**Onboarding & Annual Training Procedure**

**COMPANY NAME**

**Version #**

**Last Revision Date:**

Document Classification

**Table of Contents**

[Policy Requirement Reference 3](#_Toc47463853)

[Procedure 4](#_Toc47463854)

**Procedure Information**

|  |  |
| --- | --- |
| **Prepared By** | |
| **Name:** |  |
| **Department / Title:** |  |
| **Email Address:** |  |
| **Phone #:** |  |

**Revision History**

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Revision Date** | **Description** | **Pages Affected** |
| 1.0 | [DATE] | Initial version of procedure | All |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Policy Requirement Reference

|  |  |  |
| --- | --- | --- |
| **Control #** | **Control Description / Requirement** | **NIST 800-53** |
| **3.2.1** | Ensure that managers, systems administrators, and users of organizational information 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 organizational information systems. | AT-2 |
| **3.2.2** | Ensure that organizational personnel are adequately trained to carry out their assigned information security-related duties and responsibilities. | AT-3 |
| **3.2.3** | Provide security awareness training on recognizing and reporting potential indicators of insider threat. | AT-2(2) |
| **3.9.1** | Screen individuals prior to authorizing access to information systems containing CUI. | PS-3 |

Procedure

The Organization:

1. Provides computer-based and/or classroom-based security awareness training to all employees and contractors accessing company information systems within 30 days of hire. Training includes, but is not limited to:
   1. Roles and responsibilities in accessing and processing sensitive information;
   2. The nature and categorization of data and information system assets;
   3. Access and authentication requirements for information systems, such as password policy, account usage, and restrictions;
   4. Requirements for the proper handling of sensitive material in paper form, including marking, transmission, storage, and destruction;
   5. Identifying and reporting security incidents, such as phishing emails, malware, and data breach;
   6. Facility security considerations, including physical access restrictions, access badges, incident reporting, and prohibited devices;
   7. Consequences for failing to properly protect information;
   8. Potential indicators and possible precursors of insider threat; and
   9. Reporting potential concerns regarding insider threat through appropriate organizational channels.
2. Conducts refresher security training for all employees and contractors on an annual basis and when new security procedures are published.
3. Ensures that personnel review and acknowledge information security policies and procedures during initial onboarding and annually thereafter.
4. Documents and maintains record of employee training for a minimum of one year.
5. Provides roles-based security training to personnel with assigned security roles and responsibilities, including information security managers / owners and system administrators, within 30 days of performing assigned duties.
6. Promotes security awareness through techniques including posters, logon screen messages, email advisories, and notices from senior organizational officials.

Procedures for screening and rescreening individuals with access to CUI; where re-screening is appropriate frequency of rescreening (i.e. background checks, drug tests, citizenship - must be US persons or US