# Awareness and Training Policy

Version [Revision #]

Last modified: [Last modified date]

Last reviewed: [Last reviewed date]

Last Approval: [Last approval date]

#### *Disclaimer*

*This policy template is created as a useful resource. However, organizations remain fully responsible for the content of their policies. Every organization is unique, and the content and format of this template must be revised to meet your organization’s specific requirements. The set of templates available from Hyperproof is not exhaustive nor inclusive; your organization may choose to use only a portion of them or to split them into multiple policies. Do not rely on this policy template to meet legal, regulatory, or contractual requirements. Review your policy in detail to ensure that it is appropriately tailored to your organization's business objectives.*

### **S**ecurity boundary under scope

1. [List of applicable systems]

### References

1. NIST 800-50: https://csrc.nist.gov/pubs/sp/800/50/r1/ipd
2. ISO/IEC 27001:2022: 7.2, 7.3, A.6.3
3. NIST 800-53 rev. 5: AT-1, AT-2, AT-2(3), AT-3, AT-4, CP-3, IR-2
4. CIS v8: 14.1, 14.2, 14.3, 14.4, 14.5, 14.6, 14.7, 14.8
5. PCI DSS 4.0: 6.2.2, 8.3.8, 9.5.13, 12.6.1, 12.6.2, 12.6.3, 12.6.3.1, 12.6.3.2, 12.10.4, 12.10.4.1
6. AICPA SOC 2 TSC: CC1.4, CC2.2

## Document ownership

 <(Choose from)>

* 1. Policy Owner:
		1. [Owner name] ([Owner email]), [Owner title]
	2. Information Security Officer:
		1. [Information officer name], ([Information officer email]), [Information officer title]
	3. System Owner(s):
		1. [System owner name], ([System owner email]), [System owner title]
	4. Process and Operational Owner(s)
		1. [process owner], ([process owner email]), [process owner title]
	5. System Administrator(s):
		1. [System admin name], ([System admin email]), [System admin title]
	6. Required Dissemination: <(Choose from)>
		1. IT Administrator
		2. Engineering
		3. Product Management
		4. Support
		5. Information Security Team
		6. [Organization name] Leadership Team
		7. Contractors
		8. Vendors
		9. Company Wide
		10. [Organization name] SIRT
	7. Optional Dissemination: <(Choose from)>
		1. IT Administrator
		2. Engineering
		3. Product Management
		4. Support
		5. Information Security Team
		6. [Organization name] Leadership Team
		7. Contractors
		8. Vendors
		9. Company Wide
		10. [Organization name] SIRT

## Purpose

The purpose of this policy is to establish a comprehensive information security and privacy awareness and training program that ensures all employees, contractors, and third-party users understand their roles and responsibilities in protecting the organization's information assets. This policy aims to:

* Enhance the overall security posture of the organization by fostering a culture of security awareness.
* Equip personnel with the necessary knowledge and skills to identify, prevent, and respond to information security and privacy threats.
* Ensure compliance with legal, regulatory, and organizational requirements related to information security and data protection.
* Mitigate risks associated with human factors in information security, such as social engineering attacks and unintentional data breaches.

## Scope

This policy applies to all employees, contractors, and third-party users who have access to the organization's information systems and data. It encompasses:

1. Initial and ongoing information security and privacy training for all personnel.
2. Specialized, role-based training tailored to the specific responsibilities and access levels of different job functions.
3. Regular awareness initiatives to keep security and privacy top of mind for all personnel.
4. Phishing simulations and social engineering tests to evaluate and enhance the effectiveness of the training program.
5. Specific training modules focused on identifying and responding to phishing, social engineering, and business email compromise (BEC) attacks.
6. Continuous evaluation and improvement of the training program to address emerging threats and changes in the regulatory landscape.

## Roles and responsibilities

<(choose from)>

| **Role** | **Person &/or Title** | **Responsibility** |
| --- | --- | --- |
| Plan and Policy Management | [Owner name], **[owner title]** | Establish the controls, implementation, and monitoring strategy for [policy topic] and associated policy and procedure |
| Executive Review | **Executive Team** | Adjusts [policy topic] parameters to meet business requirements and appropriate risk appetite. Approves risk model and supporting risk documentation that applies to the [policy topic] Policy. Reads, understands and approves after appropriate editing, the [policy topic] Policy. |
| Approval and Commitment | **Executive Team** | Responsible for approval, and commitment to information security controls. Members of the leadership team of [Organization] to include [list of executive approvers]. |
| Information System Owner | [Information officer name], **[Information officer title]** | Responsible for the overall implementation, development, integration, modification, or operation and maintenance of configuration management. Develops operational strategies and tactics to comply with configuration management policy in coordination with the information systems administrators, the information security officer, and functional “end users.” |
| Operations | [Operational owner], **Operational owner title]** |  |
| Information Systems Administrators | **System Administrators**  | Effectively manages the daily implementation, monitoring, and maintenance of operational security controls, as directed by the System Owner and Information Security Officer. |
| Human Resource | [HR name], **[HR title]** | Setups HR wellbeing strategies, coordinates travel policy across the organization. Initiates emergency travel considerations, including crisis management when required. |
| End Users |  **End Users** | Users of information systems are required to comply with policy and procedures in the [policy topic] policy. |
| Providers | **[provider type]** | [provider service description] |

## Management commitment

* 1. [Organization] executive management affirms its commitment to the establishment, implementation, resourcing, monitoring, and effectiveness of [policy topic] controls and policy
	2. Management has reviewed and approved this policy.
	3. This policy demonstrates management's commitment to maintaining adequate controls as part of its information security management and privacy objectives. These objectives include compliance with applicable laws, regulatory requirements, executive orders, industry best practices, standards, guidelines, and contractual commitments.
	4. Management agrees to regularly review and update this policy to ensure that it effectively meets the organization’s business and compliance objectives.

## Coordination among organizational entities

1. The [responsible group] creates policy and procedure and is responsible for overall configuration management.
2. Policy and procedures will be reviewed, modified, and disseminated to required consumers.
3. The [responsible group] is responsible for coordinating documentation review and updating the policy.
4. The [responsible group] is responsible for communicating the policy and procedures to applicable required and optional parties.
5. The [responsible group] is responsible for training applicable required and optional parties on compliance with the policy and procedures.

## Compliance

* 1. Employees who violate this policy may be subject to appropriate disciplinary action up to and including discharge as well as both civil and criminal penalties.
	2. Non-employees, including, without limitation, contractors, may be subject to termination of contractual agreements, denial of access to IT resources, and other actions as well as both civil and criminal penalties

## Definitions

* 1. **Awareness Campaign:** A series of coordinated activities designed to increase employee knowledge and understanding of information security and privacy practices.
	2. **Business Email Compromise (BEC):** A type of cyber attack where attackers use email fraud to target organizations with the goal of stealing money or sensitive information.
	3. **Compliance:** Adherence to laws, regulations, guidelines, and specifications relevant to the organization's business processes.
	4. **Data Protection:** The process of safeguarding important information from corruption, compromise, or loss.
	5. **Incident Response:** The approach taken by an organization to prepare for, detect, contain, and recover from a data breach or cyber attack.
	6. **Information Security:** The practice of preventing unauthorized access, use, disclosure, disruption, modification, inspection, recording, or destruction of information.
	7. **ISO/IEC 27001:** An international standard providing a framework for information security management systems (ISMS) to ensure the security of information assets.
	8. **NIST Special Publication 800-53:** A set of guidelines for federal information systems to ensure they meet necessary security and privacy requirements.
	9. **Phishing:** A technique used by attackers to trick individuals into providing sensitive information, such as usernames, passwords, and credit card details, by masquerading as a trustworthy entity in electronic communications.
	10. **Role-Based Training:** Training programs tailored to the specific responsibilities and access levels of different job roles within an organization.
	11. **Security Incident:** Any event that compromises the confidentiality, integrity, or availability of an information system.
	12. **Social Engineering:** Manipulative tactics used by attackers to trick individuals into divulging confidential or personal information that may be used for fraudulent purposes.
	13. **Training Needs Assessment:** A process used to determine what training is necessary for different job roles within an organization to ensure employees have the required knowledge and skills to protect information assets.
	14. **Vulnerability Management:** The practice of identifying, classifying, remediating, and mitigating vulnerabilities within information systems.
	15. **Threat Awareness:** The understanding and recognition of potential security threats and the knowledge of how to respond to them.

## Policy

#### Training Program Development

The [responsible party] is required to:

* + 1. Develop an information security and privacy awareness training program that aligns with organizational policies, legal requirements, and industry best practices, including guidelines from NIST, ISO 27001, and other relevant standards.
		2. Ensure the training program includes materials on security policies, data protection regulations, threat awareness, and best practices for safeguarding sensitive information.
		3. Review and update the training program annually or whenever significant changes to policies, technologies, or regulatory requirements occur.

#### Mandatory Training

The [responsible party] shall:

* + 1. Require all employees, contractors, and third-party users to complete initial information security and privacy training upon hiring or engagement.
		2. Ensure that annual refresher training is mandatory for all personnel to reinforce their understanding and awareness of information security and privacy policies and practices.
		3. Track and document the completion of training by all relevant personnel and provide reports to senior management.

#### Role-Based Training

The [responsible party] is required to:

* + 1. Provide additional, specialized training for employees based on their roles and responsibilities within the organization, ensuring that personnel with access to sensitive information or critical systems receive more comprehensive training.
		2. Tailor training modules to address specific security risks associated with various job functions, including IT staff, human resources, and finance departments.
		3. Develop specialized content and targeted training modules addressing the unique security risks and responsibilities associated with different job functions. This includes:
			1. Executive Management: Training focused on strategic security planning, risk management, and regulatory compliance.
			2. IT Personnel: In-depth training on technical security controls, incident response, system configuration, vulnerability management, and secure coding practices.
			3. Human Resources: Training on handling sensitive employee data, recognizing social engineering tactics, and understanding privacy laws and regulations.
			4. Finance and Accounting: Focused training on safeguarding financial information, recognizing fraudulent activities, and secure payment processing.
			5. Sales, Operations, and Marketing: Education on data privacy, handling customer information securely, and awareness of phishing attempts targeting customer contact lists.
		4. Provide ongoing role-based training to address evolving threats and regulatory changes. Ensure employees receive updates on new security policies, technologies, and practices relevant to their roles.
		5. For those employees with critical incident response roles, incorporate hands-on exercises, simulations, and case studies relevant to each role to enhance understanding and application of security practices.

#### Awareness Initiatives

The [responsible party] shall:

* + 1. Conduct regular information security and privacy awareness campaigns using a variety of methods, such as email reminders, posters, newsletters, and workshops, to keep security top of mind for all personnel.
		2. Develop and disseminate educational materials on emerging threats, security incidents, and best practices for maintaining data protection.

#### Training on Phishing, Social Engineering, and Business Email Compromise

The [responsible party] shall:

* + 1. Develop and deliver specific training modules focused on identifying and responding to phishing attempts, social engineering, and business email compromise (BEC) attacks.
		2. Ensure training includes real-world examples of phishing emails and BEC scams, teaching employees how to recognize common indicators of these threats.
		3. Provide guidelines on safe email practices, such as verifying the authenticity of email senders, not clicking on suspicious links, and reporting suspected phishing attempts to the IT department immediately.
		4. Incorporate interactive elements, such as quizzes and simulations, to enhance the training experience and reinforce learning.

#### Phishing and Social Engineering Tests

The [responsible party] is required to:

* + 1. Implement regular phishing simulations and social engineering tests to evaluate the effectiveness of the training program and the vigilance of employees.
		2. Analyze the results of these tests to identify areas of improvement and adjust training content accordingly.

#### Evaluation and Improvement

The [responsible party] shall:

* + 1. Regularly assess the effectiveness of the information security and privacy awareness and training program through surveys, feedback, and performance metrics.
		2. Use assessment results to make continuous improvements to the program, ensuring it remains relevant and effective in addressing current security challenges.

#### Record Keeping

The [responsible party] is required to:

* + 1. Maintain comprehensive records of all training activities, including attendance logs, training materials, and assessment results.
		2. Ensure that records are stored securely and are accessible for auditing and compliance purposes.

#### Compliance and Enforcement

The [responsible party] shall:

* + 1. Monitor compliance with the information security and privacy awareness and training policy and report non-compliance to senior management.
		2. Implement corrective actions for individuals who fail to complete mandatory training, including additional training sessions and potential disciplinary measures.

## Policy exemptions

* 1. Requests for exceptions to this policy shall be reviewed by the [exemption officer 1] and the [exemption officer 2] and/or the [responsible group].
	2. Employees requesting exceptions shall provide such requests to [exemption communication channel].
	3. The request should specifically state the scope of the exception along with justification for granting the exception, the potential impact or risk attendant upon granting the exception, risk mitigation measures to be undertaken by the [responsible group], initiatives, actions, and a timeframe for achieving the minimum compliance level with the policies set forth herein.

## Related documents

* 1. [list of related documents, including:
		1. Policies
		2. Procedures
		3. Standards
		4. Documentation
		5. Regulations
		6. Legal context

]

## Revision history

* 1. This policy is reviewed and, if necessary, updated annually and may also be updated to reflect changes in the environment.
	2. Every change to this plan must be reviewed and evidence of review and acceptance noted with a signature below. This plan requires the signature of: <(choose from)>
		1. The Information Security Officer
		2. Officer of the [Organization name] Leadership Team
	3. All changes requiring approval must be communicated to the required parties

| **Rev. #** | **Revision Date** | **Description** | **Author** | **Owner** | **Exec. reviewer** |
| --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |

## Approval history

| **Step** | **Approver** | **Job Function** | **Signature** | **Approval Date** |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |