position and the individuals assigned access as needed;
4. Remove Department positions and/or 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 and/or Building Manager, or their designee(s) shall:

1. Establish and enforce physical access authorizations at entry/exit points to the office, Facility and Restricted Access Areas where Confidential Information and/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 and/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; and
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, 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 and/or Building Manager, or their designee(s) shall:
Control the physical access to information System Output Devices in order to prevent unauthorized individuals from obtaining Confidential Information and/or Financial Instruments.

H. Monitoring Physical Access

Each individual Facility Building Committee and/or Building Manager shall:

1. 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 and/or Building Manager shall:

1. Maintain visitor access records to the office, Facility and Restricted Access Areas where Confidential Information and/or Financial Instruments reside for the required document retention period.