Attachment 1

# Department of the Interior

# Security Control Standard

## Physical and Environmental Protection

**April 2011**

Version: 1.1

# Signature Approval Page

| Designated Official | |
|---|---|
| Bernard J. Mazer, Department of the Interior, Chief Information Officer | |
| **Signature:** | **Date:** |

# REVISION HISTORY

| Author | Version | Revision Date | Revision Summary |
|---|---|---|---|
| Chris Peterson | 0.1 | January 21, 2011 | Initial draft |
| Timothy Brown | 0.2 | January 25, 2011 | Incorporated comments into body text |
| Timothy Brown | 0.21 | February 15, 2011 | Checked/added cloud moderate to high |
| Timothy Brown | 1.0 | February 17, 2011 | Final review and version change to 1.0 |
| Lawrence K. Ruffin | 1.1 | April 29, 2011 | Final revisions and version change to 1.1 |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

# TABLE OF CONTENTS

**REVISION HISTORY** ..... **3**

**TABLE OF CONTENTS** ..... **4**

**SECURITY CONTROL STANDARD: PHYSICAL AND ENVIRONMENTAL PROTECTION** ..... **5**

PE-1 PHYSICAL AND ENVIRONMENTAL POLICY AND PROCEDURES ..... 5
PE-2 PHYSICAL ACCESS AUTHORIZATIONS ..... 6
PE-3 PHYSICAL ACCESS CONTROL ..... 7
PE-4 ACCESS CONTROL FOR TRANSMISSION MEDIUM ..... 8
PE-5 ACCESS CONTROL FOR OUTPUT DEVICES ..... 8
PE-6 MONITORING PHYSICAL ACCESS ..... 9
PE-7 VISITOR CONTROL ..... 9
PE-8 ACCESS RECORDS ..... 10
PE-9 POWER EQUIPMENT AND POWER CABLING ..... 10
PE-10 EMERGENCY SHUTOFF ..... 10
PE-11 EMERGENCY POWER ..... 11
PE-12 EMERGENCY LIGHTING ..... 12
PE-13 FIRE PROTECTION ..... 12
PE-14 TEMPERATURE AND HUMIDITY CONTROLS ..... 13
PE-15 WATER DAMAGE PROTECTION ..... 13
PE-16 DELIVERY AND REMOVAL ..... 14
PE-17 ALTERNATE WORK SITE ..... 14
PE-18 LOCATION OF INFORMATION SYSTEM COMPONENTS ..... 15

# SECURITY CONTROL STANDARD: PHYSICAL AND ENVIRONMENTAL PROTECTION

The National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 describes the required process for selecting and specifying security controls for an information system based on its security categorizing, including tailoring the initial set of baseline security controls and supplementing the tailored baseline as necessary based on an organizational assessment of risk.

This standard specifies organization-defined parameters that are deemed necessary or appropriate to achieve a consistent security posture across the Department of the Interior. In addition to the NIST SP 800-53 Physical and Environmental Protection (PE) control family standard, supplemental information is included that establishes an enterprise-wide standard for specific controls within the control family. In some cases additional agency-specific or Office of Management and Budget (OMB) requirements have been incorporated into relevant controls. Where the NIST SP 800-53 indicates the need for organization-defined parameters or selection of operations that are not specified in this supplemental standard, the System Owner shall appropriately define and document the parameters based on the individual requirements, purpose, and function of the information system. The supplemental information provided in this standard is required to be applied when the Authorizing Official (AO) has selected the control, or control enhancement, in a manner that is consistent with the Department's IT security policy and associated information security Risk Management Framework (RMF) strategy.

Additionally, information systems implemented within cloud computing environments shall select, implement, and comply with any additional and/or more stringent security control requirements as specified and approved by the Federal Risk and Authorization Management Program (FedRAMP) unless otherwise approved for risk acceptance by the AO. The additional controls required for implementation within cloud computing environments are readily identified within the Priority and Baseline Allocation table following each control and distinguished by the control or control enhancement represented in **bold red text**.

## *PE-1 PHYSICAL AND ENVIRONMENTAL POLICY AND PROCEDURES*

Applicability: Bureaus and Offices

Control: The organization develops, disseminates, and reviews/updates at least annually:

a. A formal, documented physical and environmental protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
b. Formal, documented procedures to facilitate the implementation of the physical and environmental protection policy and associated physical and environmental protection controls.

Supplemental Guidance: This control is intended to produce the policy and procedures that are required for the effective implementation of selected security controls and control enhancements in the physical and environmental protection family. The policy and procedures are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Existing organizational policies and procedures may make the need for additional specific policies and procedures unnecessary. The physical and environmental protection policy can be included as part of the general information

security policy for the organization. Physical and environmental protection procedures can be developed for the security program in general and for a particular information system, when required. The organizational risk management strategy is a key factor in the development of the physical and environmental protection policy. Related control: PM-9.

Control Enhancements: None.

References: NIST Special Publications 800-12, 800-100.

Priority and Baseline Allocation:

| | | | |
|---|---|---|---|
| **P1** | **LOW** PE-1 | **MOD** PE-1 | **HIGH** PE-1 |

## *PE-2 PHYSICAL ACCESS AUTHORIZATIONS*

Applicability: All Information Systems

Control: The organization:

a. Develops and keeps current a list of personnel with authorized access to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible);
b. Issues authorization credentials;
c. Reviews and approves the access list and authorization credentials at least annually, removing from the access list personnel no longer requiring access.

Supplemental Guidance: Authorization credentials include, for example, badges, identification cards, and smart cards. Related control: PE-3, PE-4.

Control Enhancements:

1. The organization authorizes physical access to the facility where the information system resides based on position or role.

References: None.

Priority and Baseline Allocation:

| | | | |
|---|---|---|---|
| **P1** | **LOW** PE-2 | **MOD** PE-2 | **HIGH** PE-2 **(1)** |

## *PE-3 PHYSICAL ACCESS CONTROL*

Applicability: All Information Systems

Control: The organization:

a. Enforces physical access authorizations for all physical access points (including designated entry/exit points) to the facility where the information system resides (excluding those areas within the facility officially designated as publicly accessible);
b. Verifies individual access authorizations before granting access to the facility;
c. Controls entry to the facility containing the information system using physical access devices and/or guards;
d. Controls access to areas officially designated as publicly accessible in accordance with the organization's assessment of risk;
e. Secures keys, combinations, and other physical access devices;
f. Inventories physical access devices at least annually; and
g. Changes combinations and keys at least annually and when keys are lost, combinations are compromised, or individuals are transferred or terminated.

Supplemental Guidance: The organization determines the types of guards needed, for example, professional physical security staff or other personnel such as administrative staff or information system users, as deemed appropriate. Physical access devices include, for example, keys, locks, combinations, and card readers. Workstations and associated peripherals connected to (and part of) an organizational information system may be located in areas designated as publicly accessible with access to such devices being safeguarded. Related controls: MP-2, MP-4, PE-2.

Control Enhancements:

1. The organization enforces physical access authorizations to the information system independent of the physical access controls for the facility.

   Enhancement Supplemental Guidance: This control enhancement applies to server rooms, media storage areas, communications centers, or any other areas within an organizational facility containing large concentrations of information system components. The intent is to provide additional physical security for those areas where the organization may be more vulnerable due to the concentration of information system components. Security requirements for facilities containing organizational information systems that process, store, or transmit Sensitive Compartmented Information (SCI) are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. See also PS-3, security requirements for personnel access to SCI.

References: FIPS Publication 201; NIST Special Publications 800-73, 800-76, 800-78; ICD 704; DCID 6/9.

Priority and Baseline Allocation:

| | | | |
|---|---|---|---|
| **P1** | **LOW** PE-3 | **MOD** PE-3 | **HIGH** PE-3(1) |

## *PE-4 ACCESS CONTROL FOR TRANSMISSION MEDIUM*

Applicability: Moderate and High Impact Information Systems

Control: The organization controls physical access to information system distribution and transmission lines within organizational facilities.

Supplemental Guidance: Physical protections applied to information system distribution and transmission lines help prevent accidental damage, disruption, and physical tampering. Additionally, physical protections are necessary to help prevent eavesdropping or in transit modification of unencrypted transmissions. Protective measures to control physical access to information system distribution and transmission lines include: (i) locked wiring closets; (ii) disconnected or locked spare jacks; and/or (iii) protection of cabling by conduit or cable trays. Related control: PE-2.

Control Enhancements: None.

References: NSTISSI No. 7003.

Priority and Baseline Allocation:

| | | | |
|---|---|---|---|
| **P1** | **LOW** Not Selected | **MOD** PE-4 | **HIGH** PE-4 |

## *PE-5 ACCESS CONTROL FOR OUTPUT DEVICES*

Applicability: Moderate and High Impact Information Systems

Control: The organization controls physical access to information system output devices to prevent unauthorized individuals from obtaining the output.

Supplemental Guidance: Monitors, printers, and audio devices are examples of information system output devices.

Control Enhancements: None.

References: None.

Priority and Baseline Allocation:

| | | | |
|---|---|---|---|
| **P1** | **LOW** Not Selected | **MOD** PE-5 | **HIGH** PE-5 |

## *PE-6 MONITORING PHYSICAL ACCESS*

Applicability: All Information Systems

Control: The organization:

a. Monitors physical access to the information system to detect and respond to physical security incidents;
b. Reviews physical access logs at least semi-annually; and
c. Coordinates results of reviews and investigations with the organization's incident response capability.

Supplemental Guidance: Investigation of and response to detected physical security incidents, including apparent security violations or suspicious physical access activities, are part of the organization's incident response capability.

Control Enhancements:

1. The organization monitors real-time physical intrusion alarms and surveillance equipment.
2. The organization employs automated mechanisms to recognize potential intrusions and initiate designated response actions.

References: None.

Priority and Baseline Allocation:

| | | | |
|---|---|---|---|
| **P1** | **LOW** PE-6 | **MOD** PE-6 (1) | **HIGH** PE-6 (1) (2) |

## *PE-7 VISITOR CONTROL*

Applicability: All Information Systems

Control: The organization controls physical access to the information system by authenticating visitors before authorizing access to the facility where the information system resides other than areas designated as publicly accessible.

Supplemental Guidance: Individuals (to include organizational employees, contract personnel, and others) with permanent authorization credentials for the facility are not considered visitors.

Control Enhancements:

1. The organization escorts visitors and monitors visitor activity, when required.

References: None.

Priority and Baseline Allocation:

| | | | |
|---|---|---|---|
| **P1** | **LOW** PE-7 | **MOD** PE-7 (1) | **HIGH** PE-7 (1) |

## *PE-8 ACCESS RECORDS*

Applicability: All Information Systems

Control: The organization:

a. Maintains visitor access records to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible); and
b. Reviews visitor access records at least monthly.

Supplemental Guidance: Visitor access records include, for example, name/organization of the person visiting, signature of the visitor, form(s) of identification, date of access, time of entry and departure, purpose of visit, and name/organization of person visited.

Control Enhancements:

1. The organization employs automated mechanisms to facilitate the maintenance and review of access records.
2. The organization maintains a record of all physical access, both visitor and authorized individuals.

References: None.

Priority and Baseline Allocation:

| | | | |
|---|---|---|---|
| **P1** | **LOW** PE-8 | **MOD** PE-8 | **HIGH** PE-8 (1) (2) |

## *PE-9 POWER EQUIPMENT AND POWER CABLING*

Applicability: Moderate and High Impact Information Systems

Control: The organization protects power equipment and power cabling for the information system from damage and destruction.

Supplemental Guidance: This control, to include any enhancements specified, may be satisfied by similar requirements fulfilled by another organizational entity other than the information security program. Organizations avoid duplicating actions already covered.

Control Enhancements: None mandated.

References: None.

Priority and Baseline Allocation:

| | | | |
|---|---|---|---|
| **P1** | **LOW** Not Selected | **MOD** PE-9 | **HIGH** PE-9 |

## *PE-10 EMERGENCY SHUTOFF*

Applicability: Moderate and High Impact Information Systems

Control: The organization:

*a.* Provides the capability of shutting off power to the information system or individual system components in emergency situations;
b. Places emergency shutoff switches or devices in [*Assignment: organization-defined location by information system or system component*] to facilitate safe and easy access for personnel; and
c. Protects emergency power shutoff capability from unauthorized activation.

Supplemental Guidance: This control applies to facilities containing concentrations of information system resources, for example, data centers, server rooms, and mainframe computer rooms.

Control Enhancements: None

References: None.

Priority and Baseline Allocation:

| | | | |
|---|---|---|---|
| **P1** | **LOW** Not Selected | **MOD** PE-10 | **HIGH** PE-10 |

## *PE-11 EMERGENCY POWER*

Applicability: Moderate and High Impact Information Systems

Control: The organization provides a short-term uninterruptible power supply to facilitate an orderly shutdown of the information system in the event of a primary power source loss.

Supplemental Guidance: This control, to include any enhancements specified, may be satisfied by similar requirements fulfilled by another organizational entity other than the information security program. Organizations avoid duplicating actions already covered.

Control Enhancements:

1. The organization provides a long-term alternate power supply for the information system that is capable of maintaining minimally required operational capability in the event of an extended loss of the primary power source.

Enhancement Supplemental Guidance: Long-term alternate power supplies for the information system are either manually or automatically activated.

References: None.

Priority and Baseline Allocation:

| | | | |
|---|---|---|---|
| **P1** | **LOW** Not Selected | **MOD** PE-11 | **HIGH** PE-11 (1) |

## *PE-12 EMERGENCY LIGHTING*

Applicability: All Information Systems

Control: The organization employs and maintains automatic emergency lighting for the information system that activates in the event of a power outage or disruption and that covers emergency exits and evacuation routes within the facility.

Supplemental Guidance: This control, to include any enhancements specified, may be satisfied by similar requirements fulfilled by another organizational entity other than the information security program. Organizations avoid duplicating actions already covered.

Control Enhancements: None Mandated.

References: None.

Priority and Baseline Allocation:

| | | | |
|---|---|---|---|
| **P1** | **LOW** PE-12 | **MOD** PE-12 | **HIGH** PE-12 |

## *PE-13 FIRE PROTECTION*

Applicability: All Information Systems

Control: The organization employs and maintains fire suppression and detection devices/systems for the information system that are supported by an independent energy source.

Supplemental Guidance: Fire suppression and detection devices/systems include, for example, sprinkler systems, handheld fire extinguishers, fixed fire hoses, and smoke detectors. This control, to include any enhancements specified, may be satisfied by similar requirements fulfilled by another organizational entity other than the information security program. Organizations avoid duplicating actions already covered.

Control Enhancements:

1. The organization employs fire detection devices/systems for the information system that activate automatically and notify the organization and emergency responders in the event of a fire.
2. The organization employs fire suppression devices/systems for the information system that provide automatic notification of any activation to the organization and emergency responders.
3. The organization employs an automatic fire suppression capability for the information system when the facility is not staffed on a continuous basis.

References: None.

Priority and Baseline Allocation:

| | | | |
|---|---|---|---|
| **P1** | **LOW** PE-13 | **MOD** PE-13 (1) (2) (3) | **HIGH** PE-13 (1) (2) (3) |

## *PE-14 TEMPERATURE AND HUMIDITY CONTROLS*

Applicability: All Information Systems

Control: The organization:

a. Maintains temperature and humidity levels within the facility where the information system resides at consistent with American Society of Heating, Refrigerating and Air-conditioning Engineers (ASHRAE) document entitled *Thermal Guidelines for Data Processing Environments*; and
b. Monitors temperature and humidity levels continuously.

Supplemental Guidance: This control, to include any enhancements specified, may be satisfied by similar requirements fulfilled by another organizational entity other than the information security program. Organizations avoid duplicating actions already covered.

Control Enhancements:

1. The organization employs automatic temperature and humidity controls in the facility to prevent fluctuations potentially harmful to the information system.

References: None.

Priority and Baseline Allocation:

| | | | |
|---|---|---|---|
| **P1** | **LOW** PE-14 | **MOD** PE-14 | **HIGH** PE-14 **(1)** |

## *PE-15 WATER DAMAGE PROTECTION*

Applicability: All Information Systems

Control: The organization protects the information system from damage resulting from water leakage by providing master shutoff valves that are accessible, working properly, and known to key personnel.

Supplemental Guidance: This control, to include any enhancements specified, may be satisfied by similar requirements fulfilled by another organizational entity other than the information security program. Organizations avoid duplicating actions already covered.

Control Enhancements:

1. The organization employs mechanisms that, without the need for manual intervention, protect the information system from water damage in the event of a water leak.

References: None.

Priority and Baseline Allocation:

| | | | |
|---|---|---|---|
| **P1** | **LOW** PE-15 | **MOD** PE-15 | **HIGH** PE-15 (1) |

## *PE-16 DELIVERY AND REMOVAL*

Applicability: All Information Systems

Control: The organization authorizes, monitors, and controls all information system components entering and exiting the facility and maintains records of those items.

Supplemental Guidance: Effectively enforcing authorizations for entry and exit of information system components may require restricting access to delivery areas and possibly isolating the areas from the information system and media libraries.

Control Enhancements: None.

References: None.

Priority and Baseline Allocation:

| | | | |
|---|---|---|---|
| **P1** | **LOW** PE-16 | **MOD** PE-16 | **HIGH** PE-16 |

## *PE-17 ALTERNATE WORK SITE*

Applicability: Moderate and High Impact Information Systems

Control: The organization:

a. Employs appropriate management, operational, and technical information system security controls at alternate work sites in accordance with the DOI Telework Policy at alternate work sites;
b. Assesses as feasible, the effectiveness of security controls at alternate work sites; and
c. Provides a means for employees to communicate with information security personnel in case of security incidents or problems.

Supplemental Guidance: Alternate work sites may include, for example, government facilities or private residences of employees. The organization may define different sets of security controls for specific alternate work sites or types of sites.

Control Enhancements: None.

References: NIST Special Publication 800-46.

Priority and Baseline Allocation:

| | | | |
|---|---|---|---|
| **P1** | **LOW** Not Selected | **MOD** PE-17 | **HIGH** PE-17 |

## *PE-18 LOCATION OF INFORMATION SYSTEM COMPONENTS*

Applicability: Moderate and High Impact Information Systems

Control: The organization positions information system components within the facility to minimize potential damage from physical and environmental hazards and to minimize the opportunity for unauthorized access.

Supplemental Guidance: Physical and environmental hazards include, for example, flooding, fire, tornados, earthquakes, hurricanes, acts of terrorism, vandalism, electromagnetic pulse, electrical interference, and electromagnetic radiation. Whenever possible, the organization also considers the location or site of the facility with regard to physical and environmental hazards. In addition, the organization considers the location of physical entry points where unauthorized individuals, while not being granted access, might nonetheless be in close proximity to the information system and therefore, increase the potential for unauthorized access to organizational communications (e.g., through the use of wireless sniffers or microphones). This control, to include any enhancements specified, may be satisfied by similar requirements fulfilled by another organizational entity other than the information security program. Organizations avoid duplicating actions already covered.

Control Enhancements:

1. The organization plans the location or site of the facility where the information system resides with regard to physical and environmental hazards and for existing facilities, considers the physical and environmental hazards in its risk mitigation strategy.

References: None.

Priority and Baseline Allocation:

| | | | |
|---|---|---|---|
| **P1** | **LOW** Not Selected | **MOD** PE-18 | **HIGH** PE-18 (1) |