3.11 PHYSICAL AND ENVIRONMENTAL PROTECTION

Quick link to Physical and Environmental Protection Summary Table

PE-1 POLICY AND PROCEDURES

Control:

a. Develop, document, and disseminate to [*Assignment: organization-defined personnel or roles*]:

   1. [*Selection (one or more): Organization-level; Mission/business process-level; System-level*] physical and environmental protection policy that:

      (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

      (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and

   2. Procedures to facilitate the implementation of the physical and environmental protection policy and the associated physical and environmental protection controls;

b. Designate an [*Assignment: organization-defined official*] to manage the development, documentation, and dissemination of the physical and environmental protection policy and procedures; and

c. Review and update the current physical and environmental protection:

   1. Policy [*Assignment: organization-defined frequency*] and following [*Assignment: organization-defined events*]; and

   2. Procedures [*Assignment: organization-defined frequency*] and following [*Assignment: organization-defined events*].

Discussion: Physical and environmental protection policy and procedures address the controls in the PE family that are implemented within systems and organizations. The risk management strategy is an important factor in establishing such policies and procedures. Policies and procedures contribute to security and privacy assurance. Therefore, it is important that security and privacy programs collaborate on the development of physical and environmental protection policy and procedures. Security and privacy program policies and procedures at the organization level are preferable, in general, and may obviate the need for mission- or system-specific policies and procedures. The policy can be included as part of the general security and privacy policy or be represented by multiple policies that reflect the complex nature of organizations. Procedures can be established for security and privacy programs, for mission or business processes, and for systems, if needed. Procedures describe how the policies or controls are implemented and can be directed at the individual or role that is the object of the procedure. Procedures can be documented in system security and privacy plans or in one or more separate documents. Events that may precipitate an update to physical and environmental protection policy and procedures include assessment or audit findings, security incidents or breaches, or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. Simply restating controls does not constitute an organizational policy or procedure.

Related Controls: AT-3, PM-9, PS-8, SI-12.

Control Enhancements: None.

References: [SP 800-12], [SP 800-30], [SP 800-39], [SP 800-100].

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-53r5

PE-2 PHYSICAL ACCESS AUTHORIZATIONS

Control:

a. Develop, approve, and maintain a list of individuals with authorized access to the facility where the system resides;

b. Issue authorization credentials for facility access;

c. Review the access list detailing authorized facility access by individuals [*Assignment: organization-defined frequency*]; and

d. Remove individuals from the facility access list when access is no longer required.

Discussion: Physical access authorizations apply to employees and visitors. Individuals with permanent physical access authorization credentials are not considered visitors. Authorization credentials include ID badges, identification cards, and smart cards. Organizations determine the strength of authorization credentials needed consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. Physical access authorizations may not be necessary to access certain areas within facilities that are designated as publicly accessible.

Related Controls: AT-3, AU-9, IA-4, MA-5, MP-2, PE-3, PE-4, PE-5, PE-8, PM-12, PS-3, PS-4, PS-5, PS-6.

Control Enhancements:

(1) PHYSICAL ACCESS AUTHORIZATIONS | ACCESS BY POSITION OR ROLE

Authorize physical access to the facility where the system resides based on position or role.

Discussion: Role-based facility access includes access by authorized permanent and regular/routine maintenance personnel, duty officers, and emergency medical staff.

Related Controls: AC-2, AC-3, AC-6.

(2) PHYSICAL ACCESS AUTHORIZATIONS | TWO FORMS OF IDENTIFICATION

Require two forms of identification from the following forms of identification for visitor access to the facility where the system resides: [*Assignment: organization-defined list of acceptable forms of identification*].

Discussion: Acceptable forms of identification include passports, REAL ID-compliant drivers' licenses, and Personal Identity Verification (PIV) cards. For gaining access to facilities using automated mechanisms, organizations may use PIV cards, key cards, PINs, and biometrics.

Related Controls: IA-2, IA-4, IA-5.

(3) PHYSICAL ACCESS AUTHORIZATIONS | RESTRICT UNESCORTED ACCESS

Restrict unescorted access to the facility where the system resides to personnel with [*Selection (one or more): security clearances for all information contained within the system; formal access authorizations for all information contained within the system; need for access to all information contained within the system;* [*Assignment: organization-defined physical access authorizations*]].

Discussion: Individuals without required security clearances, access approvals, or need to know are escorted by individuals with appropriate physical access authorizations to ensure that information is not exposed or otherwise compromised.

Related Controls: PS-2, PS-6.

References: [FIPS 201-2], [SP 800-73-4], [SP 800-76-2], [SP 800-78-4].

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-53r5

PE-3 PHYSICAL ACCESS CONTROL

Control:

a. Enforce physical access authorizations at [*Assignment: organization-defined entry and exit points to the facility where the system resides*] by:

   1. Verifying individual access authorizations before granting access to the facility; and

   2. Controlling ingress and egress to the facility using [*Selection (one or more):* [*Assignment: organization-defined physical access control systems or devices*]; *guards*];

b. Maintain physical access audit logs for [*Assignment: organization-defined entry or exit points*];

c. Control access to areas within the facility designated as publicly accessible by implementing the following controls: [*Assignment: organization-defined physical access controls*];

d. Escort visitors and control visitor activity [*Assignment: organization-defined circumstances requiring visitor escorts and control of visitor activity*];

e. Secure keys, combinations, and other physical access devices;

f. Inventory [*Assignment: organization-defined physical access devices*] every [*Assignment: organization-defined frequency*]; and

g. Change combinations and keys [*Assignment: organization-defined frequency*] and/or when keys are lost, combinations are compromised, or when individuals possessing the keys or combinations are transferred or terminated.

Discussion: Physical access control applies to employees and visitors. Individuals with permanent physical access authorizations are not considered visitors. Physical access controls for publicly accessible areas may include physical access control logs/records, guards, or physical access devices and barriers to prevent movement from publicly accessible areas to non-public areas. Organizations determine the types of guards needed, including professional security staff, system users, or administrative staff. Physical access devices include keys, locks, combinations, biometric readers, and card readers. Physical access control systems comply with applicable laws, executive orders, directives, policies, regulations, standards, and guidelines. Organizations have flexibility in the types of audit logs employed. Audit logs can be procedural, automated, or some combination thereof. Physical access points can include facility access points, interior access points to systems that require supplemental access controls, or both. Components of systems may be in areas designated as publicly accessible with organizations controlling access to the components.

Related Controls: AT-3, AU-2, AU-6, AU-9, AU-13, CP-10, IA-3, IA-8, MA-5, MP-2, MP-4, PE-2, PE-4, PE-5, PE-8, PS-2, PS-3, PS-6, PS-7, RA-3, SC-28, SI-4, SR-3.

Control Enhancements:

(1) PHYSICAL ACCESS CONTROL | SYSTEM ACCESS

Enforce physical access authorizations to the system in addition to the physical access controls for the facility at [*Assignment: organization-defined physical spaces containing one or more components of the system*].

Discussion: Control of physical access to the system provides additional physical security for those areas within facilities where there is a concentration of system components.

Related Controls: None.

(2) PHYSICAL ACCESS CONTROL | FACILITY AND SYSTEMS

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-53r5

Perform security checks [*Assignment: organization-defined frequency*] at the physical perimeter of the facility or system for exfiltration of information or removal of system components.

Discussion: Organizations determine the extent, frequency, and/or randomness of security checks to adequately mitigate risk associated with exfiltration.

Related Controls: AC-4, SC-7.

(3) PHYSICAL ACCESS CONTROL | CONTINUOUS GUARDS

Employ guards to control [*Assignment: organization-defined physical access points*] to the facility where the system resides 24 hours per day, 7 days per week.

Discussion: Employing guards at selected physical access points to the facility provides a more rapid response capability for organizations. Guards also provide the opportunity for human surveillance in areas of the facility not covered by video surveillance.

Related Controls: CP-6, CP-7, PE-6.

(4) PHYSICAL ACCESS CONTROL | LOCKABLE CASINGS

Use lockable physical casings to protect [*Assignment: organization-defined system components*] from unauthorized physical access.

Discussion: The greatest risk from the use of portable devices—such as smart phones, tablets, and notebook computers—is theft. Organizations can employ lockable, physical casings to reduce or eliminate the risk of equipment theft. Such casings come in a variety of sizes, from units that protect a single notebook computer to full cabinets that can protect multiple servers, computers, and peripherals. Lockable physical casings can be used in conjunction with cable locks or lockdown plates to prevent the theft of the locked casing containing the computer equipment.

Related Controls: None.

(5) PHYSICAL ACCESS CONTROL | TAMPER PROTECTION

Employ [*Assignment: organization-defined anti-tamper technologies*] to [*Selection (one or more): detect; prevent*] physical tampering or alteration of [*Assignment: organization-defined hardware components*] within the system.

Discussion: Organizations can implement tamper detection and prevention at selected hardware components or implement tamper detection at some components and tamper prevention at other components. Detection and prevention activities can employ many types of anti-tamper technologies, including tamper-detection seals and anti-tamper coatings. Anti-tamper programs help to detect hardware alterations through counterfeiting and other supply chain-related risks.

Related Controls: SA-16, SR-9, SR-11.

(6) PHYSICAL ACCESS CONTROL | FACILITY PENETRATION TESTING

[Withdrawn: Incorporated into CA-8.]

(7) PHYSICAL ACCESS CONTROL | PHYSICAL BARRIERS

Limit access using physical barriers.

Discussion: Physical barriers include bollards, concrete slabs, jersey walls, and hydraulic active vehicle barriers.

Related Controls: None.

(8) PHYSICAL ACCESS CONTROL | ACCESS CONTROL VESTIBULES

Employ access control vestibules at [*Assignment: organization-defined locations within the facility*].

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-53r5

Discussion: An access control vestibule is part of a physical access control system that typically provides a space between two sets of interlocking doors. Vestibules are designed to prevent unauthorized individuals from following authorized individuals into facilities with controlled access. This activity, also known as piggybacking or tailgating, results in unauthorized access to the facility. Interlocking door controllers can be used to limit the number of individuals who enter controlled access points and to provide containment areas while authorization for physical access is verified. Interlocking door controllers can be fully automated (i.e., controlling the opening and closing of the doors) or partially automated (i.e., using security guards to control the number of individuals entering the containment area).

Related Controls: None.

References: [FIPS 201-2], [SP 800-73-4], [SP 800-76-2], [SP 800-78-4], [SP 800-116].

PE-4 ACCESS CONTROL FOR TRANSMISSION

Control: Control physical access to [*Assignment: organization-defined system distribution and transmission lines*] within organizational facilities using [*Assignment: organization-defined security controls*].

Discussion: Security controls applied to system distribution and transmission lines prevent accidental damage, disruption, and physical tampering. Such controls may also be necessary to prevent eavesdropping or modification of unencrypted transmissions. Security controls used to control physical access to system distribution and transmission lines include disconnected or locked spare jacks, locked wiring closets, protection of cabling by conduit or cable trays, and wiretapping sensors.

Related Controls: AT-3, IA-4, MP-2, MP-4, PE-2, PE-3, PE-5, PE-9, SC-7, SC-8.

Control Enhancements: None.

References: None.

PE-5 ACCESS CONTROL FOR OUTPUT DEVICES

Control: Control physical access to output from [*Assignment: organization-defined output devices*] to prevent unauthorized individuals from obtaining the output.

Discussion: Controlling physical access to output devices includes placing output devices in locked rooms or other secured areas with keypad or card reader access controls and allowing access to authorized individuals only, placing output devices in locations that can be monitored by personnel, installing monitor or screen filters, and using headphones. Examples of output devices include monitors, printers, scanners, audio devices, facsimile machines, and copiers.

Related Controls: PE-2, PE-3, PE-4, PE-18.

Control Enhancements:

(1) ACCESS CONTROL FOR OUTPUT DEVICES | ACCESS TO OUTPUT BY AUTHORIZED INDIVIDUALS

[Withdrawn: Incorporated into PE-5.]

(2) ACCESS CONTROL FOR OUTPUT DEVICES | LINK TO INDIVIDUAL IDENTITY

Link individual identity to receipt of output from output devices.

Discussion: Methods for linking individual identity to the receipt of output from output devices include installing security functionality on facsimile machines, copiers, and printers. Such functionality allows organizations to implement authentication on output devices prior to the release of output to individuals.

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-53r5

Related Controls: None.

(3) ACCESS CONTROL FOR OUTPUT DEVICES | MARKING OUTPUT DEVICES

[Withdrawn: Incorporated into PE-22.]

References: [IR 8023].

PE-6 MONITORING PHYSICAL ACCESS

Control:

a. Monitor physical access to the facility where the system resides to detect and respond to physical security incidents;

b. Review physical access logs [*Assignment: organization-defined frequency*] and upon occurrence of [*Assignment: organization-defined events or potential indications of events*]; and

c. Coordinate results of reviews and investigations with the organizational incident response capability.

Discussion: Physical access monitoring includes publicly accessible areas within organizational facilities. Examples of physical access monitoring include the employment of guards, video surveillance equipment (i.e., cameras), and sensor devices. Reviewing physical access logs can help identify suspicious activity, anomalous events, or potential threats. The reviews can be supported by audit logging controls, such as AU-2, if the access logs are part of an automated system. Organizational incident response capabilities include investigations of physical security incidents and responses to the incidents. Incidents include security violations or suspicious physical access activities. Suspicious physical access activities include accesses outside of normal work hours, repeated accesses to areas not normally accessed, accesses for unusual lengths of time, and out-of-sequence accesses.

Related Controls: AU-2, AU-6, AU-9, AU-12, CA-7, CP-10, IR-4, IR-8.

Control Enhancements:

(1) MONITORING PHYSICAL ACCESS | INTRUSION ALARMS AND SURVEILLANCE EQUIPMENT

Monitor physical access to the facility where the system resides using physical intrusion alarms and surveillance equipment.

Discussion: Physical intrusion alarms can be employed to alert security personnel when unauthorized access to the facility is attempted. Alarm systems work in conjunction with physical barriers, physical access control systems, and security guards by triggering a response when these other forms of security have been compromised or breached. Physical intrusion alarms can include different types of sensor devices, such as motion sensors, contact sensors, and broken glass sensors. Surveillance equipment includes video cameras installed at strategic locations throughout the facility.

Related Controls: None.

(2) MONITORING PHYSICAL ACCESS | AUTOMATED INTRUSION RECOGNITION AND RESPONSES

Recognize [*Assignment: organization-defined classes or types of intrusions*] and initiate [*Assignment: organization-defined response actions*] using [*Assignment: organization-defined automated mechanisms*].

Discussion: Response actions can include notifying selected organizational personnel or law enforcement personnel. Automated mechanisms implemented to initiate response actions include system alert notifications, email and text messages, and activating door locking mechanisms. Physical access monitoring can be coordinated with intrusion detection

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-53r5

systems and system monitoring capabilities to provide integrated threat coverage for the organization.

Related Controls: SI-4.

(3) MONITORING PHYSICAL ACCESS | VIDEO SURVEILLANCE

(a) Employ video surveillance of [*Assignment: organization-defined operational areas*];

(b) Review video recordings [*Assignment: organization-defined frequency*]; and

(c) Retain video recordings for [*Assignment: organization-defined time period*].

Discussion: Video surveillance focuses on recording activity in specified areas for the purposes of subsequent review, if circumstances so warrant. Video recordings are typically reviewed to detect anomalous events or incidents. Monitoring the surveillance video is not required, although organizations may choose to do so. There may be legal considerations when performing and retaining video surveillance, especially if such surveillance is in a public location.

Related Controls: None.

(4) MONITORING PHYSICAL ACCESS | MONITORING PHYSICAL ACCESS TO SYSTEMS

Monitor physical access to the system in addition to the physical access monitoring of the facility at [*Assignment: organization-defined physical spaces containing one or more components of the system*].

Discussion: Monitoring physical access to systems provides additional monitoring for those areas within facilities where there is a concentration of system components, including server rooms, media storage areas, and communications centers. Physical access monitoring can be coordinated with intrusion detection systems and system monitoring capabilities to provide comprehensive and integrated threat coverage for the organization.

Related Controls: None.

References: None.

PE-7 VISITOR CONTROL

[Withdrawn: Incorporated into PE-2 and PE-3.]

PE-8 VISITOR ACCESS RECORDS

Control:

a. Maintain visitor access records to the facility where the system resides for [*Assignment: organization-defined time period*];

b. Review visitor access records [*Assignment: organization-defined frequency*]; and

c. Report anomalies in visitor access records to [*Assignment: organization-defined personnel*].

Discussion: Visitor access records include the names and organizations of individuals visiting, visitor signatures, forms of identification, dates of access, entry and departure times, purpose of visits, and the names and organizations of individuals visited. Access record reviews determine if access authorizations are current and are still required to support organizational mission and business functions. Access records are not required for publicly accessible areas.

Related Controls: PE-2, PE-3, PE-6.

Control Enhancements:

(1) VISITOR ACCESS RECORDS | AUTOMATED RECORDS MAINTENANCE AND REVIEW

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-53r5

Maintain and review visitor access records using [*Assignment: organization-defined automated mechanisms*].

Discussion: Visitor access records may be stored and maintained in a database management system that is accessible by organizational personnel. Automated access to such records facilitates record reviews on a regular basis to determine if access authorizations are current and still required to support organizational mission and business functions.

Related Controls: None.

(2) VISITOR ACCESS RECORDS | PHYSICAL ACCESS RECORDS

[Withdrawn: Incorporated into PE-2.]

(3) VISITOR ACCESS RECORDS | LIMIT PERSONALLY IDENTIFIABLE INFORMATION ELEMENTS

Limit personally identifiable information contained in visitor access records to the following elements identified in the privacy risk assessment: [*Assignment: organization-defined elements*].

Discussion: Organizations may have requirements that specify the contents of visitor access records. Limiting personally identifiable information in visitor access records when such information is not needed for operational purposes helps reduce the level of privacy risk created by a system.

Related Controls: RA-3, SA-8.

References: None.

PE-9 POWER EQUIPMENT AND CABLING

Control: Protect power equipment and power cabling for the system from damage and destruction.

Discussion: Organizations determine the types of protection necessary for the power equipment and cabling employed at different locations that are both internal and external to organizational facilities and environments of operation. Types of power equipment and cabling include internal cabling and uninterruptable power sources in offices or data centers, generators and power cabling outside of buildings, and power sources for self-contained components such as satellites, vehicles, and other deployable systems.

Related Controls: PE-4.

Control Enhancements:

(1) POWER EQUIPMENT AND CABLING | REDUNDANT CABLING

Employ redundant power cabling paths that are physically separated by [*Assignment: organization-defined distance*].

Discussion: Physically separate and redundant power cables ensure that power continues to flow in the event that one of the cables is cut or otherwise damaged.

Related Controls: None.

(2) POWER EQUIPMENT AND CABLING | AUTOMATIC VOLTAGE CONTROLS

Employ automatic voltage controls for [*Assignment: organization-defined critical system components*].

Discussion: Automatic voltage controls can monitor and control voltage. Such controls include voltage regulators, voltage conditioners, and voltage stabilizers.

Related Controls: None.

References: None.

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-53r5

PE-10 EMERGENCY SHUTOFF

Control:

a. Provide the capability of shutting off power to [*Assignment: organization-defined system or individual system components*] in emergency situations;

b. Place emergency shutoff switches or devices in [*Assignment: organization-defined location by system or system component*] to facilitate access for authorized personnel; and

c. Protect emergency power shutoff capability from unauthorized activation.

Discussion: Emergency power shutoff primarily applies to organizational facilities that contain concentrations of system resources, including data centers, mainframe computer rooms, server rooms, and areas with computer-controlled machinery.

Related Controls: PE-15.

Control Enhancements:

(1) EMERGENCY SHUTOFF | ACCIDENTAL AND UNAUTHORIZED ACTIVATION

[Withdrawn: Incorporated into PE-10.]

References: None.

PE-11 EMERGENCY POWER

Control: Provide an uninterruptible power supply to facilitate [*Selection (one or more): an orderly shutdown of the system; transition of the system to long-term alternate power*] in the event of a primary power source loss.

Discussion: An uninterruptible power supply (UPS) is an electrical system or mechanism that provides emergency power when there is a failure of the main power source. A UPS is typically used to protect computers, data centers, telecommunication equipment, or other electrical equipment where an unexpected power disruption could cause injuries, fatalities, serious mission or business disruption, or loss of data or information. A UPS differs from an emergency power system or backup generator in that the UPS provides near-instantaneous protection from unanticipated power interruptions from the main power source by providing energy stored in batteries, supercapacitors, or flywheels. The battery duration of a UPS is relatively short but provides sufficient time to start a standby power source, such as a backup generator, or properly shut down the system.

Related Controls: AT-3, CP-2, CP-7.

Control Enhancements:

(1) EMERGENCY POWER | ALTERNATE POWER SUPPLY — MINIMAL OPERATIONAL CAPABILITY

Provide an alternate power supply for the system that is activated [*Selection: manually; automatically*] and that can maintain minimally required operational capability in the event of an extended loss of the primary power source.

Discussion: Provision of an alternate power supply with minimal operating capability can be satisfied by accessing a secondary commercial power supply or other external power supply.

Related Controls: None.

(2) EMERGENCY POWER | ALTERNATE POWER SUPPLY — SELF-CONTAINED

Provide an alternate power supply for the system that is activated [*Selection: manually; automatically*] and that is:

(a) Self-contained;

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-53r5

(b) Not reliant on external power generation; and

(c) Capable of maintaining [*Selection: minimally required operational capability; full operational capability*] in the event of an extended loss of the primary power source.

Discussion: The provision of a long-term, self-contained power supply can be satisfied by using one or more generators with sufficient capacity to meet the needs of the organization.

Related Controls: None.

References: None.

PE-12 EMERGENCY LIGHTING

Control: Employ and maintain automatic emergency lighting for the system that activates in the event of a power outage or disruption and that covers emergency exits and evacuation routes within the facility.

Discussion: The provision of emergency lighting applies primarily to organizational facilities that contain concentrations of system resources, including data centers, server rooms, and mainframe computer rooms. Emergency lighting provisions for the system are described in the contingency plan for the organization. If emergency lighting for the system fails or cannot be provided, organizations consider alternate processing sites for power-related contingencies.

Related Controls: CP-2, CP-7.

Control Enhancements:

(1) EMERGENCY LIGHTING | ESSENTIAL MISSION AND BUSINESS FUNCTIONS

Provide emergency lighting for all areas within the facility supporting essential mission and business functions.

Discussion: Organizations define their essential missions and functions.

Related Controls: None.

References: None.

PE-13 FIRE PROTECTION

Control: Employ and maintain fire detection and suppression systems that are supported by an independent energy source.

Discussion: The provision of fire detection and suppression systems applies primarily to organizational facilities that contain concentrations of system resources, including data centers, server rooms, and mainframe computer rooms. Fire detection and suppression systems that may require an independent energy source include sprinkler systems and smoke detectors. An independent energy source is an energy source, such as a microgrid, that is separate, or can be separated, from the energy sources providing power for the other parts of the facility.

Related Controls: AT-3.

Control Enhancements:

(1) FIRE PROTECTION | DETECTION SYSTEMS — AUTOMATIC ACTIVATION AND NOTIFICATION

Employ fire detection systems that activate automatically and notify [*Assignment: organization-defined personnel or roles*] and [*Assignment: organization-defined emergency responders*] in the event of a fire.

Discussion: Organizations can identify personnel, roles, and emergency responders if individuals on the notification list need to have access authorizations or clearances (e.g., to enter to facilities where access is restricted due to the classification or impact level of

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-53r5

information within the facility). Notification mechanisms may require independent energy sources to ensure that the notification capability is not adversely affected by the fire.

Related Controls: None.

(2) FIRE PROTECTION | SUPPRESSION SYSTEMS — AUTOMATIC ACTIVATION AND NOTIFICATION

(a) Employ fire suppression systems that activate automatically and notify [*Assignment: organization-defined personnel or roles*] and [*Assignment: organization-defined emergency responders*]; and

(b) Employ an automatic fire suppression capability when the facility is not staffed on a continuous basis.

Discussion: Organizations can identify specific personnel, roles, and emergency responders if individuals on the notification list need to have appropriate access authorizations and/or clearances (e.g., to enter to facilities where access is restricted due to the impact level or classification of information within the facility). Notification mechanisms may require independent energy sources to ensure that the notification capability is not adversely affected by the fire.

Related Controls: None.

(3) FIRE PROTECTION | AUTOMATIC FIRE SUPPRESSION

[Withdrawn: Incorporated into PE-13(2).]

(4) FIRE PROTECTION | INSPECTIONS

Ensure that the facility undergoes [*Assignment: organization-defined frequency*] fire protection inspections by authorized and qualified inspectors and identified deficiencies are resolved within [*Assignment: organization-defined time period*].

Discussion: Authorized and qualified personnel within the jurisdiction of the organization include state, county, and city fire inspectors and fire marshals. Organizations provide escorts during inspections in situations where the systems that reside within the facilities contain sensitive information.

Related Controls: None.

References: None.

PE-14 ENVIRONMENTAL CONTROLS

Control:

a. Maintain [*Selection (one or more): temperature; humidity; pressure; radiation;* [*Assignment: organization-defined environmental control*]] levels within the facility where the system resides at [*Assignment: organization-defined acceptable levels*]; and

b. Monitor environmental control levels [*Assignment: organization-defined frequency*].

Discussion: The provision of environmental controls applies primarily to organizational facilities that contain concentrations of system resources (e.g., data centers, mainframe computer rooms, and server rooms). Insufficient environmental controls, especially in very harsh environments, can have a significant adverse impact on the availability of systems and system components that are needed to support organizational mission and business functions.

Related Controls: AT-3, CP-2.

Control Enhancements:

(1) ENVIRONMENTAL CONTROLS | AUTOMATIC CONTROLS

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-53r5

Employ the following automatic environmental controls in the facility to prevent fluctuations potentially harmful to the system: [*Assignment: organization-defined automatic environmental controls*].

Discussion: The implementation of automatic environmental controls provides an immediate response to environmental conditions that can damage, degrade, or destroy organizational systems or systems components.

Related Controls: None.

(2) ENVIRONMENTAL CONTROLS | MONITORING WITH ALARMS AND NOTIFICATIONS

Employ environmental control monitoring that provides an alarm or notification of changes potentially harmful to personnel or equipment to [*Assignment: organization-defined personnel or roles*].

Discussion: The alarm or notification may be an audible alarm or a visual message in real time to personnel or roles defined by the organization. Such alarms and notifications can help minimize harm to individuals and damage to organizational assets by facilitating a timely incident response.

Related Controls: None.

References: None.

PE-15 WATER DAMAGE PROTECTION

Control: Protect the system from damage resulting from water leakage by providing master shutoff or isolation valves that are accessible, working properly, and known to key personnel.

Discussion: The provision of water damage protection primarily applies to organizational facilities that contain concentrations of system resources, including data centers, server rooms, and mainframe computer rooms. Isolation valves can be employed in addition to or in lieu of master shutoff valves to shut off water supplies in specific areas of concern without affecting entire organizations.

Related Controls: AT-3, PE-10.

Control Enhancements:

(1) WATER DAMAGE PROTECTION | AUTOMATION SUPPORT

Detect the presence of water near the system and alert [*Assignment: organization-defined personnel or roles*] using [*Assignment: organization-defined automated mechanisms*].

Discussion: Automated mechanisms include notification systems, water detection sensors, and alarms.

Related Controls: None.

References: None.

PE-16 DELIVERY AND REMOVAL

Control:

a. Authorize and control [*Assignment: organization-defined types of system components*] entering and exiting the facility; and

b. Maintain records of the system components.

Discussion: Enforcing authorizations for entry and exit of system components may require restricting access to delivery areas and isolating the areas from the system and media libraries.

Related Controls: CM-3, CM-8, MA-2, MA-3, MP-5, PE-20, SR-2, SR-3, SR-4, SR-6.

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-53r5

Control Enhancements: None.

References: None.

PE-17 ALTERNATE WORK SITE

Control:

a. Determine and document the [*Assignment: organization-defined alternate work sites*] allowed for use by employees;

b. Employ the following controls at alternate work sites: [*Assignment: organization-defined controls*];

c. Assess the effectiveness of controls at alternate work sites; and

d. Provide a means for employees to communicate with information security and privacy personnel in case of incidents.

Discussion: Alternate work sites include government facilities or the private residences of employees. While distinct from alternative processing sites, alternate work sites can provide readily available alternate locations during contingency operations. Organizations can define different sets of controls for specific alternate work sites or types of sites depending on the work-related activities conducted at the sites. Implementing and assessing the effectiveness of organization-defined controls and providing a means to communicate incidents at alternate work sites supports the contingency planning activities of organizations.

Related Controls: AC-17, AC-18, CP-7.

Control Enhancements: None.

References: [SP 800-46].

PE-18 LOCATION OF SYSTEM COMPONENTS

Control: Position system components within the facility to minimize potential damage from [*Assignment: organization-defined physical and environmental hazards*] and to minimize the opportunity for unauthorized access.

Discussion: Physical and environmental hazards include floods, fires, tornadoes, earthquakes, hurricanes, terrorism, vandalism, an electromagnetic pulse, electrical interference, and other forms of incoming electromagnetic radiation. Organizations consider the location of entry points where unauthorized individuals, while not being granted access, might nonetheless be near systems. Such proximity can increase the risk of unauthorized access to organizational communications using wireless packet sniffers or microphones, or unauthorized disclosure of information.

Related Controls: CP-2, PE-5, PE-19, PE-20, RA-3.

(1) LOCATION OF SYSTEM COMPONENTS | FACILITY SITE

[Withdrawn: Moved to PE-23.]

References: None.

PE-19 INFORMATION LEAKAGE

Control: Protect the system from information leakage due to electromagnetic signals emanations.

Discussion: Information leakage is the intentional or unintentional release of data or information to an untrusted environment from electromagnetic signals emanations. The security categories

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-53r5

or classifications of systems (with respect to confidentiality), organizational security policies, and risk tolerance guide the selection of controls employed to protect systems against information leakage due to electromagnetic signals emanations.

Related Controls: AC-18, PE-18, PE-20.

Control Enhancements:

(1) INFORMATION LEAKAGE | NATIONAL EMISSIONS POLICIES AND PROCEDURES

Protect system components, associated data communications, and networks in accordance with national Emissions Security policies and procedures based on the security category or classification of the information.

Discussion: Emissions Security (EMSEC) policies include the former TEMPEST policies.

Related Controls: None.

References: [FIPS 199].

PE-20 ASSET MONITORING AND TRACKING

Control: Employ [*Assignment: organization-defined asset location technologies*] to track and monitor the location and movement of [*Assignment: organization-defined assets*] within [*Assignment: organization-defined controlled areas*].

Discussion: Asset location technologies can help ensure that critical assets—including vehicles, equipment, and system components—remain in authorized locations. Organizations consult with the Office of the General Counsel and senior agency official for privacy regarding the deployment and use of asset location technologies to address potential privacy concerns.

Related Controls: CM-8, PE-16, PM-8.

Control Enhancements: None.

References: None.

PE-21 ELECTROMAGNETIC PULSE PROTECTION

Control: Employ [*Assignment: organization-defined protective measures*] against electromagnetic pulse damage for [*Assignment: organization-defined systems and system components*].

Discussion: An electromagnetic pulse (EMP) is a short burst of electromagnetic energy that is spread over a range of frequencies. Such energy bursts may be natural or man-made. EMP interference may be disruptive or damaging to electronic equipment. Protective measures used to mitigate EMP risk include shielding, surge suppressors, ferro-resonant transformers, and earth grounding. EMP protection may be especially significant for systems and applications that are part of the U.S. critical infrastructure.

Related Controls: PE-18, PE-19.

Control Enhancements: None.

References: None.

PE-22 COMPONENT MARKING

Control: Mark [*Assignment: organization-defined system hardware components*] indicating the impact level or classification level of the information permitted to be processed, stored, or transmitted by the hardware component.

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-53r5

Discussion: Hardware components that may require marking include input and output devices. Input devices include desktop and notebook computers, keyboards, tablets, and smart phones. Output devices include printers, monitors/video displays, facsimile machines, scanners, copiers, and audio devices. Permissions controlling output to the output devices are addressed in AC-3 or AC-4. Components are marked to indicate the impact level or classification level of the system to which the devices are connected, or the impact level or classification level of the information permitted to be output. Security marking refers to the use of human-readable security attributes. Security labeling refers to the use of security attributes for internal system data structures. Security marking is generally not required for hardware components that process, store, or transmit information determined by organizations to be in the public domain or to be publicly releasable. However, organizations may require markings for hardware components that process, store, or transmit public information in order to indicate that such information is publicly releasable. Marking of system hardware components reflects applicable laws, executive orders, directives, policies, regulations, and standards.

Related Controls: AC-3, AC-4, AC-16, MP-3.

Control Enhancements: None.

References: [IR 8023].

PE-23 FACILITY LOCATION

Control:

a. Plan the location or site of the facility where the system resides considering physical and environmental hazards; and

b. For existing facilities, consider the physical and environmental hazards in the organizational risk management strategy.

Discussion: Physical and environmental hazards include floods, fires, tornadoes, earthquakes, hurricanes, terrorism, vandalism, an electromagnetic pulse, electrical interference, and other forms of incoming electromagnetic radiation. The location of system components within the facility is addressed in PE-18.

Related Controls: CP-2, PE-18, PE-19, PM-8, PM-9, RA-3.

References: None.

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-53r5