5.9 Physical and Environmental Protection (PE) Policy

PURPOSE

Physical and environmental protection policy and procedures address the controls that are implemented within systems and organizations.

POLICY

01. PHYSICAL ACCESS AUTHORIZATIONS

1. Develop, approve, and maintain a list of individuals with authorized access to the facilities where the information systems reside.
2. Issue authorization credentials for facility access.
3. Review the access list detailing authorized facility access by individuals and remove individuals from the facility access list when access is no longer required.
4. Remove individuals from the facility access list when access is not longer required.

02. PHYSICAL ACCESS CONTROL

1. Enforce physical access authorizations by verifying individual access authorizations before granting access to the facility and controlling ingress/egress to the facility using agency implemented procedures and controls.
2. Maintain physical access audit logs for the physically secure location and agency-defined sensitive areas.
3. Provide physical access devices including but not limited to keys, locks, combinations, biometric readers, placards, and/or card readers to control access to areas within the facility officially designated as non-publicly accessible.
4. Escort visitors and control visitor activity in all physically secure locations.
5. Secure keys, combinations, and other physical access devices.
6. Inventory all agency-issued physical access devices annually and change combinations and keys when keys are lost, combinations are compromised, or when individuals possessing the keys or combinations are transferred or terminated.

03. ACCESS CONTROL FOR TRANSMISSION

1. Control physical access to information system distribution and transmission lines and devices within organizational facilities using agency-implemented procedures and controls.

04. ACCESS CONTROL FOR OUTPUT DEVICES

1. Control physical access to output from monitors, printers, scanners, audio devices, facsimile machines, and copiers to prevent unauthorized individuals from obtaining the output.

05. MONITORING PHYSICAL ACCESS

1. Monitor physical access to the facility where the system resides to detect and respond to physical security incidents.
2. Review physical access logs quarterly and upon occurrence of any physical, environmental, or security-related incidents involving CJI, or systems used to process, store, or transmit CJI, and coordinate results of reviews and investigations with the organizational incident response capability.
3. Monitor physical access to the facility where the system resides using physical intrusion alarms and surveillance equipment.

07. VISITOR ACCESS RECORDS

1. Maintain visitor access records to the facility where the system resides for one (1) year, and review visitor access records quarterly.
2. Report anomalies in visitor access records to organizational personnel with physical and environmental protection responsibilities and organizational personnel with information security responsibilities.
3. Limit personally identifiable information contained in visitor access records to the minimum PII necessary to achieve the purpose for which it is collected (see Section 4.3).

08. POWER EQUIPMENT AND CABLING

1. Protect power equipment and power cabling for the information system from damage and destruction.

Note: This control only applies to data centers as defined in Appendix A Terms and Definitions.

09. EMERGENCY SHUTOFF

1. Provide the capability of shutting off power to all information systems in emergency situations.
2. Place emergency shutoff switches or devices in easily accessible locations to facilitate access for authorized personnel and protect emergency power shutoff capability from unauthorized activation.

Note: This control only applies to data centers as defined in Appendix A Terms and Definitions.

10. EMERGENCY POWER

1. Provide an uninterruptible power supply to facilitate an orderly shutdown of the information system or transition of the information system to an alternate power source in the event of a primary power source loss.

Note: This control only applies to data centers as defined in Appendix A Terms and Definitions.

11. EMERGENCY LIGHTING

1. 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.

Note: This control only applies to data centers as defined in Appendix A Terms and Definitions.

12. FIRE PROTECTION

1. Employ and maintain fire suppression and detection devices/systems that are supported by an independent energy source.
2. Employ fire detection systems that activate automatically and notify organizational personnel with physical and environmental protection responsibilities and police, fire, or emergency medical personnel in the event of a fire.

Note: This control only applies to data centers as defined in Appendix A Terms and Definitions.

13. ENVIRONMENTAL CONTROLS

1. Maintain adequate HVAC levels within the facility where the system resides at recommended system manufacturer levels and monitor environmental control levels continuously.

Note: This control only applies to data centers as defined in Appendix A Terms and Definitions.

14. WATER DAMAGE PROTECTION

1. 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.

Note: This control only applies to data centers as defined in Appendix A Terms and Definitions.

15. DELIVERY AND REMOVAL

1. Authorize and control information system-related components entering and exiting the facility and maintain records of the system components.

16. ALTERNATE WORK SITE

1. Determine and document all alternative facilities or locations allowed for use by employees employing the following controls at the alternate work sites:
   1. Limit access to the area during CJI processing times to only those personnel authorized by the agency to access or view CJI.
   2. Lock the area, rom, or storage container when unattended.
   3. Position information system devices and documents containing CJI in such a way as to prevent unauthorized individuals from access and view.
   4. Follow the encryption requirements found in SC-13 and SC-28 for electronic storage (i.e., data at rest) of CJI.
2. Assess the effectiveness of controls at alternate work sites and provide a means for employees to communicate with information security and privacy personnel in case of incidents.

PROCEDURES

Agency must provide the procedures on how the policies will be implemented.

Compliance

Employees who violate this policy may be subject to appropriate disciplinary action up to and including discharge as well as both civil and criminal penalties. Non-employees, including, without limitation, contractors, may be subject to termination of contractual agreements, denial of access to IT resources, and other actions as well as both civil and criminal penalties.

REFERENCE

AC-17, AC-18, CP-7.