					Insert Registered Legal Entity Name Here							
Document number: P08					Document Title: **Information Security Awareness and Training Policy**							
Version: 1.0		Effective Date: 01.01.2025			Document Owner:							
X	Policy		Standard		Procedure		Form		Register		Other	

Revision history				
Revision number	**Revision Date**	**Changes**	**Reviewed by**	**Process owner**

Approvals			
Name	**Title**	**Date**	**Signature**

Aligned with standards and regulations

Standard/Regulation	Clause/Article	Comment
ISO/IEC 27001:2022	Clause 7.3, Annex A Control 6.3	Establishes awareness and training requirements addressed by this policy
ISO/IEC 27002:2022	Control 6	Supports appropriate role-based awareness training
NIST SP 800-53 Rev.5	AT-1 to AT-5	Aligns with policy and procedures, awareness training, role-based training, training records, and contact with security groups
EU GDPR	Articles 32, 39; Recital 78	Mandates training for personnel handling personal data and general staff awareness
EU NIS2	Articles 21(2)(a, b), 21(3)	Requires risk and security training policies and awareness initiatives
EU DORA	Articles 5, 8, 13	Requires ICT risk awareness and training as part of resilience controls
COBIT 2019	APO07, DSS05, MEA	Reinforces workforce awareness, user education, and compliance monitoring

1. Purpose

1.1 This policy establishes the formal framework to ensure that all personnel are aware of their information security responsibilities and receive the training necessary to protect the Confidentiality, Integrity, and Availability of information assets.

1.2 It supports ISO/IEC 27001 Clause 7.3 and Annex A Control 6.3 by requiring a structured, risk-informed awareness and training framework tailored to organizational roles and evolving threats.

1.3 This policy contributes to reducing human-related vulnerabilities, promoting security-conscious behavior, and continually reinforcing secure practices in line with regulatory and contractual requirements.

2. Scope

2.1 This policy applies to all internal and external individuals with access to organizational information systems, data, or facilities, including:

2.1.1 Employees and contractors (full-time, part-time, temporary workers)

2.1.2 Contractors, third-party service providers, consultants, vendors, and interns

2.1.3 Third parties with logical or physical access under service agreements

2.2 The scope includes:

2.2.1 Initial onboarding security awareness training

2.2.2 Role-specific training (e.g., developers, finance personnel, privileged users)

2.2.3 Periodic refresher training and awareness campaigns

2.2.4 Ad hoc training in response to incidents or new threats

2.3 Training delivery mechanisms covered under this policy include e-learning, in-person briefings, simulations, knowledge tests, posters, newsletters, and mandatory acknowledgments.

3. Objectives

3.1 Ensure that all personnel understand their responsibilities for safeguarding organizational assets and complying with security policies.

3.2 Provide ongoing, measurable awareness training aligned with role-based risk exposure.

3.3 Embed secure behaviors into daily operations by reinforcing practices such as secure password use, incident reporting and management, and phishing resistance.

3.4 Ensure regulatory compliance and audit readiness for information security training requirements across industries and jurisdictions.

3.5 Reduce security incidents resulting from negligence, lack of awareness, or poor judgment through behavioral conditioning and continuous reinforcement.

4. Roles and Responsibilities

4.1 Top Management

4.1.1 Approves the Information Security Training Strategy and ensures it is adequately resourced and embedded in corporate priorities.

4.1.2 Monitors compliance at the management level and enforces adherence to this policy across departments.

4.2 CISO / ISMS Manager

4.2.1 Owns this policy and defines the awareness and training framework in line with risk, compliance, and business needs.

4.2.2 Oversees the design, delivery, tracking, and review of all security training initiatives.

4.2.3 Ensures that training is refreshed periodically and reflects evolving threats and emerging technologies.

[... Sections 4.3–8 are not included in this preview. Purchase the full document to access the complete policy content. ...]

9. Review and Update Requirements

9.1 Review Frequency

9.1.1 This policy and the associated training program must be reviewed:

9.1.1.1 Annually, or

9.1.1.2 Following major incidents involving human error or insider threats

9.1.1.3 When significant new technologies or threats are introduced

9.1.1.4 In response to changes in legal, contractual, or certification obligations

9.2 Review Process

9.2.1 The review shall be led by the CISO in coordination with:

9.2.1.1 Human Resources (HR) and Training departments

9.2.1.2 Legal and Data Protection Officers

9.2.1.3 IT Security and Operational Risk functions

9.2.2 All updates must be:

9.2.2.1 Approved by the ISMS Steering Committee

9.2.2.2 Version-controlled and documented in the ISMS Document Register

9.2.2.3 Communicated to users where material changes affect training scope or responsibilities

9.3 Content Update Governance

9.3.1 Training modules and awareness materials must be reviewed every 12 months to ensure:

9.3.1.1 Relevance to the threat landscape

9.3.1.2 Regulatory accuracy

9.3.1.3 Format compatibility (e.g., accessibility, localization)

9.3.2 Outdated or misleading content must be withdrawn immediately and replaced with approved alternatives.

10. Related Policies and Linkages

10.1 This policy is supported by, and supports the enforcement of:

10.1.1 P01 – Information Security Policy: Establishes security awareness as a foundational control in the organization's Information Security Management System (ISMS).

10.1.2 P03 – Acceptable Use Policy: Requires user acknowledgment during training and clarifies responsibilities associated with daily technology use.

10.1.3 P07 – Onboarding and Termination Policy: Ensures training is embedded at onboarding and tracked throughout employment.

10.1.4 P06 – Risk Management Policy: Links human-centered training to threat modeling and residual risk reduction strategies.

10.1.5 P33 – Audit and Compliance Monitoring Policy: Validates that awareness controls are operational, measurable, and effective during audits.

10.2 Together, these policies form a comprehensive behavioral control framework integrating awareness, accountability, and cultural reinforcement.

11. Reference Standards and Frameworks

11.1 ISO/IEC 27001

11.1.1 Clause 7.3 – Awareness: Requires organizations to ensure that workers are aware of information security policies and their responsibilities. This policy operationalizes that requirement through structured onboarding, periodic training, and measurable campaign participation.

11.1.2 Annex A Control 6.3 – Information Security Awareness, Education, and Training: Fully addressed through initial, role-based, and ongoing training programs tailored to user risk profiles.

11.2 ISO/IEC 27002:2022 – Control 6

11.2.1 Supports the development and delivery of awareness training appropriate to job roles, emphasizing the reinforcement of secure behaviors and periodic updates based on threat intelligence and audit feedback.

11.3 NIST SP 800-53 Rev.5

11.3.1 AT-1 to AT-5 (Awareness and Training Family): This policy aligns with AT-1 (Policy and Procedures), AT-2 (Awareness Training), AT-3 (Role-Based Training), AT-4 (Security Training Records), and AT-5 (Contact with Security Groups).

11.3.2 IA-5, AC-2: Reinforces user responsibility for secure authentication and acceptable use, both of which are central to the behavioral outcomes of awareness programs.

11.3.3 IR-1 through IR-8: Incident response preparedness is strengthened through targeted awareness campaigns and simulations.

11.4 EU GDPR (2016/679)

11.4.1 Article 32 – Security of Processing: Mandates that personnel handling personal data be trained to recognize, prevent, and report risks to personal information. This policy ensures that data handlers and all relevant roles are trained accordingly.

11.4.2 Article 39 – Tasks of the Data Protection Officer: Includes raising awareness and training staff involved in processing operations.

11.4.3 Recital 78: Encourages appropriate awareness measures to ensure robust security practices and adherence to policy.

11.5 EU NIS2 Directive (2022/2555)

11.5.1 Article 21(2)(a, b): Requires entities to adopt policies on risk analysis and security training for all relevant personnel. This policy meets that requirement by establishing continuous, role-sensitive training processes.

11.5.2 Article 21(3): Encourages the promotion of cybersecurity risk awareness among management and staff through awareness initiatives and simulations.

11.6 EU DORA (2022/2554)

11.6.1 Article 13 – Digital Operational Resilience Strategy: Mandates that ICT risk awareness and training form part of the governance model. This policy ensures that human risk is addressed through ongoing education and threat simulation.

11.6.2 Articles 5 and 8: Emphasize the importance of internal control frameworks, of which awareness and training are foundational components for ICT resilience and cyber hygiene.

11.7 COBIT 2019

11.7.1 APO07 – APO07 Manage Human Resources: Reinforces the need to develop awareness of security responsibilities and embed this within workforce management.

11.7.2 DSS05 – DSS05: Establishes controls over user education and incident reporting, both of which are integral to this policy.

11.7.3 MEA03 – Monitor, Evaluate, and Assess Compliance: Requires effectiveness reviews of user behavior and policy adherence, implemented here through phishing tests, quizzes, and awareness campaign metrics.