					[Insert Registered Legal Entity Name Here]						
Document number: P8S					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-2, AT-4	
EU NIS2	Article 21(2)(i)	
EU DORA	Articles 13	
COBIT 2019	BAI08, DSS05	
EU GDPR	Article 32, 39	

<table>
<tr><td colspan="5"></td><td colspan="7">[Insert Registered Legal Entity Name Here]</td></tr>
<tr><td colspan="5">Document number:
P8S</td><td colspan="7">Document Title:
<b>Information Security Awareness and Training Policy</b></td></tr>
<tr><td colspan="2">Version:
1.0</td><td colspan="3">Effective Date:
01.01.2025</td><td colspan="7">Document Owner:</td></tr>
<tr><td>X</td><td>Policy</td><td></td><td>Standard</td><td></td><td>Procedure</td><td></td><td>Form</td><td></td><td>Register</td><td></td><td>Other</td></tr>
</table>

1. **Purpose**
   - 1.1. This policy ensures that all employees and contractors understand their responsibilities regarding information security.
   - 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. The policy enables compliance with ISO/IEC 27001, NIS2, GDPR, and DORA by making security awareness part of everyday work behavior 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 training for new personnel
     - 2.2.2. Annual security refresher training
     - 2.2.3. Ad hoc awareness activities (e.g., incident-related updates, posters, or tips)
   - 2.3. 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. Provide employees with the ability to identify and avoid common threats such as phishing, malware, and data leaks.
   - 3.3. Establish documentation of training completion to demonstrate compliance with legal, contractual, and audit requirements.
   - 3.4. Maintain up-to-date training content that reflects the organization’s policies, threats, and applicable regulations.
   - 3.5. Foster a proactive mindset among staff where security is considered part of daily responsibility.
4. **Roles and Responsibilities**
   - 4.1. **General Manager**
     - 4.1.1. Approves training requirements and ensures resources are allocated.
     - 4.1.2. Reviews completion reports and escalates non-compliance where necessary.
   - 4.2. **Office Manager / HR**
     - 4.2.1. Coordinates training delivery for new hires and annual refreshers.
     - 4.2.2. Maintains training records and completion logs.
     - 4.2.3. Ensures staff acknowledgment of core security policies and NDAs.
   - 4.3. **Department Managers**
     - 4.3.1. Ensure their teams attend required training.
     - 4.3.2. Follow up on non-completion and support staff participation.
     - 4.3.3. Reinforce key messages in team meetings or one-on-ones.
   - 4.4. **Employees and Contractors**
     - 4.4.1. Must complete training within the assigned timeframe.

4.4.2. Must adhere to the principles taught, including password hygiene, clean desk practices, and reporting suspicious activity.

4.4.3. Are expected to stay alert and responsive to new security communications or updates.

5. Governance Requirements

5.1. Onboarding Awareness Requirements

5.1.1. All new hires must receive an introductory security briefing on:

5.1.1.1. Password and authentication practices

5.1.1.2. Acceptable use of systems

5.1.1.3. Incident reporting expectations

5.1.1.4. Clean desk and remote work security

5.1.2. This briefing must be documented in a centralized training log and signed or acknowledged by the employee.

[.....]