**FACILITY-RELATED CONTROL SYSTEMS**

**PLAN OF ACTION AND MILESTONES PROCEDURE (POAM)**



**[Replace ESTCP Logo with Organization Logo]**

**June 20, 2017**

**Organization Address**

**City, State, Zip Code**

Table of Contents

[HOW THIS DOCUMENT IS ORGANIZED 5](#_Toc485736887)

[1.1 PURPOSE 6](#_Toc485736888)

[1.2 SCOPE 6](#_Toc485736889)

[1.3 SYSTEM DESCRIPTION 6](#_Toc485736890)

EXECUTIVE SUMMARY

This document supports the Plan of Action & Milestones for [ORGANIZATION]. The plan of action and milestones (POA&M) is one of three key documents in the security authorization package and describes the specific tasks that are planned: (i) to correct any weaknesses or deficiencies in the security controls noted during the assessment; and (ii) to address the residual vulnerabilities in the information system.

POA&Ms are used by the authorizing official to monitor progress in correcting weaknesses or deficiencies noted during the security control assessment.

Prepared by

| Identification of Organization that this Document Prepared by | | |
| --- | --- | --- |
| Logo | Organization Name |  |
| Street Address |  |
| Suite/Room/Building |  |
| City, State Zip |  |

Prepared for

| Identification of Organization that this Document was Prepared for | | |
| --- | --- | --- |
| Logo | Organization Name |  |
| Street Address |  |
| Suite/Room/Building |  |
| City, State Zip |  |

TEMPLATE REVISION HISTORY

| **Date** | **Page(s)** | **Description** | **Author** |
| --- | --- | --- | --- |
| 06/20/2017 | All | Initial Document - The document was modeled after the FedRAMP template but modified to ESTCP format | Michael Chipley |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

ABOUT THIS DOCUMENT

This document has been developed to provide guidance and procedures for [ORGANIZATION]. mitigations of risks as determined in the System Security Plan.

HOW THIS DOCUMENT IS ORGANIZED

This document is divided into two sections. Some sections include subsections.

|  |  |
| --- | --- |
| Section 1 | Describes the introduction and provides an overview and includes the purpose of the document as well as the authorities and standards. |
| Section 2 | Describes the methodology used to create the POA&M. |
| Appendix A | Describes acronyms used. |
| Appendix B | Describes references used. |

1 INTRODUCTION AND PURPOSE

The plan of action and milestones (POA&M) is one of three key documents in the security authorization package and describes the specific tasks that are planned: (i) to correct any weaknesses or deficiencies in the security controls noted during the assessment; and (ii) to address the residual vulnerabilities in the information system.

POA&Ms are used by the authorizing official to monitor progress in correcting weaknesses or deficiencies noted during the security control assessment.

1.1 PURPOSE

The purpose of POA&M is to facilitate a disciplined and structured approach to mitigating risks in accordance with [ORGANIZATION]’s corporate priorities. POA&Ms are based on the findings and recommendations of the security assessment report excluding any remediation actions taken.

POA&M’s are based on: (i) the security categorization of the information system; (ii) the specific weaknesses or deficiencies in deployed security controls; (iii) the importance of the identified security control weaknesses or deficiencies; and (iv) [ORGANIZATION]’s proposed risk mitigation approach to address the identified weaknesses or deficiencies in the security controls (e.g., prioritization of risk mitigation actions, allocation of risk mitigation resources).

The POA&M identifies: (i) the tasks to be accomplished with a recommendation for completion either before or after information system implementation; (ii) the resources required to accomplish the tasks; (iii) any milestones in meeting the tasks; and (iv) the scheduled completion dates for the milestones.

1.2 SCOPE

The scope of the POA&M includes all management, operational, and technical security controls that are deemed less than effective (i.e., having unacceptable weaknesses or deficiencies in the control implementation). Then ISSM is required to submit updated POA&Ms to the [ORGANIZATION] Inc. AO at least quarterly or as needed (i.e., when new weaknesses are identified or remediation actions are taken to close any existing POA&M items).

1.3 SYSTEM DESCRIPTION

The [ORGANIZATION] Corporate Information System has been determined to have a security categorization of [**Moderate, Moderate, Moderate]**.

Reference the [ORGANIZATION] Corporate Information Systems IT Technology Plan (ITCP) for a top level system description and network architecture diagram.

2.0 METHODOLOGY

POA&Ms must include all known security weaknesses within the cloud information system. Weakness information is gathered and reported using embedded [ORGANIZATION] Inc. POA&M workbook.

The System POA&M worksheet consists of two sections. The top portion of the POA&M tracks FISMA system performance measurements while the bottom portion tracks IT system weaknesses.

The top portion of the POA&M tracks the measures in the table below.

|  |  |
| --- | --- |
| **Measure** | **Details** |
| **FIPS 199 Risk Impact Level** | Systems are categorized as **Low, Moderate, or High** based on a completed FIPS 199/800-60 evaluation. |
| **Federal or Contractor System** | Systems are identified as either **Federal or Contractor.** Contractor systems are identified as any system that processes or handles federal-owned information on behalf of the government that are housed at non-government facilities including contractor, consultant, or other third party (includes Federal agencies/departments) sites. |

The bottom portion of the POA&M worksheet is the corrective action plan used to track IT security weaknesses.

**Column A – POAM ID**. – A unique identifier must be assigned to each POA&M item.

**Column B -- Weakness Description.** Describe weaknesses identified during the assessment process. Sensitive descriptions of specific weaknesses are not necessary, but sufficient data must be provided to permit oversight and tracking, demonstrate awareness of the weakness, and facilitate the creation of specific milestones to address the weakness. Where it is necessary to provide more sensitive data, the POA&M should note the fact of its special sensitivity.

**Column C – Point of Contact (POC).** Identify the person/role that [ORGANIZATION] Inc. can hold responsible for resolving the weakness. A POC must be identified and documented for each weakness reported.

**Column D -- Resources Required.** Identify any resources, obstacles and challenges needed to resolve the weakness (e.g., lack of personnel or expertise, development of new system to replace insecure legacy system, etc.).

A completion date must be assigned to every weakness, to include the month, day, and year.   If a weakness is resolved before or after the originally scheduled completion date, enter the actual completion date in the *Status* column. Also, if the time to correct the weakness extends beyond the original scheduled date of completion, the reasons for the delay must be noted in the *Milestone Changes* column together with a revised scheduled date of completion. The *Scheduled Completion Date* column must not change once it is recorded. If there are changes to scheduled completion date(s), note them in the Column F, *Milestone Changes*.

**Column E -- Scheduled Completion Date.** A completion date must be assigned to every weakness, to include the month, day, and year.   If a weakness is resolved before or after the originally scheduled completion date, enter the actual completion date in the *Status* column. Also, if the time to correct the weakness extends beyond the original scheduled date of completion, the reasons for the delay must be noted in the *Milestone Changes* column together with a revised scheduled date of completion. The *Scheduled Completion Date* column must not change once it is recorded. If there are changes to scheduled completion date(s), note them in the Column G, *Milestone Changes*.

**Column F – Milestones with Completion Dates.** A milestone will identify specific requirements to correct an identified weakness. Each weakness must have a milestone documented that identifies specific actions to correct the weakness with an associated completion date.  *Milestone with Completion Date* entries shall not change once it is recorded.

**Column G – Source of Discovery.** Identify sources for all weaknesses. Ensure this is consistent with the Security Assessment Report (SAR), if used (Note: [ORGANIZATION] uses the POAM and monthly audits as a living SAR).

**Column H -- Status.** A status of *Completed or Ongoing* must be assigned to each weakness.

* *Completed* — This status is assigned when all corrective actions have been applied to a weakness such that the weakness is successfully mitigated.  The *Date of Completion* shall be recorded for a completed weakness.
* *Ongoing* — This status is assigned to both current weaknesses that have not exceeded the associated *Scheduled Completion Date* and delayed weaknesses.

Non-Conforming Controls need to be added in the POA&M. As technology evolves, Non-Conforming Controls need to be revaluated as mitigation techniques may surface that did not previously exist at the time of the decision or countermeasure costs may decrease affecting the original Non-Conforming Controls.

• False positives must be clearly identified within the POAM/SAR, along with supporting evidence (e.g., clean scan report) do not have to be identified in the POA&M.

• Each line item on the POA&M/SAR must have a unique identifier.

• All high and critical risk findings must be remediated prior to receiving a Provisional Authorization.

• Moderate findings shall have a mitigation date within 90 days of Authorization date.

APPENDIX A. ACRONYMS

|  |  |
| --- | --- |
| **Acronym** | **Definition** |
| AC | Authentication Category |
| AP | Assurance Profile |
| API | Application Programming Interface |
| ATO | Authorization to Operate |
| C&A | Certification & Accreditation |
| COTS | Commercial Off the Shelf |
| FIPS PUB | Federal Information Processing Standard Publication |
| FISMA | Federal Information Security Management Act |
| GSS | General Support System |
| IaaS | Infrastructure as a Service (Model) |
| IATO | Interim Authorization to Operate |
| ID | Identification |
| IT | Information Technology |
| LAN | Local Area Network |
| NIST | National Institute of Standards and Technology |
| PIA | Privacy Impact Assessment |
| POA&M | Plan of Action and Milestones |
| POC | Point of Contact |
| RA | Risk Assessment |
| Rev. | Revision |
| SA | Security Assessment |
| SAR | Security Assessment Report |
| SDLC | System Development Life Cycle |
| SP | Special Publication |
| SSP | System Security Plan |
| VLAN | Virtual Local Area Network |

APPENDIX B. REFERENCES

Laws and Regulations:

* Federal Information Security Management Act of 2002, Title III – Information Security, P.L. 107-347.
* Consolidated Appropriations Act of 2005, Section 522.
* USA PATRIOT Act (P.L. 107-56), October 2001.

OMB Circulars:

* OMB Circular A-130, Management of Federal Information Resources, November 2000.
* OMB Memorandum M-05-24, Implementation of Homeland Security Presidential Directive (HSPD) 12—Policy for a Common Identification Standard for Federal Employees and Contractors, August 2005.
* OMB Memorandum M-06-16, Protection of Sensitive Agency Information, June, 2006.

FIPS Publications:

* FIPS PUB 199, Standards for Security Categorization of Federal Information and Information Systems
* FIPS PUB 200, Minimum Security Requirements for Federal Information and Information Systems
* FIPS PUB 201, Personal Identity Verification (PIV) of Federal Employees and Contractors

NIST Publications:

* NIST 800-18, Guide for Developing Security Plans for Information Technology Systems
* NIST 800-26, Security Self-Assessment Guide for Information Technology Systems
* NIST 800-30, Risk Management Guide for Information Technology Systems
* NIST 800-34, Contingency Planning Guide for Information Technology Systems
* NIST 800-37, Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach
* NIST 800-47, Security Guide for Interconnecting Information Technology Systems
* NIST 800-53 Rev3, Recommended Security Controls for Federal Information Systems and Organizations
* NIST 800-53A Rev1, Guide for Assessing the Security Controls in Federal Information System and Organizations
* NIST 800-60 Rev1, Guide for Mapping Types of Information and Information Systems to Security
* NIST 800-63, Electronic Authentication Guideline: Recommendations of the National Institute of Standards and Technology
* NIST 800-64, Security Considerations in the Information System Development Life Cycle