



MARCO Federal Managed Computer Services



Cybersecurity Maturity Model Certification Initiative



Contingency Planning Policy

Document No
MOJVII-306-00

<i>Effective Date</i>	<i>Review Date</i>	<i>Version</i>	<i>Page No.</i>
02/15/2021	02/01/2021	3	1 of 10

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 the. This policy applies to all employees, contractors, and all other users of information and information systems that support the operation and assets of the. This is a living document subject to change in accordance with NIST SP 800-53 and CMMC v 1.02

Responsibilities

All covered personnel who utilize MARCO-ONOPA JV II IT resources are responsible for adhering to this policy and any local Access Control requirements.

Role	Definition
MOJVII Management	Chief Information Officer (CIO), and the Chief Information Security Officer (CISO), are assigned the responsibility for ensuring that the goals and requirements of the Access Control Policy are met.
Information Security	The Information Security function is responsible for the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction to provide confidentiality, integrity, and availability
MOJVII Security Liaison	MOJVII Security liaison is responsible for ensuring that security risks are managed in compliance with the requirements by collaborating with organizational entities.

Covered Personnel	Covered personnel are required to understand their security responsibilities and have the requisite skills and knowledge to ensure the effective execution of the roles they are assigned to reduce the risk of unauthorized access, use or modification of IT Resources (theft, fraud, or misuse of facilities).
Third Parties	Third party service providers must ensure that all IT systems and applications developed for the MOJVII conform to this and other applicable Enterprise Information Technology Policies, Standards and Procedures. Non-conforming IT systems cannot be deployed unless the purchasing entity and their contractor have jointly applied for and received, in writing from the CIO or designee, notice that a specified exception will be permitted.

All MOJVII information assets must 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 requirements set forth by MOJVII to implement the family of Contingency Planning security controls.

MOJVII must develop, adopt and adhere to a formal, documented contingency planning procedure that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. The appropriate level of information technology business continuity management must be in place to sustain the operation of critical information technology services to support the continuity of vital business functions and the timely delivery of critical automated business services to MOJVII's customers.

Appropriate planning and testing processes must be in place to ensure that, in the event of a significant business interruption, critical production environments can be recovered and sustained to meet business requirements. To facilitate the effective recovery of systems and compliance with this policy, coordination is required between the Department of Information Technology (DIT), MOJVII business units. This policy covers mainframe, distributed environments, and cloud-hosted environments, e.g. Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), Software-as-a-Service (SaaS).

MOJVII has adopted the Contingency Planning security principles established in NIST SP 800-53, "Contingency Planning" control guidelines as the official policy for this security domain. The "CP" designator identified in each control represents the NIST-specified identifier for the Contingency Planning control family. The following subsections in this document outline the Contingency Planning requirements that MOJVII must implement and maintain in order to be compliant with this policy. This policy shall be reviewed annually, at a minimum.

CP-2 – Contingency Plan

MOJVII's information assets must be available to authorized users when needed. MOJVII are required to manage information technology risks appropriately as required in state and federal laws. MOJVII must develop a contingency plan/disaster recovery plan for the recovery of information assets for which MOJVII is named as owner for all known threats to availability, including natural disasters, accidents, malicious destruction, failures, and denial of services. Management shall coordinate contingency plan development with organizational elements responsible for formally documenting the Business Continuity (BC) & Disaster Recovery (DR) Plan that covers all of MOJVII's critical applications, and includes procedures or references to procedures to be used for the recovery of systems that perform MOJVII's essential mission and critical business processes.

Application criticality has the following four categories (Definitions may be found in MOJVII Glossary of Information Technology Terms):

- i. MOJVIIwide Critical
- ii. Department Critical
- iii. Program Critical
- iv. Non-Critical

MOJVII Critical systems must provide disaster recovery capabilities to ensure timely recover

and restoration of service as part of their disaster recovery strategy. MOJVII must coordinate contingency plan development and execution with MOJVII divisions and groups responsible for related plans. Plans related to contingency plans for MOJVII information systems include, for example, Business Continuity Plans, Disaster Recovery Plans, Continuity of Operations Plans, Crisis Communications Plans, Critical Infrastructure Plans, Cyber Incident Response Plans, Insider Threat Implementation Plan, and Occupant Emergency Plans.

MOJVII plans must include the following:

- a. Be developed prior to implementation as part of the development life cycle for technology development or deployment by MOJVII to address all production processing environments and assets.
- b. Identify essential missions and business functions and associated contingency requirements.
- c. Provide recovery time and recovery point objectives, restoration priorities, and metrics; and estimate the following three downtime factors for consideration as a result of a disruptive event:
 - i. Maximum Tolerable Downtime (MTD) - The amount of time mission/business process can be disrupted without causing significant harm to the organization's mission.
 - ii. Recovery Time Objective (RTO) - RTO defines the maximum amount of time that a system resource can remain unavailable before there is an unacceptable impact on other system resources, supported mission/business functions, and the MTD.
 - iii. Recovery Point Objective (RPO) - The RPO represents the point in time, prior to a disruption or system outage, to which mission/business process data shall be recovered (given the most recent backup copy of the data) after an outage.
- d. Identify contingency roles, responsibilities, assigned individuals with contact information.
- e. Address eventual, full information asset restoration without deterioration of the security measures originally planned and implemented.
- f. Be reviewed and approved by designated officials within MOJVII.
- g. Be distributed to relevant system owners and stakeholders.
- h. Coordinate contingency planning activities with incident handling activities.
 - i. Be revised to address changes to the organization, information asset, or environment of operation and problems encountered during contingency plan implementation, execution, or testing.
- j. Protect the contingency plan from unauthorized disclosure and modification.
- k. Address the protection of the health and safety of the employees of MOJVII.
- l. Address the protection of assets of MOJVII and minimize financial, reputational, legal and/or regulatory exposure.
- m. Create crisis teams and response plans for threats and incidents.
- n. Require that employees are made aware of their roles and responsibilities in the BC/DR Plan and in plan execution through training and awareness programs.
- o. Coordination with Contingency Plan Administrators and the Operations Team must occur for all potential outages that may result in a failover or recovery situation.

- p. Be reviewed and submitted to MOJVII CIO on an annual basis, and as otherwise requested by MOJVII CIO.
- q. Support the resumption of essential missions and business functions within MOJVII-defined time period of contingency plan activation.
- r. Define the time period for resumption of essential mission/business functions dependent on the severity/extent of disruptions to the information system and its supporting infrastructure.
- s. Define within the contingency plan and Business Impact Analysis (BIA) the time period in which the system needs to be operational to support essential mission and business functions.

CP-3 – Contingency Plan Training

MOJVII must train personnel in their contingency roles and responsibilities with respect to the information assets. Training and awareness programs shall ensure that MOJVII understands the roles each individual within MOJVII in a disaster/or adverse situation. The MOJVII must provide contingency training to information system users for the following conditions:

- i. Prior to assuming a contingency role or responsibility,
- ii. When required by information system changes,
- iii. Annually thereafter.

CP-4 – Contingency Plan Testing and Exercises

MOJVII must coordinate contingency plan testing with MOJVII divisions and groups responsible for related plans. MOJVII must do the following:

- a. Develop test objectives and success criteria to enable an adequate assessment of the Disaster Recovery and/or Restoration procedures.
- b. Test and/or exercise the contingency plan for the critical information assets annually, at a minimum, in order to determine the plan’s effectiveness and the organization’s readiness to execute the plan.
- c. Develop a contingency plan exercise after action report.
- d. Initiate corrective actions to ensure the procedures are adequate to restore/recover critical application processes.

Table 1 – Test Types

Test Type	Description
Walk-Through	A participatory session featuring an oral walk-through of the technology recovery plan and of the specific tasks documented within the plan. This exercise should confirm the plan’s design and identify role and responsibility gaps or other weaknesses in the plan. This type of exercise can be used on alternating years between more complete testing for lower criticality systems.
Table-Top	A participatory session using example interruptions led by a facilitator to test the integrity of the disaster recovery plan as well as the readiness of the participating staff to respond to an adverse event.

Stand-Alone	Tests one or more specific components of a technology recovery plan in isolation from other components. Focuses on data restoration with network connectivity and is usually limited to a single platform or system. It may or may not include testing application interdependencies.
Partial Integration	Tests one or more specific components of a technology recovery plan. Includes testing data restoration with network connectivity and testing some interdependencies with applications and/or platforms.
Full End-to-End	Tests the technology recovery plan in a technology recovery testing environment without risk to the production environment, tests all components of the technology recovery plan and all functionality of an application. Includes testing transactions and testing all interdependencies with other applications and/or platforms. Tests shall be conducted at alternate sites or other recovery arrangements of the testing organization, personnel, equipment, facilities and processes.

CP-5 – Contingency Plan Update

Withdrawn: Incorporated into CP-2.

CP-6 – Contingency Plan Alternate Storage Site

MOJVII must establish an alternate storage site for systems that are defined as critical including necessary agreements to permit the storage and recovery of information asset backup information. MOJVII must do the following:

- a. Ensure that the alternate storage site provides information security safeguards that meet the comparable protection standards of the primary site.
- b. Establish a site in a location that is separate from the primary facility to ensure that the risk of a disruption (e.g. natural disasters, structural failures, hostile cyber attacks) affecting both the primary and alternate site is low or otherwise is at an acceptable level, based on an assessment of risk.
- c. Identify potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster and outlines explicit mitigation actions. Area-wide disruptions refer to those types of disruptions that are broad in geographic scope (e.g., hurricane, regional power outage) with such determinations made by MOJVII based on MOJVII assessments of risk. Explicit mitigation actions include, for example:
 - i. Duplicating backup information at other alternate storage sites if access problems occur at originally designated alternate sites;
 - ii. Planning for physical access to retrieve backup information if electronic accessibility to the alternate site is disrupted.
- d. This control is optional for LOW risk information systems.

CP-7 – Contingency Plan Alternate Processing Site

MOJVII must do the following:

- a. Establish an alternate processing site including necessary agreements to permit the resumption of information asset operations for essential missions and business functions within defined recovery times and recovery points when the primary processing capabilities are unavailable. Alternate processing sites shall provide a Service Level Agreement (SLA) that contains priority- of-service provisions in accordance with the information system's requirements in the event of a disruption or disaster. This may be in the form of a priority-of-service provision or through a provider with a sufficient network of facilities to ensure available capacity.
- b. Ensure that equipment and supplies required to resume operations are available at the alternate site or contracts are in place to support delivery to the site in time to support MOJVII-defined time period for transfer/resumption.
- c. Ensure that the alternate storage site provides information security safeguards that meet the comparable protection standards of the primary site.
- d. Identify an alternate processing site that is separated from the primary processing site to reduce susceptibility to the same threats.
- e. Determine what is considered a sufficient degree of separation between primary and alternate processing sites based on the types of threats that are of concern.
- f. Identify potential accessibility problems to the alternate processing site in the event of an area-wide disruption or disaster.
- g. Outline and document explicit mitigation actions within the contingency plan.
- h. Develop alternate processing site agreements that contain priority-of-service provisions in accordance with MOJVII availability requirements (including recovery time objectives). Priority- of-service agreements refer to negotiated agreements with service providers that ensure that MOJVII receive priority treatment consistent with their availability requirements including defined RTO and RPO objectives as defined in the business impact analysis (BIA) and contingency plan.
- i. This control is optional for LOW risk information systems.

CP-8 – Telecommunications Services

MOJVII must do the following:

- a. Establish alternate telecommunications services with telecommunication service providers that provide communications transmission services to maintain a state of readiness or to respond to and manage any event or crisis.
- b. Communications transmission services must include necessary agreements to permit the resumption of information asset operations for essential missions and business functions within defined recovery time and recovery points when the primary telecommunications capabilities are unavailable.
- c. Develop primary and alternate telecommunications service agreements that contain priority-of- service provisions in accordance with MOJVII availability requirements (including

recovery time objectives).

- d. Request Telecommunications Service Priority for all telecommunications services used for national security emergency preparedness if the primary and/or alternate telecommunications services are provided by a common carrier.
- e. Consider the potential mission/business impact in situations where telecommunications service providers are servicing other organizations with similar priority-of-service provisions.
- f. Obtain alternate telecommunications services to reduce the likelihood of sharing a single point of failure with primary telecommunications services.
- g. This control is optional for LOW risk information systems.

CP-9 – Information System Backup

MOJVII must conduct backups of system-level information, such as operating system files and application software from MOJVII managed laptops, workstations, servers, and user level information, such as user level files stored on a shared network drive, at a frequency that is consistent with MOJVII defined recovery time objectives (RTO), and Recovery Point (RPO) objectives. In addition, MOJVII must protect the confidentiality and integrity of backup information at storage location(s).

CP-9 (1) – Information System Backup – Testing for Reliability/Integrity (Moderate Control)

MOJVII must test backup information quarterly to verify media reliability and information integrity.

CP-10 – Information System Recovery and Reconstitution

MOJVII must do the following:

- a. Provide for the recovery and reconstitution of MOJVII's mission essential function(s)/processes and/or critical business services, including transaction-based information systems, to a known state after a disruption, compromise, or failure within defined RTO and RPO objectives.
- b. Applications categorized as MOJVIIwide and or Department critical are recommended to have viable disaster recovery support, approval, budget in place, and be exercised according to policy.
- c. Ensure plan activations are documented and recorded, and post-activation reviews are conducted to evaluate the effectiveness of the plan(s).
- d. Update the plan(s) where necessary, and provide a formal report to MOJVII CIO within 30 days of post-activation review.

CP-11 – Alternate Communication Protocols (Optional)

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

CP-12 – Safe Mode (Optional)

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

CP-13 – Alternative Security Mechanisms (Optional)

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 State agencies 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:		

