					Insert Registered Legal Entity Name Here							
Document number: P08S					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	
ISO/IEC 27002:2022	Control 6	
NIST SP 800-53 Rev.5	AT-2, AT-4	
EU NIS2	Article 21(2)(i)	
EU DORA	Article 13	
COBIT 2019	BAI08, DSS05	
EU GDPR	Articles 32, 39	

1. Purpose

1.1. This policy ensures that all Employees and Contractors understand their information security responsibilities.

1.2. It aims to reduce the likelihood of human error, improve the ability to detect and report incidents, and foster a security-aware culture across the organization.

1.3. This policy supports compliance with ISO/IEC 27001, NIS2, GDPR, and DORA by embedding Security Awareness into day-to-day working practices and role-based expectations.

2. Scope

2.1. This policy applies to all employees, contractors, interns, and third parties who have access to company systems or data.

2.2. It includes:

2.2.1. Initial onboarding Security Awareness training for new personnel

2.2.2. Annual refresher training

2.2.3. Ad hoc training activities (e.g., incident-related updates, posters, or tips)

2.3. This policy applies across all job roles, Departments, and work locations.

3. Objectives

3.1. Ensure all staff receive timely, understandable, and relevant Security Awareness training.

3.2. Enable employees to identify and avoid common threats such as phishing, malware, and data leakage.

3.3. Establish documented records of completion to demonstrate compliance with legal, contractual, and audit requirements.

3.4. Maintain up-to-date training content that reflects the organization’s policies, threat landscape, and applicable regulations.

3.5. Foster a proactive mindset among staff whereby security is treated as part of their day-to-day responsibilities.

4. Roles and Responsibilities

4.1. General Manager

4.1.1. Approves training requirements and ensures appropriate resources are allocated.

4.1.2. Reviews completion reports and escalates non-compliance where necessary.

4.2. Office Manager / Human Resources (HR)

4.2.1. Coordinates training delivery for new hires and annual refresher training.

4.2.2. Maintains training records and completion logs.

4.2.3. Ensures staff acknowledge core security policies and Non-Disclosure Agreements (NDAs).

[... 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. Annual Review

9.1.1. This policy must be reviewed annually by the General Manager and Human Resources (HR) to ensure it reflects current risks, regulatory requirements, and workforce needs.

9.2. Interim Updates

9.2.1. Policy and training content must also be reviewed and revised following:

9.2.1.1. A significant security incident

9.2.1.2. Legal or contractual changes

9.2.1.3. Organizational restructuring or system migrations

9.3. Version Control and Distribution

9.3.1. Every update must include:

9.3.1.1. Version number and effective date

9.3.1.2. Summary of changes

9.3.1.3. Approval by the General Manager

9.3.1.4. An archive of all prior versions retained for at least three years

9.4. Employee Communication

9.4.1. Policy updates must be communicated to all staff, and acknowledgment must be obtained where material changes are made.

10. Related Policies and Linkages

10.1. This policy supports the following:

10.1.1. P2S – Governance Roles and Responsibilities Policy: Assigns responsibility for training coordination and oversight

10.1.2. P3S – Acceptable Use Policy: Reinforces behavioral expectations addressed in training

10.1.3. P4S – Access Control Policy: Ensures users understand the importance of access security

10.1.4. P7S – Onboarding and Termination Policy: Embeds training into the onboarding process

10.1.5. P30S – Incident Response Policy: Ensures staff know how to report incidents promptly and correctly

11. Reference Standards and Frameworks

11.1. ISO/IEC 27001

11.1.1. Clause 7.3 – Requires organizations to ensure personnel are aware of their responsibilities and the security implications of their activities

11.2. ISO/IEC 27002

11.2.1. Control 6.3 – Sets out expectations for the scope and delivery of security awareness, education, and training

11.3. NIST SP 800-53 Rev.5

11.3.1. AT-2 – Requires awareness training for users with system access

11.3.2. AT-4 – Covers role-based training and consequences for non-compliance

11.4. EU GDPR

11.4.1. Article 32 – Requires security measures, including staff training, to protect personal data

11.4.2. Article 39 – Requires Data Protection Officers to oversee awareness and training where applicable

11.5. EU NIS2 Directive

11.5.1. Article 21(2)(i) – Requires ongoing cybersecurity awareness and training programs

11.6. EU DORA

11.6.1. Article 13 – Requires financial entities to implement education and training for all staff with ICT-related responsibilities

11.7. COBIT 2019

11.7.1. BAI08 – Manage Knowledge: Ensures staff are competent and appropriately trained

11.7.2. DSS05 – Manage Security Services: Emphasizes awareness as a key protective control