# Risk Assessment Procedure

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

# Purpose

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

# Scope

This procedure is consistent with CMMC and covers all risk 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, 3.11.1 - 3.11.3
* CMMC RA.L2-3.11.1 – RA.L2-3.11.3
* [COMPANY NAME] – RA – 3.11 - Risk Assessment Policy

# Procedure Statements

**RA.L2-3.11.1 – Periodically assess the risk to organizational operations (including mission, functions, image or reputation), organizational assets and individuals, resulting from the operation of organizational systems and the associated processing, storage or transmission of CUI:**

1. [COMPANY NAME] conducts an assessment of risk to operations annually or upon entrance of new assets, which includes the likelihood and magnitude of harm from:
   * + Mission, functions, image, or reputation.
     + Unauthorized access, use, disclosure, disruption, modification, or destruction of the systems.
     + Company assets and individuals resulting from the operation of company systems and the associated processing, storage, and transmission of CUI data.
     + Privacy related problems for individuals arising from the intentional processing of personally identifiable information.
2. Risk assessments are also considered from external parties (e.g., service providers, individuals accessing organizational systems, outsourcing entities). Areas of weakness or vulnerabilities that could lead to risks may include:
   * + Poorly designed and executed business processes.
     + Inadvertent actions of people, such as disclosure or modification of information.
     + Intentional actions of people, such as insider threat and fraud.
     + Failure of systems to perform as intended.
     + Failures of technology.
     + External events, such as natural disasters, public infrastructure, and supply chain failures.
   * Identified risks are prioritized based on defined risk criteria to include risk categories, identified sources of risk and specific risk measurement criteria. The risk is to be analyzed to determine the severity of the risk and its impact on the organization and potential threat. The <Role> identifies organizational functions and IT assets to support the required actions.
   * The results of any risk assessment will be provided in a summary report and will be stored centrally in the <designated repository>. A Plan of Actions & Milestones (POA&M) will be maintained separately by the <role>for any items that could not be remediated; identifying mitigation actions including dates when/if the finding can be closed. The results of the risk assessment(s) will be reviewed at least annually and/or when applicable milestone dates are reached by the <role>, <FSO>, and <HR>.
   * The results of the risk assessment(s) will be provided to the <CEO> for dissemination to the larger organization. The <role>will provide a copy to the <CEO> upon completion of the assessment(s) and any identified findings of a critical nature are conveyed to all senior leadership via weekly meetings. If the issue identified is deemed critical, then the <role>works with the <CEO> to reach a resolution.

**RA.L2-3.11.2 - Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified:**

1. [COMPANY NAME] employs [Microsoft Windows Server Update Service (WSUS)] and [Nessus Professional scanning solution from Tenable, managed by SecureStrux (MSSP)] to scan for vulnerabilities associated with the Information System and network components, including hosted applications, patch management, ports, protocols, and services. Microsoft WSUS automatically provides patch management updates weekly, [Nessus Professional vulnerability scanner] is performed on a quarterly basis.
2. [The Nessus Professional vulnerability scanner] scans for vulnerabilities on organizational devices connected to the network (e.g., servers, desktops, laptops, virtual machines, firewalls, switches, printers), creates a prioritized list of asset vulnerabilities ordered by their level of severity and describes each vulnerability and the steps needed to fix it vulnerability scans are performed on applications with the defined frequency.
3. [The Nessus Professional vulnerability scanner] scans for application vulnerabilities, creates a prioritized list of asset vulnerabilities ordered by their level of severity and describes each vulnerability and the steps needed to fix it vulnerability scans are performed on applications with the defined frequency.
4. [The Nessus Professional vulnerability scanner] scans for vulnerabilities on organizational devices connected to the network creates a prioritized list of asset vulnerabilities ordered by their level of severity and describes each vulnerability and the steps needed to fix it vulnerability scans are performed on applications when new vulnerabilities are identified.
5. [The Nessus Professional vulnerability scanner] scans for application vulnerabilities, creates a prioritized list of asset vulnerabilities ordered by their level of severity and describes each vulnerability and the steps needed to fix it vulnerability scans are performed on applications when new vulnerabilities are identified.

* Vulnerability scanning occurs on assets regardless of OS and/or operational context. This includes all [COMPANY NAME] information systems. Vulnerability scanning identifies threats based on impact of exploit to the environment.
* At least weekly, the <role> and/or the <IT Team> review the findings and prioritizes any items that need to be addressed.

**RA.L2-3.11.3 - Remediate vulnerabilities in accordance with risk assessments:**

1. The <role> and <role> performs, reviews, and analyzes vulnerability scan results on a quarterly basis. Vulnerability scanning schedules can occur more frequently dependent continuous monitoring scheduling and risk.
2. The <role>, or designee of, remediate identified vulnerabilities within 30 days of discovery. All other findings are managed and maintained through the continuous monitoring process, in conjunction with the <FSO> and <HR>.

* The <role> creates a prioritized list based on the risk assessment of the vulnerabilities to be fixed and records the status of the actions taken or reasoning of action not taken.
* The <role> and <role> analyzes vulnerability scan reports to determine whether reported vulnerabilities apply to the system (e.g., ensuring identified vulnerabilities are not false positives).
* The <role> and <role> attempts to discern what information about the system is discoverable by adversaries, documents the information, determines associated risk, and takes corrective action to mitigate the findings.
* Vulnerability scan results are reported to the <role>, who shares information obtained from the vulnerability scanning process with the <Security Team> to help eliminate similar vulnerabilities in other Information Systems. Information sharing is done at the discretion of the <Security Team> using secured means of communication.

**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 |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |