For High-Impact Information Systems

FAMILY: PHYSICAL AND ENVIRONMENTAL PROTECTION **CLASS:** OPERATIONAL

PE-1 PHYSICAL AND ENVIRONMENTAL PROTECTION POLICY AND PROCEDURES - The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, physical and environmental protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the physical and environmental protection policy and associated physical and environmental protection controls.

PE-1.1 - Examine physical and environmental protection policy and procedures; other relevant documents or records, **and**

Interview organizational personnel with physical and environmental protection responsibilities to determine if the following requirements are met to determine if the following requirements are met:

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	The organization develops and documents physical and environmental protection policy and procedures.				
(ii)	The organization disseminates physical and environmental protection policy and procedures to appropriate elements within the organization.				
(iii)	Responsible parties within the organization periodically review physical and environmental protection policy and procedures.				
(iv)	The organization updates physical and environmental protection policy and procedures when organizational review indicates updates are required.				

PE-1.2- Examine physical and environmental protection policy and procedures; other relevant documents or records, **and**

Interview organizational personnel with physical and environmental protection responsibilities to determine if the following requirements are met:

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	The physical and environmental protection policy addresses purpose,				

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
	scope, roles and responsibilities, management commitment, coordination among organizational entities, and compliance.				
(ii)	The physical and environmental protection policy is consistent with the organization's mission and functions and with applicable laws, directives, policies, regulations, standards, and guidance.				
(iii)	The physical and environmental protection procedures address all areas identified in the physical and environmental protection policy and address achieving policy-compliant implementations of all associated security controls.				

PE-2 PHYSICAL ACCESS AUTHORIZATIONS - The organization 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) and issues appropriate authorization credentials. Designated officials within the organization review and approve the access list and authorization credentials [Assignment: organization-defined frequency, at least annually].

PE-2.1 - Examine physical and environmental protection policy; procedures addressing physical access authorizations; authorized personnel access list; authorization credentials; other relevant documents or records to determine if the following requirements are met:

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	The organization identifies areas within the facility that are publicly accessible.				
(ii)	The organization defines the frequency of review and approval for the physical access list and authorization credentials for the facility.				
(iii)	The organization develops and keeps current lists 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).				
(iv)	The organization issues appropriate authorization credentials (e.g., badges, identification cards, smart cards) .				
(v)	Designated officials within the organization review and approve the access list and authorization credentials at the organization-defined				

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
	frequency, at least annually.				

PE-3 PHYSICAL ACCESS CONTROL - The organization controls all physical access points (including designated entry/exit points) to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible) and verifies individual access authorizations before granting access to the facility. The organization controls access to areas officially designated as publicly accessible, as appropriate, in accordance with the organization's assessment of risk.

PE-3.1- Examine physical and environmental protection policy; procedures addressing physical access control; physical access control logs or records; other relevant documents or records to determine if the following requirements are met:

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	The organization controls all physical access points (including designated entry/exit points) to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible).				
(ii)	The organization verifies individual access authorizations before granting access to the facility.				
(iii)	The organization also controls access to areas officially designated as publicly accessible, as appropriate, in accordance with the organization's assessment of risk.				

and

Test physical access control capability to determine if the following requirements are met:

Test Steps		S	N	Findings	Initials & Date
1	With prior approval, ensure that the organization controls all physical access points and verify that individual access is authorized before granting access to the facility.				

PE-3.2 - Examine physical and environmental protection policy; procedures addressing physical access control; physical access control logs or records; maintenance records; records of key and lock combination changes; storage locations for keys and access devices; other relevant documents or records to determine if the following requirements are met:

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	Physical access devices (e.g., keys, locks, card readers) used at the facility are functioning properly and maintenance on these devices occurs on a regular and scheduled basis.				
(ii)	The organization secures keys, combinations and other access devices on a regular basis.				
(iii)	Keys and combinations to locks within the facility are periodically changed or when keys are lost, combinations are compromised, or individuals are transferred or terminated.				

and

Test physical access control devices to determine if the following requirements are met:

Test Steps		S	N	Findings	Initials & Date
1	Verify that Physical access devices such as keys, locks and card readers function properly.				

PE-3.3 - Examine physical and environmental protection policy; procedures addressing physical access control; FIPS 201; NIST Special Publications 800-73, 800-76, and 800-78; information system design documentation; other relevant documents or records to determine if the following requirements are met:

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	The access control system is consistent with FIPS 201 and NIST Special Publication 800-73 (where the federal Personal Identity Verification (PIV) credential is used as an identification-token and token-based access control is employed).				

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(ii)	The access control system is consistent with NIST Special Publication 800-78 (where the token-based access control function employs cryptographic verification) .				
(iii)	The access control system is consistent with NIST Special Publication 800-76 (where the token-based access control function employs biometric verification).				

and

Test physical access control devices to determine if the following requirements are met:

Test Steps		S	N	Findings	Initials & Date
1	Verify where the federal Personal Identity Verification (PIV) credential is used as an identification token and token-based access control that these devices are functioning properly.				

PE-4 ACCESS CONTROL FOR TRANSMISSION MEDIUM - The organization controls physical access to information system distribution and transmission lines within organizational facilities.

PE-4.1 - Examine physical and environmental protection policy; procedures addressing access control for transmission medium; information system design documentation; facility communications and wiring diagrams; other relevant documents or records to determine if the following requirements are met:

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	Determine if the organization controls physical access to information system distribution and transmission lines within organizational facilities.				

PE-5 ACCESS CONTROL FOR DISPLAY MEDIUM - The organization controls physical access to information system devices that display information to prevent unauthorized individuals from observing the display output.

PE-5.1 - Examine physical and environmental protection policy; procedures addressing access control for display medium; facility layout of information system components; other relevant documents or records to determine if the following requirements are met:

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	Determine if the organization controls physical access to information system devices that display information to prevent unauthorized individuals from observing the display output.				

PE-6 MONITORING PHYSICAL ACCESS - The organization monitors physical access to the information system to detect and respond to physical security incidents.

PE-6.1 - Examine physical and environmental protection policy; procedures addressing physical access monitoring; physical access logs or records; other relevant documents or records, **and**

Interview organizational personnel with physical access monitoring responsibilities to determine if the following requirements are met:

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	Determine if the organization monitors physical access to the information system to detect and respond to physical security incidents.				

and

Test physical access monitoring capability to determine if the following requirements are met:

Test Steps		S	N	Findings	Initials & Date
1	Verify that organization monitors physical access to the information system to detect and respond to physical security incidents.				

PE-6(1).1 - Examine physical and environmental protection policy; procedures addressing physical access monitoring; intrusion alarm/surveillance equipment logs or records; other relevant documents or records, to determine if the following requirements are met:

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	Determine if the organization monitors real-time intrusion alarms and surveillance equipment.				

PE-7 VISITOR 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.

PE-7.1 - Examine physical and environmental protection policy; procedures addressing visitor access control; visitor access control logs or records; other relevant documents or records, **and**

Interview organizational personnel with visitor access control responsibilities to determine if the following requirements are met:

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	Determine if 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.				

and

Test visitor access control capability to determine if the following requirements are met:

Test Steps		S	N	Findings	Initials & Date
1	Verify that physical and environmental protection policy are adhered to.				
2	Verify procedures addressing visitor access control are met according to documented policy.				

PE-7(1).1 - Examine Physical and environmental protection policy; procedures addressing visitor access control; visitor access control logs or records; other relevant documents or records, **and**

Interview organizational personnel with visitor access control responsibilities to determine if the following requirements are met:

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	Determine if the organization escorts visitors and monitors visitor activity, when required.				

PE-8 ACCESS RECORDS - The organization maintains visitor access records to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible) that includes: (i) name and organization of the person visiting; (ii) signature of the visitor; (iii) form of identification; (iv) date of access; (v) time of entry and departure; (vi) purpose of visit; and (vii) name and organization of person visited. Designated officials within the organization review the visitor access records [Assignment: organization-defined frequency].

PE-8.1 - Examine physical and environmental protection policy; procedures addressing facility access records; information system security plan (for organization-defined frequency for review of visitor access records);facility access control records; other relevant documents or records to determine if the following requirements are met:

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	The organization defines the frequency of review for visitor access records.				
(ii)	The organization maintains visitor access records to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible) that includes: - name and organization of the person visiting. - signature of the visitor - form of identification - date of access - time of entry and departure - purpose of visit - name and organization of person visited.				
(iii)	Designated officials within the organization review the visitor access				

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
	logs in accordance with organization-defined frequency.				

PE-9 POWER EQUIPMENT AND POWER CABLING - The organization protects power equipment and power cabling for the information system from damage and destruction.

PE-9.1 - Examine physical and environmental protection policy; procedures addressing power equipment and cabling protection; facility housing power equipment and cabling; other relevant documents or records to determine if the following requirements are met:

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	Determine if the organization protects power equipment and power cabling for the information system from damage and destruction.				

PE-10 EMERGENCY SHUTOFF - The organization provides, for specific locations within a facility containing concentrations of information system resources, the capability of shutting off power to any information system component that may be malfunctioning or threatened without endangering personnel by requiring them to approach the equipment.

PE-10.1 - Examine physical and environmental protection policy; procedures addressing power source emergency shutoff; emergency shutoff controls or switches; other relevant documents or records to determine if the following requirements are met:

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	The organization defines the specific locations within a facility containing concentrations of information system resources (e.g., data centers, server rooms, mainframe rooms) .				
(ii)	The organization provides, for specific locations within a facility containing concentrations of information system resources, the capability of shutting off power to any information system component that may be malfunctioning or threatened without endangering personnel by requiring them to approach the equipment.				

PE-11 EMERGENCY POWER - 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.

PE-11.1 - Examine physical and environmental protection policy; procedures addressing emergency power; uninterruptible power supply documentation; other relevant documents or records to determine if the following requirements are met:

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	Determine if 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.				

and

Test uninterruptible power supply to determine if the following requirements are met:

Test Steps		S	N	Findings	Initials & Date
1	Validate that the uninterruptible power supply is used during an orderly shutdown during power loss.				

PE-12 EMERGENCY LIGHTING - The organization employs and maintains automatic emergency lighting that activates in the event of a power outage or disruption and that covers emergency exits and evacuation routes.

PE-12.1 - Examine physical and environmental protection policy; procedures addressing emergency lighting; emergency lighting documentation; emergency lighting test records; emergency exits and evacuation routes; other relevant documents or records to determine if the following requirements are met:

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	The organization employs and maintains automatic emergency lighting systems that activates in the event of a power outage or disruption.				
(ii)	The organization employs and maintains automatic emergency lighting systems that cover emergency exits and evacuation routes.				

and

Test emergency lighting capability to determine if the following requirements are met:

Test Steps		S	N	Findings	Initials & Date
1	Validate that the emergency lighting function in accordance with the physical and environmental protection policy and procedures.				

PE-13 FIRE PROTECTION - The organization employs and maintains fire suppression and detection devices/systems that can be activated in the event of a fire.

PE-13.1 - Examine physical and environmental protection policy; procedures addressing fire protection; fire suppression and detection devices/systems; fire suppression and detection devices/systems documentation; test records of fire suppression and detection devices/systems; other relevant documents or records to determine if the following requirements are met:

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	Determine if the organization employs and maintains fire suppression and detection devices/systems that can be activated in the event of a fire.				

PE-13(1).1 - Examine physical and environmental protection policy; procedures addressing fire protection; facility housing the information system; alarm service level agreements; test records of fire suppression and detection devices/systems; fire suppression and detection devices/systems documentation; other relevant documents or records to determine if the following requirements are met:

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	The organization employs fire detection devices/systems that activate automatically.				
(ii)	The organization employs fire detection devices/systems that notify the organization and emergency responders in the event of a fire.				

and

Test simulated fire detection and automated notifications to determine if the following requirements are met:

Test Steps		S	N	Findings	Initials & Date
1	Validate that the fire protection alarm services satisfies the physical and environmental protection policy.				

PE-13(2).1 - Examine physical and environmental protection policy; procedures addressing fire protection; fire suppression and detection devices/systems documentation; facility housing the information system; alarm service level agreements; test records of fire suppression and detection devices/systems; other relevant documents or records to determine if the following requirements are met:

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	Determine if the organization employs fire suppression devices/systems that provide automatic notification of any activation to the organization and emergency responders.				

and

Test simulated fire detection and automated notifications to determine if the following requirements are met:

Test Steps		S	N	Findings	Initials & Date
1	Validate that the fire protection fire suppression and detection devices satisfies the physical and environmental protection policy.				

PE-13(3).1 - Examine physical and environmental protection policy; procedures addressing fire protection; facility housing the information system; alarm service level agreements; facility staffing plans; test records of fire suppression and detection devices/systems; other relevant documents or records to determine if the following requirements are met:

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	Determine if the organization employs an automatic fire suppression capability in facilities that are not staffed on a continuous basis.				

and

Test simulated fire detection and automated notifications to determine if the following requirements are met:

Test Steps		S	N	Findings	Initials & Date
1	Validate that the fire protection automatic fire suppression and detection devices satisfies the physical and environmental protection policy.				

PE-14 TEMPERATURE AND HUMIDITY CONTROLS - The organization regularly maintains, within acceptable levels, and monitors the temperature and humidity within the facility where the information system resides.

PE-14.1 - Examine physical and environmental protection policy; procedures addressing temperature and humidity control; facility housing the information system; temperature and humidity controls; temperature and humidity controls documentation; temperature and humidity records; other relevant documents or records to determine if the following requirements are met:

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	The organization regularly maintains, within acceptable levels, the temperature and humidity within the facility where the information system resides.				
(ii)	The organization regularly monitors the temperature and humidity within the facility where the information system resides.				

PE-15 WATER DAMAGE PROTECTION - The organization protects the information system from water damage resulting from broken plumbing lines or other sources of water leakage by providing master shutoff valves that are accessible, working properly, and known to key personnel.

PE-15.1 - Examine physical and environmental protection policy; procedures addressing water damage protection; facility housing the information system; master shutoff values; list of key personnel with knowledge of location and activation procedures for master shutoff values for the plumbing system; master shutoff value documentation; other relevant documents or records, **and**

Interview organization personnel with physical and environmental protection responsibilities to determine if the following requirements are met:

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	The organization identifies key personnel with knowledge of location and operational procedures for activating master shutoff valves for plumbing system.				
(ii)	The organization protects the information system from water damage resulting from broken plumbing lines or other sources of water leakage by providing master shutoff valves that are accessible, working properly, and known to key personnel.				

and

Test simulated master water shutoff value activation for the plumbing system to determine if the following requirements are met:

Test Steps		S	N	Findings	Initials & Date
1	Validate that the water systems satisfies the physical and environmental protection policy.				

PE-16 DELIVERY AND REMOVAL - The organization authorizes and controls information system-related items entering and exiting the facility and maintains appropriate records of those items.

PE-16.1 - Examine physical and environmental protection policy; procedures addressing delivery and removal of information system components from the facility; facility housing the information system; records of items entering and exiting the facility; other relevant documents or records, **and**

Interview organization personnel with tracking responsibilities for information system components entering and exiting the facility to determine if the following requirements are met:

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	The organization controls information system-related items (i.e., hardware, firmware, software) entering and exiting the facility.				
(ii)	The organization maintains appropriate records of items entering and				

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
	exiting the facility.				

PE-17 ALTERNATE WORK SITE - The organization employs appropriate management, operational, and technical information system security controls at alternate work sites.

PE-17.1 - Examine physical and environmental protection policy; procedures addressing alternate work sites for organizational personnel; list of management, operational, and technical security controls required for alternate work sites; other relevant documents or records, **and**

Interview organization personnel using alternate work sites to determine if the following requirements are met:

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	Determine if the organization employs appropriate management, operational, and technical information system security controls at alternate work sites.				

PE-18 LOCATION OF INFORMATION SYSTEM COMPONENTS - 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.

PE-18.1 - Examine physical and environmental protection policy; procedures addressing positioning of information system components; documentation providing the location and position of information system components within the facility; other relevant documents or records to determine if the following requirements are met:

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	The organization positions information system components within the facility to minimize potential damage from physical and environmental hazards.				
(ii)	The organization positions information system components within the facility to minimize the opportunity for unauthorized access.				