Policy #:	Title:	Effective Date:
x.xx	Physical and Environmental Protection Policy	MM/DD/YY

PURPOSE

To ensure that Information Technology (IT) resources are protected by physical and environmental security measures that prevent physical tampering, damage, theft, or unauthorized physical access.

REFERENCE

National Institute of Standards and Technology (NIST) Special Publications (SP): NIST SP 800-53a – Physical and Environmental Protection (PE), NIST SP 800-46, NIST SP 800-73, SP NIST 800-76, SP NIST 800-78, SP NIST 800-116; Intelligence Community Directive (ICD): 704 705; Department of Defense (DoD): Instruction 5200.39 Critical Program Information (CPI) Protection; Federal Identity, Credential, and Access Management (FICAM) publication: Personal Identity Verification (PIV) in Enterprise Access Control System (E-PACS) (2012)

POLICY

This policy is applicable to all departments and users of IT resources and assets.

1. PHYSICAL ACCESS AUTHORIZATIONS
   IT Department shall:

   a. Develop, approve, and maintain a list of individuals with authorized access to the facilities where the information systems reside.

   b. Issue authorization credentials for facility access.

   c. Review the access list detailing authorized facility access by individuals and remove individuals from the facility access list when access is no longer required.

2. PHYSICAL ACCESS CONTROL
   IT Department shall:

   a. Enforce physical access authorizations by verifying individual access authorizations before granting access to the facility.

   b. Control ingress/egress to the facility using electronic access control systems (e.g., RFID card readers, biometric scanners), security guards, and video surveillance.

c. Maintain physical access audit logs for main entry/exit points, server rooms, data centers, and other sensitive areas, retained for a minimum of 90 days.

d. Provide physical barriers (e.g., locked doors, turnstiles, reception desks), surveillance cameras, and signage to control access to areas within the facility officially designated as publicly accessible.

e. Escort visitors and monitors visitor activity in estricted areas such as server rooms, IT equipment storage, and critical infrastructure zones. Visitors must sign in/out and wear visitor badges.

f. Secure keys, combinations, and other physical access devices.

g. Inventory all physical access devices (e.g., master keys, access badges, biometrics enrollment records) every 6 months, or upon significant staffing changes.

h. Change combinations and keys annually, and immediately if keys are lost, combinations are compromised, or individuals with access are transferred, terminated, or reassigned.

3. FACILITY PENETRATION TESTING
   IT Department shall:

   a. Employ a penetration testing process that includes annual, unannounced attempts to bypass or circumvent security controls associated with physical access points to the facility.

4. ACCESS CONTROL FOR TRANSMISSION MEDIUM
   IT Department shall:

   a. Control physical access to information system distribution and transmission lines (e.g., network cables, fiber optic lines, conduit paths) within entity facilities using locked conduits, secure cable trays, restricted access to telecommunications rooms, and video surveillance. Inspections shall be performed semi-annually to verify the integrity and security of these transmission mediums.
5. ACCESS CONTROL FOR OUTPUT DEVICES
   IT Department shall:

   a. Control physical access to information system output devices to prevent unauthorized individuals from obtaining the output.

      Controlling physical access to output devices includes, for example, placing output devices in locked rooms or other secured areas and allowing access to authorized individuals only, and placing output devices in locations that can

be monitored by personnel. Monitors, printers, copiers, scanners, facsimile machines, and audio devices are examples of information system output devices.

6. MONITORING PHYSICAL ACCESS
   IT Department shall:

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

   b. Review physical access logs at least monthly and upon occurrence of security incidents, unauthorized access attempts, or anomalies detected by surveillance systems; and coordinate results of reviews and investigations with the organizational incident response team.

7. VISITOR ACCESS RECORDS
   IT Department shall:

   a. Maintain visitor access records to the facility where the information system resides for a period of at least 12 months, in line with regulatory and auditing requirements; and review visitor access records on a monthly basis or in response to security incidents or audit requests.

8. POWER EQUIPMENT AND CABLING
   IT Department shall:

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

   b. Determine the types of protection necessary for power equipment and cabling employed at different locations both internal and external to organizational facilities and environments of operation. This includes, for example, generators and power cabling outside of buildings, internal cabling and uninterruptable power sources within an office or data center, and power sources for self-contained entities such as vehicles and satellites.

9. EMERGENCY SHUTOFF
   IT Department shall:

   a. Provide the capability of shutting off power to the information system or individual system components in emergency situations.

   b. Place emergency shutoff switches or devices in to facilitate safe and easy access for personnel; and protect emergency power shutoff capability from unauthorized activation.

10. EMERGENCY POWER
    IT Department shall:

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

    b. Provide a long-term alternate power supply for the information system that is capable of maintaining minimally required operational capability in the event of an extended loss of the primary power source.

11. EMERGENCY LIGHTING
    IT Department shall:

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

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

12. FIRE PROTECTION
    IT Department shall:

    a. Employ and maintain fire suppression and detection devices/systems for the information system that are supported by an independent energy source.

       This applies primarily to facilities containing concentrations of information system resources including, for example, data centers, server rooms, and mainframe computer rooms. Fire suppression and detection devices/systems include, for example, sprinkler systems, handheld fire extinguishers, fixed fire hoses, and smoke detectors.

13. TEMPERATURE AND HUMIDITY CONTROLS
    IT Department shall:

    a. Maintain temperature and humidity levels within the facility where the information system resides at manufacturer-recommended or industry-accepted levels, to ensure optimal operating conditions for IT equipment.

    b. Monitor temperature and humidity levels continuously using automated environmental sensors, with alerts configured in real-time to notify IT staff of deviations potentially harmful to personnel or equipment. Logs shall be retained for a minimum of 12 months to support incident analysis and compliance.

14. WATER DAMAGE PROTECTION
    IT Department shall:

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

       This applies primarily to facilities containing concentrations of information system resources including, for example, 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.

15. DELIVERY AND REMOVAL
    IT Department shall:

    a. Authorize, monitor, and control entering and exiting the facility and maintain records of those items delivered and removed from facility.

       Effectively enforcing authorizations for entry and exit of information system components may require restricting access to delivery areas and possibly isolating the areas from the information system and media libraries.

16. ALTERNATE WORK SITE
    IT Department shall:

    a. Employ security controls at alternate work sites.

    b. Assess as feasible, the effectiveness of security controls at alternate work sites.

    c. Provide a means for employees to communicate with information security personnel in case of security incidents or problems.

       Alternate work sites may include, for example, other government facilities or private residences of employees. While commonly distinct from alternative processing sites, alternate work sites may provide readily available alternate locations as part of contingency operations. Staff may define different sets of security controls for specific alternate work sites or types of sites depending on the work-related activities conducted at those sites.

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.

POLICY EXCEPTIONS

Requests for exceptions to this policy shall be reviewed by the Chief Information Security Officer (CISO) and the Chief Information Officer (CIO). Departments requesting exceptions shall provide such requests to the CIO. The request should specifically state the scope of the exception along with justification for granting the exception, the potential impact or risk attendant upon granting the exception, risk mitigation measures to be undertaken by the IT Department, initiatives, actions and a time-frame for achieving the minimum compliance level with the policies set forth herein. The CIO shall review such requests; confer with the requesting department.

RESPONSIBLE DEPARTMENT

Chief Information Office

DATE ISSUED/DATE REVIEWED

Date Issued:	MM/DD/YYYY
Date Reviewed:	MM/DD/YYYY