					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

Standard/Regulation	Clause/Article	Comment
ISO/IEC 27001:2022	Clauses 6.1, 6.3, 8	Incident management, continual improvement, operational control
ISO/IEC 27002:2022	Controls 5.24, 5.25	Incident detection, readiness, learning
NIST SP 800-53 Rev.5	IR-4, IR-5, IR-6	Incident handling and monitoring, reporting
EU GDPR	Article 33	Breach notification requirements
EU NIS2	Article 23	Mandatory cyber incident reporting
EU DORA	Article 17	ICT incident management
COBIT 2019	DSS02, DSS04	Service request and incident management, continuity

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 harm, protect customer data, and meet regulatory obligations such as the GDPR 72-hour personal data breach notification requirement.

1.3. This policy establishes clear responsibilities, communication steps, and post-incident follow-up, including in small organizations without a dedicated Information 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 incident types, 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 caused by cyberattacks 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 identifying and escalating security incidents.

3.2. Ensure that incidents are reported, logged, and addressed within predefined timeframes.

3.3. Enable rapid containment of harm, data recovery, and service restoration.

3.4. Ensure that affected parties, such as customers and regulators, are notified where required by law.

3.5. Prevent recurrence through root cause analysis, corrective actions, 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 its implementation.

4.1.2. Oversees incident response activities and approves notifications to regulators or customers.

4.1.3. Reviews post-incident reports and ensures that policy updates are made where required.

4.1.4. May delegate coordination duties but retains accountability.

4.2. IT Provider / System Administrator (internal or external)

4.2.1. Detects and investigates potential security incidents.

4.2.2. Implements containment and recovery actions, for example by disabling access or restoring backups.

4.2.3. Notifies the General Manager of all confirmed or suspected incidents within one hour of discovery.

4.2.4. Maintains an incident log with timestamps, impact assessments, and response actions.

[... 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. Scheduled Review

9.1.1. This policy must be reviewed at least once every 12 months by the General Manager (GM) to ensure:

9.1.1.1. Alignment with ISO/IEC 27001:2022 controls

9.1.1.2. Responsiveness to new threats, risks, and incidents

9.1.1.3. Ongoing compliance with legal and contractual obligations, for example GDPR and DORA

9.2. Trigger Events

9.2.1. This policy must also be reviewed and updated following:

9.2.1.1. Any high-severity incident or regulatory notification

9.2.1.2. Introduction of new IT infrastructure or system changes

9.2.1.3. Amendments to legal requirements relating to security breaches

9.3. Review Documentation and Distribution

9.3.1. All reviews and changes must be documented in the policy change log.

9.3.2. Updated versions must be distributed to all employees, vendors, and IT providers involved in security or system operations.

9.3.3. Evidence of staff awareness, for example meeting notes or email confirmations, must be retained for audit readiness.

10. Related Policies and Linkages

10.1. This policy must be applied in coordination with the following SME policies:

10.1.1. P1S – Information Security Policy: Sets the overall expectations for maintaining confidentiality, integrity, and availability during operations, including incident handling.

10.1.2. P2S – Governance Roles and Responsibilities Policy: Establishes authority and accountability structures for incident detection, reporting, and escalation.

10.1.3. P4S – Access Control Policy: Enables immediate access revocation during incident response actions.

10.1.4. P8S – Information Security Awareness and Training Policy: Ensures all employees can identify and report security incidents effectively.

10.1.5. P17S – Data Protection and Privacy Policy: Guides legal personal data breach notification procedures under GDPR and supports regulatory compliance during incidents.

10.1.6. P22S – Logging and Monitoring Policy: Provides the necessary tools and visibility for detecting, analyzing, and auditing security events.

10.1.7. P31S – Evidence Collection and Forensics Policy: Supports investigation and legal defensibility of incident-related actions by guiding proper evidence handling.

10.2. These policies collectively establish the SME operational framework for detecting, responding to, and recovering from information security incidents.

11. Reference Standards and Frameworks

11.1. ISO/IEC 27001

11.1.1. Clause 6.1 – Requires risk treatment plan activities, including preparation for incidents.

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

11.1.3. Clause 8.1 – Emphasizes operational control for managing incidents and disruptions.

11.2. ISO/IEC 27002

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

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

11.3. NIST SP 800-53 Rev.5

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

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

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

11.4. EU GDPR

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

11.5. EU NIS2 Directive (2022/2555)

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

11.6. EU DORA Regulation (2022/2554)

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

11.7. COBIT 2019

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

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