# Awareness and Training 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 Awareness and Training of the IT environment at [COMPANY NAME].

# Scope

This procedure is consistent with CMMC and covers all awareness and training 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 800-171, 3.2.1 – 3.2.3
* CMMC AT.L2-3.2.1 – AT.L2-3.2.3
* [COMPANY NAME] – AT – 3.2 – Awareness and Training Policy

# Procedure Statements

**AT.L.2-3.2.1 – Ensure that managers, system administrators and users of organizational systems are made aware of the security risks associated with their activities and of the applicable policies, standards and procedures related to the security of those systems:**

1. Security risks associated with organizational activities involving CUI are identified but not limited to: as phishing attacks, computer hygiene, safe internet searching, and acceptable use of devices and technologies.
2. Policies, standards, and procedures related to the security of the system are identified within the CMMC Domain Package (3.1-3.14 Policies & Procedures) in which staff are required to annually train on.
3. Managers, systems administrators, and users of the system are made aware of the security risks associated with their activities by taking the annual training courses that are preselected per staff member and includes but is not limited to training on phishing attacks, computer hygiene, safe internet searching, and acceptable use of devices and technologies. Courses are preselected by the <role> to adhere to relevant cybersecurity vulnerabilities and threats.
   * + Current CUI Specific course work, security awareness course list and retention of completed training for users can be located in the individual’s Security Folders maintained on the *<designated repository>* and available upon request.
     + This training is conducted:
       1. As part of initial onboarding training for all new users within *30* days of employment
       2. When required due to changes in the policy and/or major changes in the organization
       3. At least annually for all security and privacy related policies.
     + Additionally, regular updates and reminders are provided to all employees via email and IM channels. As new Security or Privacy training is identified, the <Role> in conjunction with Human Resources reviews the training to determine whom requires the training and how to implement it. All training is created in house or pull from an official Gov’t source by the [COMPANY NAME] IT department.
     + In addition, phishing campaigns are designed by [COMPANY NAME] and provide security awareness to users.
4. Managers, systems administrators, and users of the system are made aware of the applicable policies, standards, and procedures related to the security of the system through their training assignments.

**AT.L2-3.2.2 – Ensure that personnel are trained to carry out their assigned information security- related duties and responsibilities:**

1. Information security-related duties, roles, and responsibilities are defined by HR. Job functions are determined at the time of hiring that govern what training path is required to be completed.
2. [COMPANY NAME] ensures that information security-related duties, roles, and responsibilities are assigned to designated personnel. Courses are preselected per staff member and includes but is not limited to training on phishing attacks, good computer hygiene, safe internet searching and acceptable use of devices and technologies. Courses are preselected by the <role> to adhere to relevant cybersecurity vulnerabilities and threats
3. Personnel are adequately trained to carry out their assigned information security-related duties, roles, and responsibilities. Individuals are required to take role-based training whether that be by research or certification training. This training is to be completed in conjunction with training listed in sections 2.1 Security Awareness Training and 2.3 Insider Threat.

* [COMPANY NAME] requires that all employees and managers take privacy and security training.
* This training is conducted:

1. As part of initial onboarding training for all new users within *30* days of employment
2. When required due to changes in the policy and/or major changes in the organization
3. At least annually for all security and privacy related policies
4. Ensure that personnel are trained to carry out information security related duties through specialized training for information security roles.
5. Ensure that information security roles are trained on new systems, applications, and tools when new systems, applications, and tools are applied to the organizational information system.
   * + Current Role-based course work, security awareness course list and retention of completed training for users can be located in the individual’s Security Folders maintained on the *<designated repository>* and available upon request.

**AT.L2-3.2.3 – Provide security awareness training on recognizing and reporting potential indicators of insider threat.**

1. Potential indicators associated with insider threats are identified in the employee’s training package however includes and not limited to: Unusual logins, Use or repeated attempted use of unauthorized applications, An increase in escalated privileges, excessive downloading of data, and unusual employee behavior.
2. Internal staff is assigned annual security awareness training on recognizing and reporting potential indicators of insider threat that must be completed and returned to Security for tracking. Courses are preselected per staff member and includes training to the process of Insider Threat with focus on internal and external influences. Insider threat courses are preselected by the <role> to adhere to relevant cybersecurity vulnerabilities and threats. [COMPANY NAME] security and privacy training includes provisions that the employee is the greatest strength and weakness to organizational security. Insider threats are identified in training and direction is provided to notify the Insider Threat Team if an issue is believed to be occurring.
   * + Insider Threat training is provided during the initial onboarding training for all new users and within 30 days of employment.
     + Current insider threat course list and retention of completed training for users can be located in the individual’s Security Folders maintained on the *<designated repository>* and available upon request.

# 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 | 12/7/2022 | SecureStrux | Initial Draft |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |