|  |  |
| --- | --- |
| [Organization Name] | **No:**  [Policy Number] |
| **IT Policy**:  **Security Awareness and Training** | **Updated:** 10/28/2024 |
| **Issued By:**  [Policy Authority]  **Owner:**  [Policy Owner] |

# 1.0 Purpose and Benefits

The purpose of the Security Awareness and Training Policy is to cultivate a security-conscious culture within the organization by providing employees with the essential knowledge and skills to recognize, prevent, and respond to security threats. This policy establishes structured training programs that address general information security principles, specific roles and responsibilities, and awareness of potential insider threats. By fostering a comprehensive understanding of security practices, the policy aims to mitigate risks associated with human error and enhance the overall security posture of the organization.

Implementing the Security Awareness and Training Policy yields several key benefits. Firstly, it empowers employees to identify and report security incidents, reducing the likelihood of successful cyberattacks and breaches. Secondly, it ensures compliance with regulatory and organizational standards, helping to avoid potential penalties or liabilities. Furthermore, the policy promotes a proactive approach to security, encouraging continuous improvement and adaptation to emerging threats. Ultimately, by investing in security training, the organization enhances its resilience against security risks and fosters trust among stakeholders, customers, and partners.

# 2.0 Authority

This policy is established under the authority of organizational management and is guided by best practices outlined in the National Institute of Standards and Technology (NIST) Cybersecurity Framework 2.0. While not mandated by law, the organization adopts this framework to enhance its cybersecurity posture and protect its information assets. The authority for enforcement and adherence to this policy is vested in the [Policy Authority], who is responsible for ensuring compliance across all departments.

# 3.0 Scope

This policy applies to all employees, contractors, third-party vendors, and any individuals or entities accessing, using, or managing the organization's information systems, networks, and physical infrastructure, regardless of the medium or format of the information. It covers all electronic, paper-based, and verbal communication, including, but not limited to, data processing systems, cloud services, email platforms, mobile devices, databases, and other digital storage mechanisms that store, transmit, or process sensitive organizational information.

The policy encompasses internal and external users, whether they access the organization's systems on-site or remotely, and includes all physical infrastructure such as data centers, workstations, and hardware that interact with or support the organization's information environment. Additionally, it extends to any devices, both personal and organizational, that connect to the corporate network or handle company data.

All users are responsible for protecting the confidentiality, integrity, and availability of information, complying with this policy and relevant laws, and familiarizing themselves with the organization's security policies and procedures to ensure the protection of organizational assets. Failure to comply with these requirements may result in disciplinary action, including termination of access rights or contractual agreements.

# 4.0 Information Statement

The Security Awareness and Training Policy is designed to ensure that all personnel are equipped with the knowledge and skills necessary to protect the organization’s information assets. This policy mandates the scheduling of security awareness training for new users and ongoing training at specified intervals or in response to significant changes within the information systems. The training content focuses on the fundamental principles of information security, operations security, and the identification and reporting of insider threats.

Additionally, role-based training is provided for staff with specific security responsibilities, including practical exercises to reinforce learning. The policy also emphasizes the importance of recognizing suspicious communications and anomalous behavior within organizational systems. Continuous monitoring and documentation of training activities ensure that personnel maintain an up-to-date understanding of security protocols, contributing to a robust security culture across the organization.

* 1. Security Awareness Training

The [Owner] shall:

1. Schedule security awareness training as part of initial training for new users.
2. Schedule security awareness training when required by information system changes and then [entity specified frequency] thereafter.
3. Determine the appropriate content of security awareness training and security awareness techniques based on the specific organizational requirements and the information systems to which personnel have authorized access. The content shall:
   1. Include a basic understanding of the need for information security and user actions to maintain security and to respond to suspected security incidents.
   2. Address awareness of the need for operations security. Security awareness techniques can include, for example, displaying posters, offering supplies inscribed with security reminders, generating email advisories/notices from senior organizational officials, displaying logon screen messages, and conducting information security awareness events.
   3. Security Awareness of Insider Threats

The [Owner] shall include security awareness training on recognizing and reporting potential indicators of insider threat.

* 1. Role-Based Security Training

The [Owner] shall:

1. Provide role-based security training to personnel with assigned security roles and responsibilities:
   1. Before authorizing access to the information system or performing assigned duties.
   2. When required by information system changes and [entity specified frequency] thereafter.
2. Designate personnel to receive initial and ongoing training in the employment and operation of environmental controls to include, for example, fire suppression and detection devices/systems, sprinkler systems, handheld fire extinguishers, fixed fire hoses, smoke detectors, temperature/humidity, HVAC, and power within the facility.
   1. Physical Security Controls

The [Owner] shall:

1. Provide initial and ongoing training in the employment and operation of physical security controls; physical security controls include, for example, physical access control devices, physical intrusion alarms, monitoring/surveillance equipment, and security guards (deployment and operating procedures).
2. Identify personnel with specific roles and responsibilities associated with physical security controls requiring specialized training.
   1. Practical Exercises

The [Owner] shall provide practical exercises in security training that reinforce training objectives; practical exercises may include, for example, security training for software developers that includes simulated cyber-attacks exploiting common software vulnerabilities (e.g., buffer overflows), or spear/whale phishing attacks targeted at senior leaders/executives. These types of practical exercises help developers better understand the effects of such vulnerabilities and appreciate the need for security coding standards and processes.

* 1. Suspicious Communications and Anomalous System Behavior

The [Owner] shall provide training to its specified staff on how to recognize suspicious communications and anomalous behavior in organizational information systems.

* 1. Continuous Monitoring

The [Owner] shall:

1. Designate personnel to document and monitor individual information system security training activities including basic security awareness training and specific information system security training.
2. Retain individual training records for a [entity specified amount of time].

# 5.0 Compliance

This policy shall take effect upon publication. Compliance is expected with all enterprise policies and standards. Policies and standards may be amended at any time; compliance with amended policies and standards is expected.

If compliance with this standard is not feasible or technically possible, or if deviation from this policy is necessary to support a business function, entities shall request an exception through the following process.

# 6.0 Policy Exceptions

Requests for exceptions to this policy must be submitted to the [Authority] by the requesting department. Each request should include the scope and justification for the exception, potential risks, proposed mitigation measures, and a timeframe for achieving compliance. The [Authority] will review and discuss these requests with the department.

# 7.0 Definitions of Key Terms

|  |  |
| --- | --- |
| **Term** | **Definition** |
| Information Systems | Any combination of hardware, software, data, and personnel that processes, stores, or transmits information, including but not limited to computers, servers, networks, and applications. |
| Users | Individuals or entities, including employees, contractors, and third-party vendors, who access or interact with the organization’s information systems and data. |
|  |  |

# 8.0 Contact Information

Submit all inquiries and requests for future enhancements to the policy owner at:

[Policy Owner’s Contact Info]

[Organization Address]

# 9.0 Review and Revision

This policy should be reviewed at least annually to keep pace with evolving regulations, threat landscapes, and organizational changes. However, more frequent reviews may be necessary following regulatory updates, cybersecurity incidents, significant technology changes, organizational shifts, or compliance audits. This policy should be revised based on these reviews and those revisions noted below.

|  |  |  |
| --- | --- | --- |
| **Date** | **Description of Change** | **Reviewer** |
|  |  |  |

# 10.0 Related Documents

[National Institute of Standards and Technology (NIST) Special Publication 800-50, Building a Cybersecurity and Privacy Learning Program](https://csrc.nist.gov/pubs/sp/800/50/r1/final)

[National Institute of Standards and Technology (NIST) Special Publications: NIST SP 800-12 – An Introduction to Information Security](https://csrc.nist.gov/pubs/sp/800/12/r1/final)