EPA IT/IM DIRECTIVE
PROCEDURE

Information Security – Physical and Environmental Protection (PE) Procedure

Directive No: CIO 2150-P-11.3

Issued by the EPA Chief Information Officer,
Pursuant to Delegation 1-19

Information Security – Physical and Environmental Protection (PE) Procedure

1. PURPOSE

The Environmental Protection Agency (EPA) is responsible for ensuring all offices within the Agency meet the minimum-security requirements defined in the Federal Information Processing Standards (FIPS) Publication 200, *Minimum Security Requirements for Federal Information and Information Systems*. All EPA information systems shall meet the security requirements by implementing the security controls defined in the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations*.

The purpose of this procedure is to facilitate the implementation of the EPA security control requirements for the Physical and Environmental Protection (PE) control family, as identified in NIST SP 800-53, Revision 5.

2. SCOPE

These procedures address all EPA information and information systems to include information and information systems used, managed or operated by a contractor, another agency or other organization on behalf of the EPA.

3. AUDIENCE

Senior Information Officials (SIO), Information Security Officers (ISO) and EPA System Owners (SO) or their official designees, for EPA-operated systems, and Service Managers (SM), for systems operated on behalf of the EPA, EPA employees, contractors and all other users of EPA information and systems.

4. AUTHORITY

- Federal Information Security Modernization Act (FISMA) of 2014, Public Law 113-283, to amend chapter 35 of title 44, United States Code (U.S.C.)
- Office of Management and Budget (OMB) Circular A-130, “Managing Information as a Strategic Resource,” July 2016
- FIPS 200, Minimum Security Requirements for Federal Information and Information Systems, March 2006
- NIST SP 800-53, Revision 5, Security and Privacy Controls for Information Systems and Organizations, September 2020
- NIST SP 800-53B, Control Baselines for Information Systems and Organizations, October 2020
- 32 CFR Section 2002, Controlled Unclassified Information, 9/14/2016

5. PROCEDURE

SIO, ISO and EPA SO or their official designees for EPA-operated systems; and SM, for systems operated on behalf of the EPA and to the extent made applicable to their management of the system through a contract or other appropriate mechanism, are responsible for implementing the controls in this procedure. EPA is adopting this procedure agency-wide, and expects these officials to develop a plan with timelines for adoption for their system(s). EPA employees, contractors and all other users of EPA information and information systems that support the operations and assets of the EPA should be aware of the content of this procedure and should follow the directions provided by SIO, ISO and EPA SO or their official designees and SM for the systems that they oversee.

The "PE" designator (e.g., PE-2, PE-3) identified for each procedure below corresponds to the NIST- identifier for the Physical and Environmental Protection control family, as identified in NIST SP 800-53, Revision 5.

NIST defines the applicable PE baseline controls in NIST 800-53B, *Control Baselines for Information Systems and Organizations*. The applicable security baseline for each impact level (Low, Moderate, High or For All Systems) as well as the Privacy Control Baseline are identified below the control name. EPA may deviate from the NIST 800-53B Security or Privacy Control Baselines by adding/removing controls or to applicable baselines and are notated with an asterisk.

PE-2 – Physical Access Authorizations
For All Systems:

1) Develop, approve, and maintain a list of individuals with authorized access to the facility where the system resides;
2) Issue authorization credentials for facility access;
3) Review the access list detailing authorized facility access by individuals quarterly or immediately upon notification that a contract has ended or a member of the staff (federal or contractor) has separated from the Agency; and
4) Remove individuals from the facility access list when access is no longer required.

PE-3 – Physical Access Control
For All Systems:

1) Enforce physical access authorizations at all physical access and exit points to non-public facilities and areas where EPA information is stored or processed by:
   a) Verifying individual access authorizations before granting access to the facility; and
   b) Controlling ingress and egress to the facility using physical access controls such as security guards; keyed, combination or electronic locks; or personal identity verification (PIV)-access turnstiles;
2) Maintain physical access audit logs for all entry/exit points to non-public spaces where EPA information is processed or stored;
3) Control access to areas within the facility designated as publicly accessible by implementing the following controls: all personnel and visitors are required to display their badges while inside the facility;

4) Escort visitors and control visitor activity at all times;
5) Secure keys, combinations, and other physical access devices;
6) Inventory office/door keys; non-PIV card devices used to access areas, cabinets, etc. every year; and
7) Change combinations and keys when directed by management and/or when keys are lost, combinations are compromised, or when individuals possessing the keys or combinations are transferred or terminated.

PE-3(1) – Physical Access Control | System Access
For High Systems:

1) Enforce physical access authorizations to the system in addition to the physical access controls for the facility at network/communicationclosets, rooms, and other areas not available to visitors.

PE-4 – Access Control for Transmission
For Moderate and High Systems:

1) Control physical access to information system distribution and transmission lines within organizational facilities using security controls, such as, locked wiring closets using keyed, combination or electronic locks; and protection of cabling by conduit or cable trays.

PE-5 – Access Control for Output Devices
For Moderate and High Systems:

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

PE-6 – Monitoring Physical Access
For All Systems:

1) Monitor physical access to the facility where the system resides to detect and respond to physical security incidents;
2) Review physical access logs monthly for Low and Moderate categorized information, weekly for High categorized information and upon occurrence of physical or cybersecurity incidents; and
3) Coordinate results of reviews and investigations with the organizational incident response capability.

PE-6(1) – Monitoring Physical Access | Intrusion Alarms / Surveillance Equipment
For Moderate and High Systems:

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

PE-6(4) – Monitoring Physical Access | Monitoring Physical Access to Systems
For High Systems:

1) Monitor physical access to the system in addition to the physical access monitoring of the facility at physical spaces, including server rooms, media storage rooms, and communication rooms (closets) containing one or more components of the system.

PE-8 – Visitor Access Records

For All Systems:

1) Maintain visitor access records to the facility where the system resides for time periods in accordance with EPA Records Control Schedule;
2) Review visitor access records in response to an information or physical security incident; and
3) Report anomalies in visitor access records to the local physical security office.

PE-8(1) – Visitor Access Records | Automated Records Maintenance and Review

For High Systems:

1) Maintain and review visitor access records using automated mechanisms or a paper-based system if no computer access system is available.

PE-8(3) – Visitor Access Records | Limit Personally Identifiable Information Elements

For Privacy Control Baseline:

1) Limit personally identifiable information contained in visitor access records to the following elements identified in the privacy risk assessment: name, organization, and POC/escort name.

PE-9 – Power Equipment and Cabling

For Moderate and High Systems:

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

PE-10 – Emergency Shutoff

For Moderate and High Systems:

1) Provide the capability of shutting off power to the information system or individual system components in emergency situations;
2) Place emergency shutoff switches or devices in locations as defined by applicable standards to facilitate access for authorized personnel; and
3) Protect emergency power shutoff capability from unauthorized activation.

PE-11 – Emergency Power

For Moderate and High Systems:

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

PE-11(1) – Emergency Power | Alternate Power Supply — Minimal Operational Capability

For High Systems:

1) Provide an alternate power supply for the system that is activated automatically and that can maintain minimally required operational capability in the event of an extended loss of the primary power source.

PE-12 – Emergency Lighting

For All Systems:

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.

PE-13 – Fire Protection

For All Systems:

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

PE-13(1) – Fire Protection | Detection Systems– Automatic Activation and Notification

For Moderate and High Systems:

1) Employ fire detection systems that activate automatically and notify the local physical security office and/or the facility management office and the local fire department in the event of a fire.

PE-13(2) – Fire Protection | Suppression Systems – Automatic Activation and Notification

For High Systems:

1) Employ fire suppression systems that activate automatically and notify the local physical security office and/or the facility management office and the local fire department; and
2) Employ an automatic fire suppression capability when the facility is not staffed on a continuous basis.

PE-14 – Environmental Controls

For All Systems:

1) Maintain temperature and humidity levels within the facility where the system resides at in conjunction with facility officials and within limits as required by the equipment being protected; and
2) Monitor environmental control levels continuously in real time.

PE-15 – Water Damage Protection

For All Systems:

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.

PE-15(1) – Water Damage Protection | Automation Support

For High Systems:

1) Detect the presence of water near the system and alert the local physical security office and/or the facility management office using automated mechanisms.

PE-16 – Delivery and Removal

For All Systems:

1) Authorize and control all information system components entering and exiting the facility; and
2) Maintain records of the system components.

PE-17 – Alternate Work Site

For Moderate and High Systems:

1) Determine and document the Regional or Program Office alternate work sites allowed for use by employees;
2) Employ the following controls at alternate work sites: to the greatest extent possible the same controls required at the primary work environment to ensure the confidentiality, integrity and availability of EPA information and information systems;
3) Assess the effectiveness of controls at alternate work sites; and
4) Provide a means for employees to communicate with information security and privacy personnel in case of incidents.

PE-18 – Location of System Components

For High Systems:

Position system components within the facility to minimize potential damage from natural and man-made physical and environmental hazards and threats and to minimize the opportunity for unauthorized access.

6. ROLES AND RESPONSIBILITIES

The Information Security – Roles and Responsibilities procedure provides roles and responsibilities for personnel who have IT security or related governance responsibility for protecting the information and information systems they operate, manage and support.

7. RELATED INFORMATION

- Federal Identity, Credential and Access Management (FICAM)
- EPA Information Security Policy
- EPA Roles and Responsibilities Procedures

8. DEFINITIONS

- **Alternate Work Site:** a location other than the official duty station that has been approved by the personnel's supervisor (e.g., residence, satellite office, flexiplace) to perform job duties.
- **Authorization Credentials:** include, for example, badges, identification cards and smart cards. Organizations determine the strength of authorization credentials needed (including level of forge-proof badges, smart cards or identification cards) consistent with Federal standards, policies and procedures.
- **Electronic Data Storage:** storage that requires electrical power to store and retrieve that data.
- **Fire Detection Systems:** systems that are used to protect and evacuate people in emergencies. Examples include fire alarms, smoke, heat and carbon monoxide detectors, voice evacuation and mass notification systems and emergency lighting systems.
- **Fire Suppression Systems:** systems that are used in conjunction with smoke detectors and fire alarms to suppress a fire. Examples include wet and dry

sprinkler systems; fire extinguishers; and dry chemical, foam and gaseous extinguishing agents.

- **Flexiplace (aka: Flexible Workplace or Telecommuting):** refers to paid employment performed away from the office, either at home or at a satellite worksite location, for an agreed-upon portion of an individual's workweek.
- **Signature (of an individual):** a mark or sign made by an individual to signify knowledge, approval, acceptance or obligation (can be accomplished manually, sometimes referred to as a "wet signature," or electronically).
- **Written (or in writing):** to officially document the action or decision, either manually or electronically, and includes a signature.

9. WAIVERS

Waivers or deviations may be requested through the EPA Risk Determination Process based on a substantive business need and the implementation of compensating controls that provide a suitable alternative to the mandated protection.

Only EPA's Chief Information Officer may authorize Agency-wide waivers or deviations from the standards herein.

10. DIRECTIVE(S) SUPERSEDED

This procedure supersedes Information Directive: CIO 2150-P-11.2, Information Security – Interim Physical and Environmental Procedures.

11. CONTACTS

For information about this directive, please contact the Office of Mission Support (OMS), Office of Information Security and Privacy (OISP) at Infosec@epa.gov.

VAUGHN NOGA Digitally signed by VAUGHN NOGA
Date: 2023.12.19 13:56:06 -05'00'

Vaughn Noga, Chief Information Officer and Deputy Assistant Administrator for Information Technology and Information Management

APPENDIX A: ACRONYMS & ABBREVIATIONS

CIO	Chief Information Officer
CISO	Chief Information Security Officer
EPA	Environmental Protection Agency
FICAM	Federal Identity, Credential and Access Management
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Modernization Act
ISO	Information Security Officer
NARA	National Archives and Records Administration
NIST	National Institute of Standards and Technology
OISP	Office of Information Security & Privacy
OMB	Office of Management and Budget
OMS	Office of Mission Support
PE	Physical and Environmental Protection
PIV	Personal Identity Verification
POC	Point of Contact
SIO	Senior Information Official
SM	Service Manager
SO	System Owner
SP	Special Publication
U.S.C.	United States Code