MARCO Federal Managed Computer Services

Cybersecurity Maturity Model Certification Initiative

Physical & Environmental Protection Policy

Document No

MOJVII-313-00

Effective Date	*Review Date*	*Version*	*Page No.*
02/15/2021	02/01/2021	3	1 of 12

Scope

Information Security Policies are the foundation for information technology security at MARCO-ONOPA JVII (MOJVII). The policies set out the information security standards required by NIST 800-171, which directs the Chief Information Officer (CIO) to establish a set of standards for information technology security to maximize the functionality, security, and interoperability of the distributed information technology assets, including, but not limited to, data classification and management, communications, and encryption technologies. This policy covers all information and information systems to include those used, managed, or operated by a contractor, an MOJVII, or other organization on behalf of MOJVII. This policy applies to all employees, contractors, and all other users of information and information systems that support the operation and assets of MOJVII. This is a living document subject to change in accordance with NIST SP 800-53 and CMMC v 1.02

Responsibilities

All covered personnel involved in the maintenance of information systems and supporting infrastructure are responsible for adhering to this policy and with any local physical and environmental security requirements.

Role	Definition
Senior Management	Senior Management (the Agency Head, the Chief Information Officer (CIO), the Chief Information Security Officer (CISO), or other designating organizational official) is responsible for the sponsorship and support of the Risk Management Plan and process, participating on the Risk Management Council, the review and approval of risk assessments and control recommendations and reporting to the SCRO what mitigation. actions have been taken.
Security Liaison	The Security Liaison is responsible for ensuring that physical and environmental risks are managed in compliance with MOJVII's requirements by collaborating with organizational entities. Liaisons are responsible for maintaining the appropriate operational security controls required for physical and environmental protection.
Facility Management	The Facility Manager, Facility Team, or other designated organizational official at management level, are responsible for site security and ensuring the facility is safe for occupancy. The Facility Manager may also have some responsibilities for authorization credentials, keys, physical access devices, etc.
Third Parties	Third party service providers are responsible for providing physical and environmental security in accordance with this policy.

PE-1 - Policy

All MOJVII information assets shall meet the required security controls defined in this policy document that are based on the National Institute of Standards and Technology (NIST) SP 800-53, Security and Privacy Controls. This document addresses the procedures and standards set forth by MOJVII to implement the family of Physical and Environmental Protection controls.

MOJVII has adopted the Identification and Authentication security principles established in

NIST SP 800-53, "Physical and Environmental Protection" control guidelines as the official policy for this security domain. The "PE" designator identified in each control represents the NIST-specified identifier for the Physical and Environmental Protection control family. The following subsections in this document outline the Physical and Environmental Protection requirements that each MOJVII shall implement and maintain in order to protect the privacy and security of sensitive information and to prevent the unauthorized use or misuse of MOJVII data. This policy shall be reviewed annually.

PE-2 – Physical Access Authorizations

MOJVII shall require that access to digital and non-digital media is restricted to authorized.

individuals only, using MOJVII-defined security measures.

a. MOJVII shall develop access policies for authorized individuals as well as visitors to MOJVII facilities.

b. Assessment of risk shall guide the selection of media, and associated information contained on that media requiring restricted access.

c. System Owners shall document policies and procedures for the media requiring restricted access, individuals authorized to access the media, and the specific measures taken to restrict access.

d. Authorization credentials (e.g., badges, identification cards, and smart cards) shall be issued to everyone accessing a restricted area.

    i. The level of access provided to everyone shall not exceed the level of access required to complete the individual's job responsibilities.

    ii. The level of access shall be reviewed and approved before access is granted.

    iii. Keys, badges, access cards, and combinations shall be issued to only those personnel who require access.

    iv. Everyone within a building must display either a MOJVII Identification (ID) Badge or a numbered and current visitor badge. These badges are the property of MOJVII and are provided to employees and visitors as a convenience.

    v. Badges must always be visible.

    vi. Keys, combinations, and other physical access devices shall be always secured to prevent unauthorized access to MOJVII facilities and assets. These shall also be inventoried on an MOJVII-defined frequency.

    vii. The unauthorized duplication of keys is prohibited. All requests for duplicate keys shall be submitted to MOJVII locksmith for review, approval, and fulfillment.

    viii. Keys shall be retrieved from the employee when they retire, terminate employment, or transfer to another position.

    ix. Keys and combinations shall be changed at least annually for secure areas housing systems with FTI data.

x. Authorizations and requirements for access shall be coordinated with facility and personnel security managers, as required or needed.

e. Access lists and authorization credentials shall be reviewed and approved quarterly to ensure the following:

   i. Access shall be limited to only authorized personnel.

   ii. The level of access provided to everyone shall be consistent with the individual's job responsibilities.

   iii. Access rights shall be promptly removed for terminated and transferred personnel or for personnel no longer requiring access to the facility where the information system resides.

f. Enforce physical access authorizations to the information system in addition to the physical access controls for the facility at spaces where restricted or highly restricted data is received, processed, stored, or transmitted.

PE-3 – Physical Access Control

MOJVII shall carefully evaluate sites and facilities that will be staffed and will house information technology equipment to identify and implement suitable controls to protect staff and MOJVII resources from environmental threats, physical intrusion and other hazards and threats.

a. Each MOJVII shall safeguard sites, buildings and locations housing its information technology assets.

b. All locations that house restricted or highly restricted data shall be designed and secured in accordance the information being protected.

c. Physical access authorizations at entry/exit points to facilities where the information systems that receive, process, store, or transmit restricted or highly restricted data reside shall be enforced by the following:

   i. Verifying individual access authorizations before granting access to the facility.

d. Controlling ingress/egress to the facility using physical access control systems/devices or guards. Authorized individuals may include MOJVII employees, contractors, vendors, and customers.

e. Physical access controls should include some form of visible identification such as a Driver License or some other picture identification, i.e. MOJVII badge.

f. An audit trail of physical access for all individuals to data centers shall be maintained including entry and exit dates and times.

   i. MOJVII shall control the number of people who have physical access to areas housing computer equipment to reduce the threats of theft, vandalism, and unauthorized system access. MOJVII should consider the following measures to control and restrict access to computing facilities:

   ii. Access shall be restricted to people with authorized purposes for visiting the computer area.

iii. Instructions shall be issued to visitors explaining security requirements and emergency procedures.

iv. Visitors shall be escorted and should wear visible identification that clearly draws attention to their restricted status.

v. Where appropriate, MOJVII shall store resources in lockable storage cupboards where the physical security controls are sufficient to protect the equipment from theft.

vi. MOJVII shall use lockable file cabinets to store restricted or highly restricted data such as paper documents and computer media in a manner that is commensurate with the information's classification status.

g. Video cameras and/or access control mechanisms shall be used to monitor individual physical access to sensitive areas.

h. The use of personal cameras, video recorders and mobile computing devices shall be restricted from high security locations to protect the information being stored.

i. Duress alarms shall be used in areas where the safety of personnel is a concern. Alarms shall be provisioned to alert others such as staff, the police department, the fire department, etc.

j. Videoconference calls where restricted or highly restricted information will be discussed shall be made in an area that is secured (i.e., offices or conference rooms where the door can be closed, and conversations cannot be overheard through thin walls).

k. Facilities that will house restricted or highly restricted data shall include, but not limited to, the following security measures:

i. Clearly defined, layered security perimeters to establish multiple barriers.

ii. Walls (of solid construction and extending from real ceiling to real floor where necessary)

iii. Card-controlled gates and doors

iv. Bars, alarms, locks, etc.

v. Bollards

vi. Video cameras and intrusion security system

vii. Staffed reception desk

viii. Fire doors on a security perimeter shall be equipped with alarms as well as devices that close the doors automatically.

PE-4 - Access Control for Transmission Medium

MOJVII shall control physical access to information system distribution and transmission lines within MOJVII facilities:

a. Protective measures to control physical access to information system distribution and transmission lines shall include the following:

i. Locked wiring closets

ii. Disconnected or locked spare network jacks

iii. Protection of cabling by conduit or cable trays

b. Publicly accessible network jacks in data centers shall provide only Internet access by default unless additional functionality is explicitly authorized.

c. Physical access to networking equipment and cabling shall be restricted to authorized personnel.

PE-5 - Access Control for Output Devices

MOJVII shall control physical access to information system output devices, such as computer monitors, facsimile machines, copiers and printers, to prevent unauthorized individuals from obtaining the output:

a. Where technically configurable, enable security functionality on printers, copiers and facsimile machines that requires users to authenticate with the device via a PIN or hardware token in order to access the device.

b. Control physical access to output devices by placing devices in controlled areas with keypad access controls or limiting access to individuals with certain types of badges.

c. Control physical access to monitors through the uses of privacy screens or by re-positioning monitors away from view by unauthorized users.

d. This control is optional for LOW-risk information systems.

PE-6 – Monitoring Physical Access

MOJVII shall ensure that physical access to information systems shall be monitored to detect and respond to physical security incidents:

a. Coordination with facility management and personnel security management personnel shall occur when responsibilities are in different organizations.

b. Physical access logs shall be reviewed at least semi-annually by the MOJVII Security Liaison or other designated MOJVII official at management level.

c. Investigations of apparent security violations or suspicious physical access activities shall be conducted. Investigations and results of reviews shall be coordinated with the MOJVII's incident response capability:

   i. Remedial actions identified because of investigations shall be developed and implemented.

   ii. Incident investigations shall follow the Incident Response Policy MOJVII-308 for requirements on incident response.

d. Investigation of and response to detected physical security incidents, including apparent security violations or suspicious physical access activities shall be part of the MOJVII's incident response procedures.

e. Operational procedures shall be developed to document how these individuals shall respond to physical access incidents.

PE-6– Monitoring Physical Access – Intrusion Alarms / Surveillance Equipment (Moderate Control)

Physical intrusion alarms and surveillance equipment shall be installed and monitored. Automated mechanisms to recognize potential intrusions and initiate designated response actions shall be employed.

PE-7 – Visitor Control

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

PE-8 – Visitor Access Records

MOJVII shall actively monitor the security access logs of areas housing information technology equipment:

a. Visitor access records for MOJVII owned computing facilities shall address the following requirements:
   i. Name and organization of the person visiting.
   ii. Signature of the visitor
   iii. Picture ID has been verified, and by whom, i.e., guard's initials
   iv. Date of access
   v. Time of entry and departure
   vi. Purpose of visit
   vii. Name of person visited.
   viii. The visitor access records shall be reviewed at least semi-annually.

b. Visitor access records for facilities housing FTI shall be maintained for five (5) years. All other facilities access records shall comply with records retention policies.

PE-9 – Power Equipment and Cabling

MOJVII shall protect power equipment and cabling for information systems from damage and destruction:

a. MOJVII shall employ multiple electric feeds to avoid a single point of failure in the power supply that are physically separated to help ensure that power continues to flow in the event one of the cables is cut or otherwise damaged.
b. Both power and communication lines should be protected.
c. MOJVII shall employ automatic voltage controls for critical system components to help ensure that power continues to flow in the event voltage fluctuates to unacceptable levels and causes damage to the information system component.
d. This control is optional for LOW-risk information systems.

PE-10 – Emergency Shutoff

MOJVII shall provide the capability of shutting off power to the information system or individual system components in emergency situations.

a. MOJVII shall locate emergency power switches near emergency exits in equipment rooms to facilitate rapid power down in case of an emergency.

b. The locations for emergency power shutoffs must be documented.

c. All necessary personnel must be informed of the emergency power shutoff locations and they must be trained to operate them safely.

d. Emergency procedures must be readily available to relevant personnel.

e. The emergency power-off capability must be protected from accidental or unauthorized activation.

f. Emergency shutoff switches are located in a visible location and clearly labeled.

g. This control is optional for LOW-risk information systems.

PE-11 – Emergency Power

MOJVII shall protect critical information technology systems from damage and data loss by installing and routinely testing a source of continuous power that ensures that the systems continue to perform during power outages and electrical anomalies (e.g., brownouts and power spikes):

a. The three primary methods for providing continuous power are as follows:
    i. Multiple electric feeds to avoid a single point of failure in the power supply.
    ii. Uninterruptible power supply (UPS)
    iii. Backup generator(s)

b. Each MOJVII shall examine the availability requirements for critical equipment and determine which combination of these three methods best meets the needs of the MOJVII.

c. MOJVII shall analyze the emergency power requirements for critical systems based on the following best practices:
    i. Use of a UPS is usually required to avoid abnormal shutdowns or to provide a clean power source during brownouts or surges. **Note**: Most UPS batteries do not last for more than four (4) hours without a continuous supply of power.
    ii. Contingency plans that include procedures to follow if the UPS fails.
    iii. Periodic inspections of UPS equipment to ensure that the equipment has the ability to sustain, for a predefined period, the power load of the systems and equipment it supports and is serviced according to the manufacturer's specifications.

d. Backup generators shall be used in combination with an UPS when requirements demand high availability and continuous processing in the event of a prolonged power failure. Such a combination both supports an orderly shutdown if the generator fails, minimizing potential for equipment damage or data loss, and can also provide continuous business operations if the cutover to the generator is too slow to provide power immediately with

no interruption. MOJVII that require a backup generator should ensure the following:

i. Contingency plans shall include procedures to follow in the event the backup generator fails.

ii. Ensure the generator has the capacity to sustain the power load required by supported equipment for a prolonged period.

iii. Ensure the generator is tested at least quarterly according to the manufacturer's specifications.

iv. The generator is serviced regularly in accordance with the manufacturer's specifications, and it has an adequate supply of fuel.

v. An adequate supply of fuel is available to ensure that the generator can perform for a prolonged period.

e. This control is optional for LOW-risk information systems.

PE-12- Emergency Lighting

MOJVII shall provide emergency lighting in case of a main power failure:

a. Automatic emergency lighting that activates in the event of a power outage or disruption and that covers emergency exits and evacuation routes within the facility shall be employed and maintained.

b. The automatic emergency lighting systems shall be tested annually to ensure they are fully operational.

c. The results of the test shall be documented.

PE-13 – Fire Protection

MOJVII shall have security controls to assure continual service of critical production systems, including controls that alert, monitor, and log intrusions, fires, explosives, smoke, water, dust, vibrations, chemicals, and electrical effects, electrical supply interferences, and electromagnetic radiation. This control applies primarily to facilities containing concentrations of information system resources including, for example, data centers, server rooms, and network closets:

a. Where appropriate, MOJVII shall provide fire-resistant storage for documents and media containing information critical to their business function.

b. Most file cabinets are not fire, smoke, or water safe and a fire-proof safe may not be water safe and may render any information that is stored in the cabinet or safe unusable; therefore, MOJVII shall consider storing duplicate copies of information at alternate locations.

c. Fire extinguishers must be checked annually and the inspection date must be documented on the extinguisher.

d. All fire protection resources must be tested annually in accordance with local or state fire regulations to ensure they can be successfully activated in the event of a fire.

PE-13 (3) – Fire Protection – Automatic Fire Suppression (Moderate Control)

a. MOJVII shall install and maintain fire detection and suppression devices that are supported by an independent power source, such as a dry pipe sprinkler system.

b. Fire detection devices/systems should activate automatically and notify emergency personnel and defined emergency responder(s) in the event of a fire when the facility is not staffed on a continuous basis.

PE-14 – Temperature and Humidity Controls

a. MOJVII shall implement and maintain automatic temperature and humidity controls in the data center(s) to prevent fluctuations potentially harmful to equipment.

b. MOJVII shall employ temperature and humidity monitoring that provide an alarm or other notification of when temperature and humidity settings are exceeded due to heating, ventilation, or air conditioning (HVAC) failures and may adversely impact information assets.

PE-15 –Water Damage Protection

a. MOJVII shall include measures to prevent water damage in the design requirements for secure data storage.

b. The facility must have master shutoff valves that are accessible, working properly, and known to key personnel, to protect the information system from damage resulting from water leakage.

PE-16 – Delivery and Removal

MOJVII shall ensure that access to delivery areas (e.g. loading docks and warehouses) is restricted and possibly isolated from the information system and media libraries in order to effectively enforce authorizations for entry and exit of information system components.

a. All types of information system components and packages that are delivered to or removed from the facility shall be authorized, monitored, and controlled.

b. Records of those items entering and exiting the facility shall be maintained.

PE-17 – Alternate Work Site

MOJVII shall provide readily available alternate work locations (e.g. governmental offices, commercial locations, employee homes, etc.) as part of contingency operations:

a. The security controls at alternate work sites shall be assessed, as feasible. Alternate work sites shall be equipped with any equipment needed to resume temporary operations such as telecommunications services such as alternative telephone services, wireless, satellite, radio that will allow employees to communicate with information security personnel in case of security incidents or problems.

b. MOJVII shall secure and protect communications with MOJVII information resources while personnel are working at off-site locations. Remote access security requirements are defined in the Access Control Policy, Section AC-17 – Remote Access.

c. Alternate work sites must meet state and federal security control requirements. If the MOJVII does not have direct control over the remote location, the MOJVII shall enter a contract with the owner of the remote location that stipulates the access controls and protection the owner shall implement. The following shall be implemented for alternate work sites:

   i. The perimeter security and physical access controls to the site and to the MOJVII's data store.

   ii. Design requirements for secure data storage (*i.e.*, fire suppression and detection equipment, heating, ventilation, and air conditioning [HVAC], measures to prevent water damage, etc.).

   iii. Equipment being used or stored at an individual alternate work site, such as hotel, home, or other alternate site, must be secured when not in use.

   iv. Equipment transported in vehicles must be hidden from casual view.

   v. Equipment must not be stored in vehicles overnight.

   vi. NIST SP 800-46, Revision 1 must be used as guidance for security in telework and remote access.

d. This control is optional for LOW-risk information systems.

PE-18 – Location of Information System Components

The MOJVII must position information system components within the facility to minimize potential damage from physical and environmental hazards and to minimize the opportunity for unauthorized access. This control is optional for LOW-risk information systems.

PE-19 – Information Leakage (Optional Control)

This control is optional for LOW and MODERATE risk information systems.

PE-20 – Asset Monitoring and Tracking (Optional Control)

This control is optional for LOW and MODERATE risk information systems.

Enforcement

Violations of this policy or failure to implement provisions of this policy may result in disciplinary action up to and including termination, civil litigation, and/or criminal prosecution.

Material Superseded

This current policy supersedes all previous versions of the policy. All MOJVII and vendors of MOJVII are expected to comply with the current implemented version of this policy.

APPROVAL SIGNATURES PAGE
Information Technology Department (ITDEPT)

MOJVII OFFICERS	SIGNATURE	DATE
CIO		
CSO		
CEO		
IASO: