**PHYSICAL AND ENVIRONMENTAL (PE)**

**PE-1: Physical and Environmental Protection Policy and Procedures**

NIST SP 800-53 Objective: The organization develops, disseminates, and reviews/updates [*Assignment: organization defined frequency]:*

a. A formal, documented security awareness and training 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 environmental protection policy and associated physical and environmental protection controls.

Control Translation: Ensure physical and environmental policy and procedures are in place.

Notes: The organizational risk management strategy is a key factor in the development of the physical and environmental policy. Related control: PM-9. This control can be applied at the General level.

How to test and evaluate: Examine SSP and Physical and Environmental Policy (if available). Verify that the policy and procedures are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance of organization/agency.

Technology specific: General

**PE-2: Physical Access Authorizations**

NIST SP 800-53 Objective: 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 [Assignment: organization-defined frequency], removing from the access list personnel no longer requiring access.

Control Translation: Ensure organization documents current list of authorized users who have physical access to the designated area and that list is reviewed according to the defined frequency.

Notes: Role based access can be a solution to this requirement. Authorization credentials include, for example badges, identification cards, and smart cards. Related controls: PE-3, PE-4.

How to test and evaluate: Examine SSP, Physical and Environmental Policy, and other applicable documents (if available) to ensure that organization documents current physical access list of authorized personnel and that list is reviewed according to the defined frequency. Collect evidence either by screenshot or hard/soft copies of documents demonstrating how authorization credentials are issued (e.g., ticket request, email, etc.) and process of approval and removal of personnel from physical access list.

Technology specific: Per datacenter

**PE-3: Physical Access Control**

NIST SP 800-53 Objective: 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;

1. Controls access to areas officially designated as publicly accessible in accordance with the organization's assessment of risk;
2. Secures keys, combinations, and other physical access devices;
3. Inventories physical access devices [Assignment: organization-defined frequency]; and
4. Changes combinations and keys [Assignment: organization-defined frequency] and when keys are lost, combinations are compromised, or individuals are transferred or terminated.

Control Translation: Ensure organization documents and implements physical access controls at facility where information system resides. Access controls include, but are not limited to, guards, physical security staff, keys, locks, combinations, and card readers.

Notes: Role based access can be a solution to this requirement. Authorization credentials include, for example badges, identification cards, and smart cards. Related controls: CA-2, MP-2, MP-4, PE-2.

How to test and evaluate: Examine SSP, Physical and Environmental Policy, and other applicable documents (if available) to ensure that organization documents physical access controls currently in place and that controls are implemented. Collect evidence either by screenshot or hard/soft copies of documents demonstrating how authorization credentials are issued (e.g., ticket request, email, etc.) and process of approval and removal of personnel from physical access list. Document type of physical access devices, model number, and how often these devices are changed or updated, for example, keys, locks, combinations, and card readers. Document how often physical access devices are inventoried.

Technology specific: Per datacenter

**PE-4: Access Control for Transmission Medium**

NIST SP 800-53 Objective: The organization controls physical access to information system distribution and transmission lines within organizational facilities.

Control Translation: Ensure organization document and implement controls for physical access to information system distribution and transmission lines within organizational facilities to help prevent accidental damage, disruption, and physical tampering.

Notes: Role based access can be a solution to this requirement. Authorization credentials to access physical access to information distribution and transmission lines can be through badges, identification cards, and smart cards. Related controls: PE-2.

How to test and evaluate: Examine SSP, Physical and Environmental Policy, and other applicable documents (if available) to ensure that organization documents physical access controls to information system distribution and transmission lines. Interview and collect evidence as to who has authorization credentials to information system distribution and transmission lines. Examine, observe, and document protective measures to control physical access to the information system distribution and transmission lines to ensure the following: wiring closets are locked, spare jacks are disconnected or locked, cables are protected by conduit or cable trays.

Technology specific: Per datacenter

**PE-5: Access Control for Output Devices**

NIST SP 800-53 Objective: The organization controls physical access to information system output devices to prevent unauthorized individuals from obtaining the output.

Control Translation: Ensure organization document and implement controls for physical access to information system output devices to prevent unauthorized individuals from obtaining the output.

Notes: N/A.

How to test and evaluate: Examine SSP, Physical and Environmental Policy, and other applicable documents (if available) to ensure that organization documents physical access controls to information system output devices to prevent unauthorized individuals from obtaining the output. Examine, observe, and document protective measures in place to control unauthorized access to devices, but are not limited to, monitors, printers, and audio devices.

Technology specific: Per datacenter

**PE-6: Monitoring Physical Access**

NIST SP 800-53 Objective: The organization:

1. Monitors physical access to information system to detect and respond to physical security incidents;
2. Reviews physical access logs [Assignment: organization-defined frequency]; and
3. Coordinates results of reviews and investigations with the organization's incident response capability.

Control Translation: Ensure organization document and implement capabilities for monitoring, investigating, and detecting physical access to information system. Reviews of physical access logs is defined and organization’s incident response capability is in place.

Notes: N/A.

How to test and evaluate: Examine SSP, Physical and Environmental Policy, and other applicable documents (if available) to ensure that organization documents monitoring of physical access controls to information system. Examine, observe, and document protective measures in place and whether monitoring is conducted in real-time. Note what physical intrusion alarms or surveillance equipment is in place. Interview personnel responsible for incident response when potential intrusions take place. Note process of incident response capability.

Technology specific: Per datacenter

**PE-7: Visitor Control**

NIST SP 800-53 Objective: The organization controls physical access to information system by authenticating visitors before authorizing access to the facility where the information system resides other than areas designated as publicly accessible.

Control Translation: Ensure organization controls physical access to include organizational personnel, contract personnel, vendors, and other visitors. Individuals must be authenticated before authorizing access.

Notes: N/A.

How to test and evaluate: Examine SSP, Physical and Environmental Policy, and other applicable documents (if available) to ensure that organization documents physical access to facility. Interview, examine, and observe if visitors are required to sign-in and what is the sign-in process (i.e., forms if ID required for visitor access to facility, etc.). Note if visitors are escorted at all times and what is the visitor authentication process.

Technology specific: Per datacenter

**PE-8: Access Records**

NIST SP 800-53 Objective: The organization:

1. Maintains visitor access records to facility where the information system resides (except for those areas within the facility officially designated as publicly accessible); and
2. Reviews visitor access records [Assignment: organization-defined frequency].

Control Translation: Ensure organization controls physical access and maintains visitor access records to the facility where information system resides.

Notes: N/A.

How to test and evaluate: Examine SSP, Physical and Environmental Policy, and other applicable documents (if available) to ensure that organization documents physical access records to facility. Interview and examine visitor access records, how often are visitor access records reviewed, and how long they are retained for. Visitor access records should include, name/organization of visitor, signature of visitor, form(s) of identification, date of access, time of entry and departure, purpose of visit, name of person visiting, and name of escort.

Technology specific: Per datacenter

**PE-9: Power Equipment and Power Cabling**

NIST SP 800-53 Objective: The organization protects power equipment and power cabling for the information system from damage and destruction.

Control Translation: Ensure organization controls the protection of power equipment and power cabling for the information system from damage and destruction.

Notes: N/A.

How to test and evaluate: Examine SSP, Physical and Environmental Policy, and other applicable documents (if available) to ensure that organization protects power equipment and cabling from damage and destruction. Interview personnel and note if redundant or parallel cabling paths are in place. Have personnel provide evidence that power equipment and power cabling for the information system is protected from damage and destruction.

Technology specific: Per datacenter

**PE-10: Emergency Shutoff**

NIST SP 800-53 Objective: The organization:

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

Control Translation: Examine if organization provides the capability of emergency power shutoff to information system.

Notes: Control enhancements are withdrawn and incorporated into PE-10.

How to test and evaluate: Examine SSP, Physical and Environmental Policy, and other applicable documents (if available) to ensure that organization documents whether emergency power shutoff capability is in place. Examine and interview personnel to confirm whether emergency power shutoff is active and connected to information system. Observe where emergency power shutoff is located and if cover is in place to protect it from unauthorized or accidental activation.

Technology specific: Per datacenter

**PE-11: Emergency Power**

NIST SP 800-53 Objective: 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.

Control Translation: Examine if organization provides UPS for short-term power supply or generator for long-term power source.

Notes: Control enhancements are withdrawn and incorporated into PE-10.

How to test and evaluate: Examine SSP, Physical and Environmental Policy, and other applicable documents (if available) to ensure that organization documents whether short-term or long-term power supply are in place. Interview personnel and ask to provide evidence that a short-term uninterruptible power supply (UPS) is in place to facilitate an orderly shutdown of the information system in the event of a primary power source loss. Collect evidence such as UPS maintenance logs, contract of UPS maintenance, and etc. Also, verify whether a long-term alternate power supply (Generator) is in place 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. Collect evidence such as generator maintenance logs, contract of generator maintenance, and etc.

Technology specific: Per datacenter

**PE-12: Emergency Lighting**

NIST SP 800-53 Objective: The organization employs and maintains automatic emergency lighting for information system that activates in the event of a power outage or disruption and that covers emergency exits and evacuation routes within the facility.

Control Translation: Examine if organization employs automatic emergency lighting for information system.

Notes: N/A.

How to test and evaluate: Examine SSP, Physical and Environmental Policy, and other applicable documents (if available) to ensure that organization documents whether emergency lighting is in place where information system resides. Interview personnel and observe emergency lighting for all areas within the facility supporting essential missions and business functions for information system. Request for fire marshal reports or other facility reports to ensure emergency lighting is tested periodically.

Technology specific: Per datacenter

**PE-13: Fire Protection**

NIST SP 800-53 Objective: The organization employs and maintains fire suppression and detection devices/systems for the information system that are supported by an independent energy source.

Control Translation: Examine if organization employs and maintains fire suppression and detection devices/systems for the information system.

Notes: N/A.

How to test and evaluate: Examine SSP, Physical and Environmental Policy, and other applicable documents (if available) to ensure that organization documents if they employ and maintain a fire suppression and detection devices/systems for information system. Interview personnel and observe fire suppression and detection devices/systems. Verify if fire suppression and detection devices/systems activate automatically and provide automatic notification to organization and emergency responders in the event of a fire. Verify if organization employs automatic fire suppression if staff is not at faculty on a continuous basis. Collect evidence such as fire marshal inspection reports to ensure it is checked and maintained periodically.

Technology specific: Per datacenter

**PE-14: Temperature and Humidity Controls**

NIST SP 800-53 Objective: The organization:

1. Maintains temperature and humidity levels within the facility where the information system resides at [Assignment: organization-defined acceptable levels]; and
2. Monitors temperature and humidity levels [Assignment; organization-defined frequency].

Control Translation: Examine if organization employs and maintains temperature and humidity controls where information system resides.

Notes: N/A.

How to test and evaluate: Examine SSP, Physical and Environmental Policy, and other applicable documents (if available) to ensure that organization documents if they employ and maintain temperature and humidity controls where information system resides. Observe to ensure acceptable temperature and humidity settings/levels are set within the facility where the information system resides. Collect evidence that temperature and humidity levels are maintained within the defined acceptable settings/levels. Interview personnel and verify how frequently temperature and humidity levels are monitored and if it is conducted within the defined frequency.

Technology specific: Per datacenter

**PE-15: Water Damage Protection**

NIST SP 800-53 Objective: 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.

Control Translation: Examine if organization employs and maintains master shutoff valves that are accessible, working properly, and known to key personnel.

Notes: N/A.

How to test and evaluate: Examine SSP, Physical and Environmental Policy, and other applicable documents (if available) to ensure that organization documents if they employ and maintain master shutoff valves that are accessible, working properly, and known to key personnel. Observe to ensure that master shutoff valves are accessible and working properly to protect the information system from damage resulting from water leakage. Ask personnel to provide list of key personnel with knowledge of the master water shutoff valves (e.g., part of training agreement, etc.). Collect evidence of what is being used without the need for manual intervention, to protect the information system from water damage in the event of a water leak.

Technology specific: Per datacenter

**PE-16: Delivery and Removal**

NIST SP 800-53 Objective: The organization authorizes, monitors, and controls [Assignment: organization-defined types of information system components] entering and exiting the facility and maintains records of those items.

Control Translation: Ensure that organization authorizes, monitors, and controls all components and devices entering and exiting the facility and that records of these activities are maintained.

Notes: N/A.

How to test and evaluate: Examine SSP, Physical and Environmental Policy, and other applicable documents (if available) to ensure that organization authorizes, monitors, and controls all components and devices entering and exiting the facility and that records of these activities are maintained. Ask personnel to provide evidence of what types of information system components to be authorized, monitored, and controlled when entering or exiting the facility (e.g., list of authorized equipment to leave or enter facility, for maintenance, etc.). Collect evidence of process for these components to be authorized, monitored, and controlled when entering and exiting the facility. Verify that records of information system components entering and exiting the facility are maintained.

Technology specific: Per datacenter

**PE-17: Alternate Work Site**

NIST SP 800-53 Objective: The organization:

1. Employs [Assignment: organization-defined management, operational, and technical information system security controls] at alternative work sites;
2. Assesses as feasible, the effectiveness of security controls at alternate work sites; and
3. Provides a means for employees to communicate with information security personnel in case of security incidents or problems.

Control Translation: Ensure that organization has alternate work site(s) in place and that physical access security controls are in place at alternate site.

Notes: N/A.

How to test and evaluate: Examine SSP, Physical and Environmental Policy, and other applicable documents (if available) to ensure that organization employs alternate work site. Interview personnel and note where alternate work site is located. Verify what type of security controls are in place at alternate work site. Verify if it is a hot, warm, or cold site.

Technology specific: Per datacenter

**PE-18: Location of Information System Components**

NIST SP 800-53 Objective: 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.

Control Translation: Ensure that organization positions equipment, devices, and components to minimize potential damage from physical environmental hazards and from unauthorized access.

Notes: N/A.

How to test and evaluate: Examine SSP, Physical and Environmental Policy, and other applicable documents (if available) to ensure that organization positions equipment, devices, and components to minimize potential damage from physical environmental hazards and from unauthorized access. Observe and note how information system components within the facility are placed and if they are positioned in areas to minimize potential damage from physical and environmental hazards and from unauthorized access.

Technology specific: Per datacenter