					[Insert Registered Legal Entity Name Here]							
Document number: P30S					Document Title: **Incident Response 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	Clauses 6.1, 6.3, 8.1	
ISO/IEC 27002:2022	Controls 5.24, 5.25	
NIST SP 800-53 Rev.5	IR-4, IR-5, IR-6	
EU GDPR	Article 33	
EU NIS2	Article 23	
EU DORA	Article 17	
COBIT 2019	DSS02, DSS04	

					[Insert Registered Legal Entity Name Here]								
Document number: P30S					Document Title: **Incident Response Policy**								
Version: 1.0		Effective Date: 01.01.2025			Document Owner:								
X	Policy		Standard		Procedure		Form		Register		Other		

1. **Purpose**
   1.1. This policy defines how the organization detects, reports, and responds to information security incidents affecting its digital systems, data, or services.
   1.2. It enables the organization to minimize damage, protect customer data, and meet regulatory obligations such as GDPR's 72-hour breach notification requirement.
   1.3. The policy ensures clear responsibilities, communication steps, and post-incident follow-up, even in small organizations without a dedicated security team.
2. **Scope**
   2.1. This policy applies to:
      2.1.1. All employees, contractors, and external IT service providers
      2.1.2. All company-managed systems and services, including websites, cloud platforms, mobile devices, laptops, and email accounts
      2.1.3. All types of incidents, including:
         2.1.3.1. Unauthorized access to data or systems
         2.1.3.2. Malware infections or ransomware
         2.1.3.3. Phishing or social engineering attempts
         2.1.3.4. System outages due to cyberattack or misuse
         2.1.3.5. Accidental disclosure or deletion of sensitive information
         2.1.3.6. Loss or theft of business devices or storage media
3. **Objectives**
   3.1. Establish a clear process for recognizing and escalating security incidents.
   3.2. Ensure that incidents are reported, logged, and acted upon within predefined timeframes.
   3.3. Enable swift containment of damage, data recovery, and service restoration.
   3.4. Ensure that affected parties (e.g., customers, regulators) are notified when required by law.
   3.5. Prevent recurrence through root cause analysis, corrective action, and policy improvement.
   3.6. Enable SMEs to meet ISO 27001 certification requirements and demonstrate accountability during audits.
4. **Roles and Responsibilities**
   4.1. **General Manager (GM)**
      4.1.1. Owns this policy and ensures it is implemented.
      4.1.2. Oversees incident response activities and approves notifications to regulators or customers.

      [….]

Reference Standards and Frameworks

ISO/IEC 27001:2022

Clause 6.1 – Requires risk treatment planning, including preparation for incidents.

Clause 6.3 – Supports continual improvement through lessons learned from security events.

Clause 8.1 – Emphasizes operational control to manage incidents and disruptions.

ISO/IEC 27002:2022

Control 5.24 – Requires a structured approach for reporting, assessing, and responding to information security incidents.

Control 5.25 – Focuses on learning from incidents to improve future readiness and system resilience.

NIST SP 800-53 Rev.5

IR-4 – Defines incident handling procedures including containment and recovery.

IR-5 – Establishes requirements for incident monitoring and analysis.

IR-6 – Mandates external and internal incident reporting protocols.

EU GDPR

Article 33 – Requires reporting of personal data breaches to regulators within 72 hours, with details on scope and mitigation.

EU NIS2 Directive (2022/2555)

Article 23 – Requires essential and important entities to notify competent authorities of significant incidents using standardized reporting formats.

EU DORA Regulation (2022/2554)

Article 17 – Requires financial entities to classify, report, and track ICT-related incidents and disruptions.

COBIT 2019

DSS02 – Manage Service Requests and Incidents: Guides effective handling of operational and security incidents in line with governance objectives.

DSS04 – Manage Continuity: Connects incident response with broader continuity and recovery strategies.