					[Insert Registered Legal Entity Name Here]								
Document number: P8					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 where applicable		
Standard/Regulation	**Clause/Article**	**Comment**
ISO/IEC 27001:2022	Clause 7.3	
ISO/IEC 27002:2022	Control 6.3	
NIST SP 800-53 Rev.5	AT-1 to AT-5	
EU GDPR	Articles 32, 39; Recital 78	
EU NIS2	Articles 21(2)(a, b), 21(3)	
EU DORA	Articles 5, 8, 13	
COBIT 2019	APO07, DSS05, MEA03	

					[Insert Registered Legal Entity Name Here]									
Document number: P8					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			

1. Purpose

1.1 This policy establishes the formal framework for ensuring all personnel are made 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 and risk-informed awareness and training program tailored to organizational roles and evolving threats.

1.3 The policy contributes to the reduction of human-related vulnerabilities, the promotion of security-conscious behavior, and the continuous reinforcement of 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:

2.1.1.1 Employees (full-time, part-time, temporary)

2.1.1.2 Contractors, consultants, vendors, and interns

2.1.1.3 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, privileged users)

2.2.3 Periodic refreshers and awareness campaigns

2.2.4 Ad hoc training in response to incidents or new threats

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

3. Objectives

3.1 To ensure that all personnel understand their responsibilities in safeguarding organizational assets and complying with security policies.

3.2 To provide ongoing, measurable awareness training aligned to role-based risk exposure.

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

3.4 To ensure regulatory compliance and audit readiness for information security training mandates across industries and jurisdictions.

3.5 To reduce security incidents resulting from negligence, unawareness, or poor judgment through behavioral conditioning and continuous reinforcement.

4. Roles and Responsibilities

4.1 **Executive Management**

4.1.1 Approves the organization's information security training strategy and ensures it is resourced and embedded into corporate priorities.

4.1.2 Monitors compliance at the management level and enforces policy adherence 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.

[.....]

11. Reference Standards and Frameworks

This policy is aligned with globally recognized security and compliance frameworks to ensure personnel are adequately informed, trained, and engaged in protecting the organization's information assets.

ISO/IEC 27001:2022

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.

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.

NIST SP 800-53 Rev.5

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).

IA-5, AC-2: Reinforces user responsibility for secure authentication and acceptable use—core to the behavioral outcomes of awareness programs.

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

EU GDPR (2016/679)

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 data handlers and all relevant roles are trained accordingly.

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

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

EU NIS2 Directive (2022/2555)

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.

Article 21(3): Encourages promoting cybersecurity risk awareness among management and staff through awareness initiatives and simulations.

EU DORA (2022/2554)

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

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

COBIT 2019

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

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

MEA03 – Monitor, Evaluate, and Assess Compliance: Calls for effectiveness review of user behavior and policy adherence—implemented here via phishing tests, quizzes, and awareness campaign metrics.