# Security Assessment Procedure

|  |  |  |  |
| --- | --- | --- | --- |
| Procedure Owner |  |  | |
| Procedure Approver(s) |  |
| Effective Date |  | Next Review Date |  |

# Purpose

The purpose of this procedure is to define a consistent approach to manage Security Assessment of the IT environment at [COMPANY NAME] .

# Scope

This procedure is consistent with CMMC and covers all security assessment procedures within [COMPANY NAME] environment. This procedure will be followed by all employees of [COMPANY NAME] . The CMMC System Security Plan (SSP) will be updated to reflect any significant modifications made to this procedure.

# Definitions

**Employees**: All individuals belonging to one or many groups defined below:

1. All individuals associated with [COMPANY NAME] through an employee – employer relationship or contract between [COMPANY NAME] and their employer or [COMPANY NAME] and individual.
2. All individuals possessing equipment issued by [COMPANY NAME] .
3. All individuals working on the premises of [COMPANY NAME] and/or utilizing the Internet services provided by [COMPANY NAME] .

# Governing Laws, Regulations, and Policies

* NIST SP 800-171, 3.12.1 - 3.12.4
* CMMC CA.L2-3.12.1 – CA.L2-3.12.4
* [COMPANY NAME] – CA – 3.12 - Security Assessment Policy

# Procedure Statements

**CA.L2-3.12.1** – **Develop a procedure for the periodic assessment of the security controls in organizational systems to determine if the controls are effective in their application. This procedure should include:**

1. [COMPANY NAME] reviews and updates the information security architecture at least on an annual basis, or when security-relevant changes require modification to the SSP to reflect updates in the enterprise architecture.
2. [COMPANY NAME] employs an assessment team that consists of:
   * + <role>: Functions as the primary Point of Contact (POC) for Information System assessments and delegates duties, as determined necessary.
     + SecureStrux (MSP): / <Role>: Functions as the secondary (POC) for information System assessment and receives delegation duties from System Administrator when assessments are scheduled.
   * [COMPANY NAME] adheres to the following System Security Plan (SSP) related requirements:
     + - * The SSP is reviewed and updated on an annual basis.
         * The SSP is updated to reflect changes to the Information Systems.
         * The SSP is updated to reflect changes to the Information System’s operating environment.
         * The SSP is updated to reflect changes that result from problems identified during plan implementation and/or security control assessments.
         * The SSP is protected from unauthorized disclosure and modification.
       - The <role> plans and coordinates security-related activities (e.g., hardware/software maintenance, system patching, etc.) affecting the Information System with all stakeholders prior to conducting such activities to reduce the impact on other organizational entities. This is accomplished using the Configuration Management (CM) Procedures processes. The <role> ensures that planned information security architecture changes are reflectected on the SSP and POA&M if applicable.
       - The <role> is responsible for continuously assessing relevant security controls to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting associated security requirements. Controls are assessed according to their defined Continuous Monitoring frequency.

**CA.L2-3.12.2 –** **Develop and implement plans of action (e.g., POA&M) designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems.**

1. The Plan of Action and Milestone (POA&M) document details security findings that are discovered during Information System assessments and/or continuous monitoring activities that cannot be mitigated within 30 days. POA&M documentation provides details that describe outstanding system vulnerabilities, including:
   * + Weakness identified.
     + Ownership of who will be accountable for ensuring remediation.
     + Description of milestones to remedy the weakness.
     + Status of remediation Ongoing or complete.
     + Completion dates.
2. The <role> develops and maintains a Plan of Action and Milestones document to correct identified deficiencies and reduce or eliminate identified vulnerabilities for the Information Systems under [COMPANY NAME]’s purview. POA&M documentation is updated on a quarterly basis with findings from security control assessments, security impact analyses, and continuous monitoring activities.
3. The POA&M is implemented to correct identified deficiencies and reduce or eliminate identified vulnerabilities. POA&M documentation includes planned remedial actions to correct weaknesses and deficiencies that are noted during the assessment of security controls. This assists in the reduction or elimination of known Information System related vulnerabilities.

**CA.L2-3.12.3 –** **Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls.**

1. The <role> is responsible for the establishment of the Continuous Monitoring practices, and for ensuring adherence to its requirements. [COMPANY NAME] implements a continuous monitoring program, which includes:
   * + Ongoing security control assessments.
     + Ongoing security status monitoring of defined metrics.
     + Ongoing analysis of security-related information generated by assessments and results.
     + Response actions to address security-related information analysis results.
   * Continuous Monitoring results, to include the security status of Information System related controls, are reported to the assessment Team. Open findings are reported to the assessment team within 24 hours of discovery.

* The <role> assesses the Information Systems according to the following frequency:
  + - During initial system set-up.
    - When system security changes have been made.

**CA.L2-3.12.4 –** **Develop, document and periodically update System Security Plans (SSPs) that describe system boundaries, system environments of operation, how security requirements are implemented and the relationships with or connections to other systems.**

1. [COMPANY NAME] develops and documents Information System security requirements that contains information necessary to serve as the System Security Plan (SSP) to include;
2. The system environment of operation is described and documented in the system security plan by describing the Information System’s function in terms of mission/business processes and listing explicit definition of the Information System’s physical boundary, including visual diagrams, [refer to Appendix A: Facility Floor Plan which indicates the components of the system boundary.]
3. Identification of each selected security control’s associated control type, implementation status (e.g., Implemented, Planned to be Implemented, Not Applicable, Inherited), and supporting rationale for any supplementation decisions
4. the method of security requirement implementation is described and documented in the system security plan;
5. The relationship with or connection to other systems is described and documented in the system security plan with an explicit definition of the Information System’s network architecture, including visual diagrams, [refer to Appendix B: Network Topology]
6. The frequency to update the system security plan is defined as annually
7. The SSP is reviewed and updated on an annual basis. When review period for the SSP is approaching. The System Administrator will position the review on the POA&M.

**Roles and Responsibilities**

|  |  |  |
| --- | --- | --- |
| **Role** | **Responsibilities** | **Contact Information** |
|  |  |  |
|  |  |  |

# Non-Compliance

Violations of this policy will be treated like other allegations of wrongdoing at [COMPANY NAME] . Allegations of misconduct will be adjudicated according to established procedures. Sanctions for non-compliance may include, but are not limited to, one or more of the following:

1. Disciplinary action according to applicable [COMPANY NAME] policies;
2. Termination of employment; and/or
3. Legal action according to applicable laws and contractual agreements.

# Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| **Version ID** | **Date of Change** | **Author** | **Rationale** |
| V.01 | 11/28/2022 | Securestrux | Initial draft |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |