MARCO Federal Managed Computer Services

Cybersecurity Maturity Model Certification
Initiative

Risk Assessment Policy

Document No

MOJVII-314-00

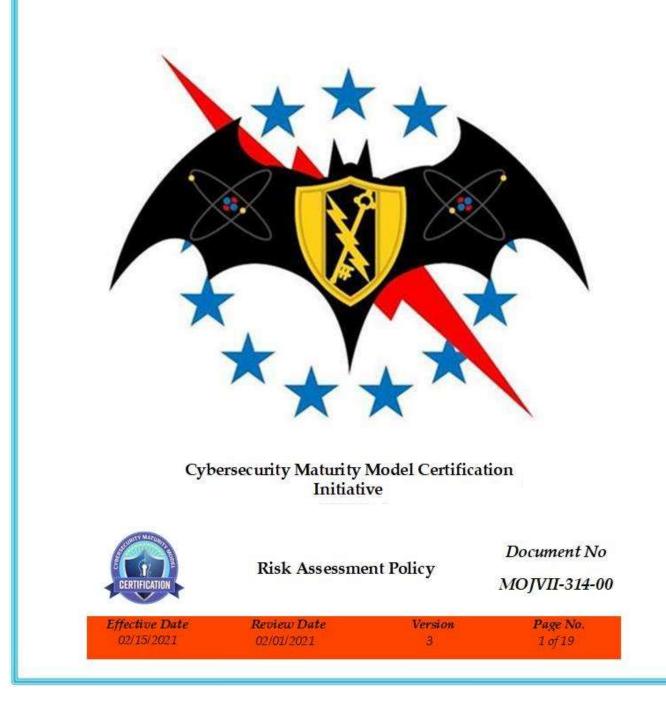| *Effective Date*	*Review Date*	*Version*	*Page No.*
02/15/2021	02/01/2021	3	1 of 19

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

This policy document provides the MOJVII risk assessment policy statements and commitment to develop, implement, maintain a Risk Assessment Policy, conduct annual risk and security assessments on all State information systems to help understand and identify all current threats, vulnerabilities and gaps within their process that may create critical risks availability, confidentiality and integrity for information systems and data of which the State is considered the owner.

Responsibilities

All covered personnel that are included in IT risk assessment activities are responsible for adhering to this policy and with any local Risk Assessment requirements.

System Owner / Administrator	System Owners/Administrators are responsible for participating in the identification and analysis process, participating on the Risk Management Council and for the implementation of technical controls.
Functional Managers	Managers in the functional areas are responsible for participating in the risk identification and analysis process, providing some participation on the Risk Management Council, and for the implementation of administrative controls.

RA-1 - Policy

All MOJVII information assets must meet the required security controls defined in this policy document that are based on the NIST SP 800-53, Security and Privacy Controls. Agencies shall manage risks appropriately. Risk management includes the identification, analysis, and management of risks associated with an MOJVII's business, information technology infrastructure, the information itself, and physical security to protect MOJVII's information technology assets and vital business functions:

a. MOJVII, through its management, must implement an appropriate Information Technology (IT) Risk Management Program to ensure the timely delivery of critical automated business services to MOJVII end-users.

b. The risk management program must identify and classify risks and implement risk mitigation as appropriate.

c. The program must include the identification, classification, prioritization, and mitigation processes necessary to sustain the operational continuity of mission critical information technology systems and resources.

d. In general, "risk" is defined as a condition or action that may adversely affect the outcome of a planned activity. Some types of risk are as follows:

   i. Business risk – The cost of and/or lost revenue associated with an interruption to normal business operations.

   ii. Organizational risk – The direct or indirect loss resulting from one or more of the following:

      1. Inadequate or failed internal processes.
      2. People
      3. Systems or external events

   iii. IT risk – The loss of an automated system, network or other critical information technology resource that would adversely affect business processes.

   iv. Legal risk – Parameters established by legislative mandates, federal and state regulations, policy directives and executive orders that impact delivery of program services.

   v. Reputational risk – General estimation, by the public, on how MOJVII services are delivered (integrity, credibility, trust, customer satisfaction, image, media relations, political involvement).

   vi. Citizen Services risk – Program services mandated by charter, legislation, or policy that provides for the delivery of MOJVII's business (education, human services, highways, law enforcement, health and safety, unemployment benefits, vital records, etc.).

MOJVII has developed a Continuous Monitoring Plan which requires that all agencies complete an annual risk and security assessment of their critical systems and infrastructure and that there are ongoing processes in place to assess the current posture of the environment. The Continuous Monitoring Plan is designed as a three-year program to ensure that all agencies are assessed using one or a combination of assessment methods identified below:

a. Third Party Independent Assessment
b. Self-Assessment

All agencies must complete a risk and security assessment annually. It is the MOJVII's responsibility to ensure that an appropriate budget amount is requested to meet the ends of the legislative mandate. The Department of Information Technology (DIT), MOJVII IT may conduct compliance readiness reviews with the Executive Branch agencies to validate cyber readiness.

Within 30 days of completion of an assessment, all agencies are required to provide MOJVII IT with the results and submit a plan to remediate the findings in the Enterprise Governance, Risk and Compliance (EGRC) tool. This tool will be used to create and maintain corrective actions plans for those deficiencies noted during a risk assessment, including vulnerability scans, and will ensure:

a. Accurate reporting on the status of corrective actions
b. Development of a process to evaluate supporting documentation and the time to monitor recommendations.

Agencies shall coordinate with MOJVII IT to address residual risks for those controls that cannot be implemented.

The MOJVII has adopted the Risk Assessment security principles established in NIST SP 800-53, "Risk Assessment" control guidelines as the official policy for this security domain. The "RA" designator identified in each control represents the NIST-specified identifier for the Risk Assessment control family. The following subsections in this document outline the Risk Assessment

requirements that the MOJVII and each MOJVII must implement and maintain to be compliant with this policy. This policy shall be reviewed annually.

Risk Management Program Activities:

The Risk Management program at a minimum shall focus on the following four types of activities:

a. **Identification of Risks**: A continuous effort to identify which risks are likely to affect business continuity and security functions and documenting their characteristics.

b. **Analysis of Risks**: An estimation of the probability, impact, and timeframe of the risks, classification into sets of related risks, and prioritization of risks relative to each other.

c. **Mitigation Planning**: Decisions and actions that will reduce the impact of risks, limit the probability of their occurrence, or improve the response to a risk occurrence. For moderate or high rated risks, mitigation plans should be developed, documented, and assigned to managers. Plans should include assigned manager's signatures.

d. **Tracking and Controlling Risks**: Collection and reporting of status information about risks and their mitigation plans, response to changes in risks over time, and management oversight of corrective measures taken in accordance with the mitigation plan.

Business Continuity Risk Management Processes:

For business continuity risk management, the focus of risk management is an impact analysis for those risk outcomes that disrupt MOJVII business. Agencies should identify the potential impacts in order to develop the strategies and justify the resources required to provide appropriate level of continuity initiatives and programs. Agencies should conduct business risk impact analysis activities that include the following:

a. Define the MOJVII's critical functions and services.

b. Define the resources (technology, staff, and facilities) that support each critical function or service.

c. Identify key relationships and interdependencies among the MOJVII's critical resources, functions, and services.

d. Estimate the decline in effectiveness over time of each critical function or service.

e. Estimate the maximum elapsed time that a critical function or service can be inoperable without a catastrophic impact.

f. Estimate the maximum amount of information or data that can be lost without a catastrophic impact to a critical function or service.

g. Estimate financial losses over time of each critical function or service.

h. Estimate tangible (non-financial) impacts over time of each critical function or service.

i. Estimate intangible impacts over time of each critical function or service.

j. Document any critical events or services that are time-sensitive or predictable and require a higher- than-normal priority (For example - tax filing dates, reporting deadlines, etc.)

k. Identify any critical non-electronic media required to support the MOJVII's critical functions or services.

l. Identify any interim or workaround procedures that exist for the MOJVII's critical functions or

services.

m. Assess the professional capability of third parties and ensure that they provide adequate contact with the agencies and meet the MOJVII's RTO and RPO requirements. Review dependence on third parties and take actions to mitigate risk.

n. Provide direction on synchronization between any manual work data and the automated systems that occur during a recovery period.

Security Risk Process:

The focus of security risk management is an assessment of those security risk outcomes that may jeopardize MOJVII assets and vital business functions or services. Agencies should identify those impacts to develop the strategies and justify the resources required to provide the appropriate level of prevention and response. It is important to use the results of risk assessment to protect critical MOJVII functions and services in the event of a security incident. The lack of appropriate security measures would jeopardize MOJVII critical functions and services. Security risk impact analysis activities include the following:

a. Identification of the Federal, State, and Local regulatory or legal requirements that address the security, confidentiality, and privacy requirements for MOJVII functions or services.

b. Identification of confidential information stored in the MOJVII's files and the potential for fraud, misuse, or other illegal activity.

c. Identification of essential access control mechanisms used for requests, authorization, and access approval in support of critical MOJVII functions and services.

d. Identification of the processes used to monitor and report to management on whatever applications, tools and technologies the MOJVII has implemented to adequately manage the risk as defined by the MOJVII (i.e., baseline security reviews, review of logs, use of IDs, logging events for forensics, etc.).

e. Identification of MOJVII's IT Change Management and Vulnerability Assessment processes.

f. Identification of security mechanisms in place to conceal MOJVII data (Encryption, PKI, etc.).

RA-2 - Security Categorization

Agencies must address the following requirements:

a. Categorization of information and the information system in accordance with applicable State and Federal laws, policies, regulations, standards, and guidance. NIST SP 800-60 Volumes 1 and 2 serves as a guidance for the categorization process. The security categories are based on the potential impact on an MOJVII should certain events occur that jeopardize the confidentiality, integrity, and availability of the information and information systems needed by the MOJVII to accomplish its assigned mission, protect its assets, fulfill its legal responsibilities, maintain its day- to-day functions, and protect individuals. The impact to MOJVII, personnel, and other external entities must be considered during the security categorization process.

b. System Owners need to be involved with the security categorization of an information system if they are responsible for:

    i.   Any interconnected system dependencies, i.e. systems that share information
    ii. A system that may inherit a security control from their respective system.

c. Include the security categorization process as a part of the system development lifecycle (SDLC). The security categorizations shall be developed early in the initiation stage ensuring the planning and implementation of the appropriate security controls throughout the SDLC

d. Ensure the security categorization decision is reviewed and approved by the authorized or designated representative.

e. Update documents to address changes to the information system/environment of operation or problems identified during plan implementation or security control assessments.

f. The Business Owner, System Owner and supporting security liaison must assist with the development of the security categorization.

Information includes all data, regardless of physical form or characteristics, made or received in connection with the transaction of public business by any MOJVII end-user. MOJVII's information shall be classified and handled in a manner that protects the information from unauthorized or accidental disclosure, modification, or loss. MOJVII must use the Data Classification and Handling Policy for detailed requirements for the storage, labeling, classification, and destruction of State data.

RA-3 - Risk Assessment

Risk assessments consider risks posed to State MOJVII operations and assets, or individuals from external parties, including but not limited to entities such as Service providers; Contractors operating information systems on behalf of the MOJVII; Individuals accessing State data and information systems; and Outsourcing organizations.

Agencies must conduct security/risk assessments to evaluate the level of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification or destruction of the information system and the information it processes, stores, or transmits.

Agencies shall conduct security/risk assessments at minimum annually, or whenever there are significant changes to the critical information system or environment of operation (including the identification of new threats and vulnerabilities), or other conditions that may impact the security state of the system.

An MOJVII-wide third-party assessment of all critical systems (Restricted or Highly Restricted) and associated security controls will be conducted at a minimum every 3 years. Agencies that completed an MOJVII-wide third-party assessment in year 1, may opt to complete a self-assessment or a more targeted and system specific assessment during years 2-3.

a. All assessment results will be provided to MOJVII IT within thirty (30) days of completion.

b. The risk assessment must consider risks posed to State's operations, assets, or individuals from external parties, including but not limited to the following:

  i. Organizations such as foreign nations and business competitors that may have an interest in information supplied to the agencies.

  ii. Service Providers:

    1. Contractors operating information systems on behalf of the State
    2. Individuals accessing MOJVII's information systems.

3. Outsourcing entities (e.g. cloud service providers (CSPs))

    i. Agencies need to obtain prior approval from the State CIO before contracting with cloud-hosted solutions or off-site hosting.

    ii. Agencies must ensure vendor compliance with Statewide security policies and obtain a Vendor Readiness Assessment Report (VRAR) from the vendor prior to contract approval. .

    ii Agencies shall ensure that contract language requires vendors to provide as attestation to their compliance, an industry recognized, third party assessment report. Examples of acceptable attestation reports include Federal Risk and Authorization Management Program (FedRAMP) certification, SOC 2 Type 2 and ISO 27001.

    iii Procurement language must also require, in addition to initial validation, cloud/vendor must annually provide the MOJVII validation of their continued compliance to State policies and procedures. This requirement includes all vendors supporting Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and/or Software as a Service (SaaS). Examples of acceptable assessment reports include Federal Risk and Authorization Management Program (FedRAMP) certification, SOC 2 Type 2 and ISO 27001. CSPs must demonstrate to the State that continuous monitoring activities are in place and compliance is being met.

c. When planning and budgeting for security/risk assessments, the MOJVII must follow these requirements:

    i. Multi-year planning and budgeting techniques must be used.

    ii. Annual assessments must be included in information system budgets and planning.

    iii. Other significant, planned activities must be considered in budgets and planning (e.g., life cycle activities, enhancements, audits) to ensure cost effective use of resources.

    iv. All information systems in an MOJVII must be considered to ensure resource efficiencies.

    v. Assessments must be coordinated between information systems with security control inheritance and other relational dependencies.

    vi. Agencies shall conduct an assessment using NIST 800-53 controls that includes at a minimum their critical systems shall be done.

    vii. An MOJVII may perform an annual self-assessment of their organization or system if they are storing, processing, or transmitting data that is classified as low or medium. An independent third-party assessment shall be completed every three years for systems storing, processing, or transmitting data classified as medium.

    viii. If an MOJVII or system stores, processes, or transmits data classified as highly restricted, the MOJVII shall use an independent assessor to conduct the annual assessment.

    ix. An independent assessor or assessment team shall assess the security controls in the information system using an ESRMO provided assessment template.

d. A Plan of Action and Milestones (POA&M) or Corrective Action Plan (CAP) for the system documenting the planned, remedial actions to correct weaknesses or deficiencies in security controls and to reduce or eliminate known vulnerabilities must be developed.

e. The existing POA&M or CAP must be updated weekly based on findings of weaknesses including, but not limited to, the following:

       i.   Reviews, tests, audits, or assessments

     ii.   Security impact analyses

    iii.   Independent verification and validation findings

    iv.   Continuous monitoring activities

     v.   Incidents

f.   All findings, recommendations, and their source must be tracked to the related item in the POA&M or CAP.

g.   Findings must be analyzed as to their level of risk (i.e., high, medium, low) and a determination must be made for appropriate action(s) to be taken to correct or mitigate, as appropriate, the identified weaknesses to an acceptable level of risk.

h.   One or more tasks to remediate a finding must be documented in the POA&M or CAP for any of the following:

       i.   Critical-level risks that are not remediated within 7 days.

     ii.   High-level risks that are not corrected within 21 days.

    iii.   Medium-level risks that are not corrected within 30 day.

    iv.   Low level risks as required by the MOJVII CIO and that are not corrected within 90 days.

f.   All findings must be entered into a corrective action plan (CAP).

Risk Assessment/Analysis

Risk assessment or analysis is the act of determining the probability that a risk will occur and the impact that event would have if it does occur. This analyzes the cause and effect of each possible event. Once risks have been identified and documented, risk analysis must be performed. During the risk analysis process, each potential risk event will be evaluated for the following:

a.   The probability that the risk will occur.
b.   The impact of the risk if it occurs.

These two factors of assessing the risk involving probability and impact shall be measured for probability using a scale of Low, Medium, and High, and giving each an associated number.

For impact, the State shall use a qualitative method for analysis as it is typically a quicker and usually more cost-effective way to analysis risks. Analysis will be performed with the goal of gathering data on the following:

a.   The likelihood of the risk occurring.
b.   The qualitative impact on the company, system, or data
c.   The quality of the risk data being utilized.

Business Risk Analysis of each business system shall be utilized to assist in impact determination.

Impact Definitions

Magnitude of Impact	Impact Definition

High	If an event could be expected to have a severe or catastrophic adverse effect on MOJVII operations, MOJVII assets, or individuals; and cause a loss of mission capability for a period that poses a threat to human life or results in a loss of major assets.
Moderate	If an event could be expected to have a serious adverse effect on MOJVII operations, MOJVII assets or individuals, and cause significant degradation in mission capability, place
	the MOJVII at a significant disadvantage, or result in major damage to assets, requiring. extensive corrective actions or repairs.
Low	If an event could be expected to have a limited adverse effect on MOJVII operations (including mission, functions, image or reputation, MOJVII assets, or individuals; and cause a negative outcome or result in limited damage to operations or assets, requiring minor corrective actions or repairs.

As Risks are identified and quantified, they are entered into the into the MOJVII IT Enterprise Risk Compliance (ERCT) reporting and tracking tool. All risks are reported based on type of risk, probability, impact, and overall risk. To determine and quantify the overall risk, the below table (based on NIST 800-30) is used.

Threat Likelihood	Low (10)	Medium (50)	High (100)
High (1.0)	Low 10 x 1.0 = 10	Medium 50 x 1.0 = 50	High 100 x 1.0 = 100
Medium (0.5)	Low 10 x 0.5 = 5	Medium 50 x 0.5 = 25	Medium 100 x 0.5 = 50
Low (0.1)	Low 10 x 0.1 = 1	Low 50 x 0.1 = 5	Low 10 x 0.1 = 10

Risk Response

For each identified risk, a response must be identified. The Security Liaison will select a risk response for each risk. The probability and impact of the risk will be the basis of recommending which actions should be taken to mitigate the risk. During response planning, strategies and plans are developed to minimize the effects of the risk to a point where the risk can be controlled and managed.

Avoid: Risk avoidance involves changing aspects of the overall business process or system architecture to eliminate the threat.

Transfer: Risk transference involves shifting the negative impact of a threat (and ownership of the response) to a third party. Risk transference does not eliminate a threat it simply makes another party responsible for managing it. This would include identifying avenues of insurance, etc.

Mitigate: Risk mitigation involves reducing the probability and/or the impact of risk threat to an acceptable level. Taking early and pro-active action against a risk is often more effective than attempting to repair the damage a realized risk has caused. Developing contingency plans are examples of risk mitigation.

Accept: Risk acceptance should normally only be taken for low-priority risks. All risks should have a recommendation of control(s) and / or alternative solutions to mitigate risk.

Risk Level	Risk Description and Necessary Actions
High	Mandatory need for corrective measures. CAP must be in place for 60 days.
Medium	Plan must be developed to mitigate corrective measures within 90 – 120 days.
Low	Decision on whether to implement corrective measures or accept the risk.

Use of Independent Assessors

When assessments must be conducted by an entity with an explicitly determined degree of independence to the organization, independence must be determined by the MOJVII CIO based on the security categorization of the information system and/or the risk to MOJVII operations and assets, and to individuals.

To make an informed, risk-based decision, the selection of independent assessors must consider the following criteria to ensure credibility of the security assessment results and to receive the most objective information possible. Preserving the impartial and unbiased nature of the assessment process including, but not limited to, freedom from any perceived or actual conflicts of interest with respect to the following:

a. The development, operation, and/or management of the information system

b. The chain of command associated with the information system.

c. The determination of security control effectiveness

d. A competitive relationship with any organization associated with the information system being assessed or impacts on their reputations.

e. Undue influence because of a contractual or other related relationship

f. The assessor's technical expertise and knowledge of State and federal requirements

RA-4 - Risk Assessment Update

Withdrawn: Incorporated into RA-3.

RA-5 - Vulnerability Scanning

All State Risk Assessment programs must include the following requirements:

a. All malware scanning software shall be current, actively running on deployed workstations and servers, and capable of generating audit logs of virus events.

b. Vulnerability scans in information systems and hosted applications must be performed on at least every 7 days and when new vulnerabilities potentially affecting the system/applications are identified and reported.

c. Vulnerability scanning shall include scanning for specific functions, ports, protocols and services that should not be accessible to users or devices and for improperly configured or incorrectly operating information flow mechanisms.

d. Real-time scanning for spyware, adware and bots (software robots) with one or more anti-spyware programs that detect these malicious programs and help inoculate the system against infection.

e. Scan for malware on files that are downloaded from the Internet or any other outside source,

including all external media, such as flash drives, CDs, etc. shall be conducted.

f. Viruses, spyware, Trojan applications and other malicious code may cause damage to MOJVII's infrastructure via Web browsers and therefore all internet traffic shall be scanned to prevent malicious code from infecting MOJVII's infrastructure.

g. External computers or networks making remote connection to internal MOJVII computers or networks shall utilize an MOJVII-approved active virus scanning and repair program and an MOJVII- approved personal firewall system (hardware or software). The MOJVII shall ensure that updates to virus scanning software and firewall systems are available to users. Non-State computers or networks making a remote connection to a public Web server are exempted.

h. Agencies shall scan their networks in order to identify any multifunctional devices (MFD)s on the network that are vulnerable and/or configured insecurely and take remediation actions.

i. Conduct scanning independently or as a coordinated effort with ESRMO.

j. Prior to commencing vulnerability scanning efforts, the following should be addressed:

    i. Scanner selection – Evaluate the mandated tools for use within the respective environments.

    ii. The network and host-based vulnerability scanner shall provide the following capabilities:

        1. Identify active hosts on networks.
        2. Identify active and vulnerable services (ports) on hosts.
        3. Identify vulnerabilities associated with discovered operating systems and applications.

 MOJVII IT shall implement a suite of automated monitoring tools to effectively monitor and identify vulnerabilities on networked computer servers and workstations. Vulnerability scanning tools and techniques are employed that promote interoperability among tools and automate parts of the vulnerability management process by using standards for the following:

    i. Enumerating platforms, software flaws, and improper configurations

    ii. Formatting and making transparent, checklists and test procedures.

    iii. Measuring vulnerability impact

    iv. Analyzing vulnerability scan reports and results from security control assessments

    v. Remediating legitimate vulnerabilities within [organization-defined response times] in accordance with an organizational assessment of risk

Sharing information obtained from the vulnerability scanning process and security control assessments with designated personnel throughout the organization to help eliminate similar vulnerabilities in other information systems (i.e., systemic weaknesses or deficiencies).

Vulnerability Management

System administrators shall ensure that all current maintenance and security vulnerability patches are applied and that only essential application services and ports are enabled and opened in the system's firewall, as applicable. Vulnerabilities that threaten the security of MOJVII's network or IT assets shall be addressed through updates and patches based upon assigned vulnerability ratings:

a. Personnel shall manage systems to reduce vulnerabilities through vulnerability testing and management, promptly installing patches and updates, and eliminating or disabling unnecessary services.

b. Agencies shall use where possible tools that express vulnerabilities in the Common Vulnerabilities and Exposures (CVE) naming convention and that use the Open Vulnerability Assessment Language (OVAL) to test for the presence of vulnerabilities.

c. Perform scans, typically, on systems and networks known to be stable and preferably during times of least impact to the critical functionality of the system. Expect vulnerability scanning to occur during various phases of the system's life cycle.

Vulnerability Risk Ratings

Where technically configurable, risk ratings shall be calculated based on active exploit threat, exploit availability, factors from the Common Vulnerability Scoring System (CVSS), and system exposure utilizing a scale of 0 to 10.0 as per the CVSS v3 "Qualitative Severity Rating Scale" for proper prioritization. If the additional combined information above is not available then the CVSS score, exploitability information, or a vendor rating where appropriate risk is reflected may be used. For general vulnerabilities that do not easily relate back to a CVE, such as unsupported software or encryption versions less than policy requirements, a vulnerability scanner rating that is above "info", or a score of 0, may be used after appropriate review.

The risk ratings assigned to a vulnerability are as follows:

a. **Critical-level Risk** (Priority/CVSS 9.0-10.0)**:** A vulnerability that could cause grave consequences and potentially lead to leakage of Restricted or Highly Restricted data, if not addressed and remediated immediately. This type of vulnerability is present within the most sensitive portions of the network or IT asset, and could cause functionality to cease, exfiltration of data, or an intruder to gain access to the network or IT asset.

b. **High-level Risk** (Priority/CVSS 7.0-8.9)**:** A vulnerability that could lead to a compromise of the network(s) and systems(s) if not addressed and remediated within the established timeframe. This vulnerability could cause functionality to cease or control of the network or IT asset to be gained by an intruder.

c. **Medium-level Risk** (Priority/CVSS 4.0-6.9)**:** A vulnerability that should be addressed within the established timeframe. Urgency in correcting this type of vulnerability still exists; however, the vulnerability may be either a more difficult exploit to perform or of lesser concern to the data owner.

d. **Low-level Risk** (Priority/CVSS 0.1-3.9)**:** A vulnerability that should be fixed; however, it is unlikely that this vulnerability alone would allow the network or IT asset to be exploited and/or it is of little consequence to the data owner. Vulnerabilities of this nature are common among most networks and IT assets and usually involve a simple patch to remedy the problem. These patches can also be defined as enhancements to the network or IT asset.

Vulnerability Mitigation

a. Mitigation timeframes for identified or assessed vulnerabilities shall be based on the assigned Vulnerability Risk Rating:

  i. **Critical-level risk** vulnerabilities must be mitigated as soon as possible. "Critical-level risk" vulnerabilities must be, at a minimum, mitigated within 7 days, and remediated (if possible) within 21 days.

  ii. **High-level risk** vulnerabilities must be mitigated or remediated within thirty (30) days.

  iii. **Medium-level risk** vulnerabilities must be mitigated or remediated within sixty (60) days.

    iv. **Low-level risk** vulnerabilities must be mitigated or remediated within ninety (90) days.

b. MOJVII vulnerability mitigation procedures must specify, at a minimum, the proposed resolution to address identified vulnerabilities, required tasks necessary to affect changes, and the assignment of the required tasks to appropriate personnel.

c. Vulnerability exceptions are permitted in documented cases where a vulnerability has been identified but a patch is not currently available. When a vulnerability risk is 'high-level' and no patch is available, steps must be taken to mitigate the risk through other compensating control methods (e.g., group policy objects, firewalls, router access control lists). A patch needs to be applied when it becomes available. When a 'high-level' risk vulnerability cannot be totally mitigated within the requisite time frame, agencies need to notify MOJVII management and the State Chief Information Officer of the condition.

d. Appropriate testing and assessment activities shall be performed after vulnerability mitigation plans have been executed to verify and validate that the vulnerabilities have been successfully addressed.

e. Appropriate notification shall be provided after vulnerability mitigation plans have been executed.

f. In the event of a zero-day vulnerability, a situation where an exploit is used before the developer of the software knows about the vulnerability, agencies shall mitigate the vulnerability immediately, if possible, and apply patches as soon as possible after the vendor provides them.

Vulnerability Information Review and Analysis

a. Relevant vulnerability information from appropriate vendors, third party research, and public domain resources shall be reviewed on a regular basis, per the MOJVII's policies and procedures.

b. Relevant vulnerability information, as discovered, shall be distributed to the appropriate MOJVII employees, including the security office.

c. Appropriate MOJVII personnel shall be alerted or notified in near real-time about warnings or announcements involving "High-risk" vulnerabilities.

Requirements for Compliance

a. Agencies must develop procedures to ensure the timely and consistent use of security patches and use a consistent vulnerability naming scheme to mitigate the impact of vulnerabilities in systems.

b. Agencies shall have an explicit and documented patching and vulnerability policy, as well as a systematic, accountable, and documented set of processes and procedures for handling patches.

c. The patching and vulnerability policy shall specify techniques an organization will use to monitor for new patches and vulnerabilities and personnel who will be responsible for such monitoring.

d. An organization's patching process shall define a method for deciding which systems are patched and which patches are installed first, as well as the method for testing and safely installing patches.

e. An MOJVII process for handling patches shall include the following:

    i. Using organizational inventories

ii. Using the Common Vulnerabilities and Exposures vulnerability naming scheme for vulnerability and patch monitoring (See http://cve.mitre.org)

iii. Patch prioritization techniques

iv. Organizational patch databases.

v. Patch testing, patch distribution, patch application verification, patch training, automated patch deployment, and automatic updating of applications

f. Agencies shall develop and maintain a list of sources of information about security problems and software updates for the system and application software.

g. Agencies shall establish a procedure for monitoring those information sources.

h. Agencies shall evaluate updates for applicability to the systems.

i. Agencies shall plan the installation of applicable updates.

j. Agencies shall install updates using a documented plan.

k. Agencies shall deploy new computers with up-to-date software.

l. After making any changes in a system's configuration or its information content, agencies shall create new cryptographic checksums or other integrity-checking baseline information for the system.

RA-5 (1) - Vulnerability Scanning – Update Tool Capability (Moderate Control)

Agencies shall employ vulnerability scanning tools that include the capability to readily update the information system vulnerabilities to be scanned. The vulnerabilities to be scanned need to be readily updated as new vulnerabilities are discovered, announced, and scanning methods developed. This updating process helps to ensure that potential vulnerabilities in the information system are identified and addressed as quickly as possible.

RA-5 (2) - Vulnerability Scanning – Frequency of Updates (Moderate Control)

MOJVII updates the information system vulnerabilities scanned prior to a new scan or when new vulnerabilities are identified and reported.

RA-5 (5) - Vulnerability Scanning – Privileged Access (Moderate Control)

Agencies shall implement privileged access authorization to an information system for vulnerability scanning activities. In certain situations, the nature of the vulnerability scanning may be more intrusive or the information system component that is the subject of the scanning may contain highly restricted information. Privileged access authorization to selected system components facilitates more thorough vulnerability scanning and protects the sensitive nature of such scanning.

RA-6 – Technical Surveillance Countermeasures Survey (Optional)

This control is optional for LOW and MODERATE risk 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 the State are expected to comply with the current implemented version of this policy.

APPENDIX A – MOJVII ANNUAL ASSESSMENT AND COMPLIANCE REPORT TEMPLATE

[MOJVII LETTER HEAD]

TO: XXXXXXXXXXX
             Chief Information Officer

FROM: [XXXXXXXX]

SUBJECT: 2021 MOJVII Compliance Report

A.   I certify that [MOJVII] has implemented the appropriate processes and procedures listed below to be in compliance with the Statewide Information Security Manual and State statues:

☐   No data of a confidential nature, as defined in the NIST SP-800-171 or federal law, was entered into, or processed through any information technology system or network established until safeguards for the data's security satisfactory to the MOJVII CIO have been designed and installed and are fully operational.

☐   MOJVII IT obtained approval from the MOJVII CIO prior to contracting for the storage, maintenance, or use of data by a private vendor.

☐   MOJVII ensured all information technology security goods, software, or services purchased using funds, or for use by MOJVII, was subject to approval by the MOJVII CIO in accordance with security standards.

☐   MOJVII completed annual risk assessments to identify compliance, operational, and strategic risks to the enterprise network. These assessments may include methods such as penetration testing or similar assessment methodologies.

☐

Type of Assessment	Completion Date	Cost for Assessment
[Enter 3rd party/vendor details or Self-Assessment]		

☐ MOJVII ensured all contracts for third party assessment and testing, was approved by the MOJVII CIO (as applicable) and resulting sanitized assessment reports were made public.

☐ MOJVII provided the full details of the MOJVII's information technology and operational requirements and of all the MOJVII's information technology security incidents within 24 hours of confirmation.

☐ MOJVII designated an MOJVII liaison in the information technology area to coordinate with the MOJVII CIO.

☐ MOJVII completed an annual assessment of contracted vendors, to comply with the current security enterprise-wide set of standards. The assessment shall include, at a minimum, the rate of compliance with the enterprise-wide security standards and an assessment of security organization, security practices, security information standards, network security architecture, and current expenditures for information technology security.

Cloud Service Provider	Cloud Offering	Service Type	Review Assessment Date
Ex. Microsoft	Office 365	IaaS / SaaS / PaaS	
[Add Rows Needed]			

☐ MOJVII submitted disaster recovery plans to the State CIO on an annual basis and as otherwise requested by the CIO

☐ MOJVII achieved completion rate ≥ 95 percent for annual Cybersecurity Awareness Training during CY 20XX

Number of Employees (including contractors), involved	Number of Users who Completed the training	Training Budget Required

☐ [MOJVII] has not completed all requirements but have identified a plan to comply. Attached is our assessment report to include corrective action plan indicating when the MOJVII will meet these requirements.

B. Below is the estimated cost to implement security measures needed for agencies to fully comply with the standards.

SECURITY / BUDGET DEFICIENCIES:

Security Gaps	Estimated Cost to Remediate	MOJVII budget approved? (Y/N)
Ex. Security boundary devices, Personnel, Training, Vulnerability Management, End of Life Support		

For additional information about this submission please contact: [INSERT MOJVII CONTACT]

APPROVAL SIGNATURES PAGE
Information Technology Department (ITDEPT)

MOJVII OFFICERS	SIGNATURE	DATE
CIO		
CSO		
CEO		
IASO:		