					Insert Registered Legal Entity Name Here							
Document number: P30					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	Clause 8.1, Clause 9	Structured processes for risk management and incident response
ISO/IEC 27002:2022	Controls 5.25–5.27	Roles, reporting, response, and improvement for incidents
NIST SP 800-53 Rev.5	IR-1 through IR-9	Comprehensive incident response lifecycle
EU GDPR	Article 33(1), 33(3)(a)–(d), 34(1), 34(2)(a)–(c)	Breach notification timelines, reporting, and communication with data subjects
EU NIS2	Article 23(1)–(4)	Notification to national authorities and structured reporting
EU DORA	Article 17(1)–(3)	Reporting of major ICT-related incidents for financial entities
COBIT 2019	DSS02, DSS04, MEA	Defines, monitors, and assesses incident management, continuity, and evaluation

1. Purpose

1.1 This policy establishes a formal framework for the identification, reporting, analysis, containment, response, recovery, and post-incident evaluation of information security incidents affecting the organization.

1.2 It ensures timely, coordinated, and effective responses to minimize operational disruption, financial loss, reputational damage, and regulatory non-compliance.

1.3 This policy also supports continuous improvement of the organization's cyber resilience through lessons learned and the integration of post-incident findings into governance, tooling, and training programs.

2. Scope

2.1 This policy applies to:

2.1.1 All personnel, including employees, contractors, consultants, and third-party service providers

2.1.2 All information systems, applications, infrastructure, networks, and data, whether on-premises, cloud-based, or hybrid

2.1.3 All types of security incidents, including but not limited to:

2.1.3.1 Unauthorized access or privilege escalation

2.1.3.2 Malware and ransomware attacks

2.1.3.3 Denial-of-service (DoS/DDoS) attacks

2.1.3.4 Data loss, leakage, or exfiltration

2.1.3.5 Insider misuse or policy violations

2.1.3.6 Physical security breaches affecting digital assets

2.2 This policy covers detection, triage, investigation, escalation, containment, evidence handling, notification, recovery, and root cause analysis.

3. Objectives

3.1 To establish a repeatable and scalable incident response capability that enables rapid detection, classification, and mitigation of security incidents.

3.2 To minimize the business impact of security events through structured containment, eradication, and system recovery procedures.

3.3 To ensure incident reporting and response are aligned with legal, regulatory, and contractual requirements, particularly those relating to breach notification timelines and evidence handling.

3.4 To support transparency and accountability through appropriate logging, documentation, and metric tracking for all security incidents.

3.5 To drive continuous improvement through post-incident reviews, corrective actions, and stakeholder training.

4. Roles and Responsibilities

4.1 Chief Information Security Officer (CISO)

4.1.1 Owns the incident response framework, ensures enforcement of this policy, and oversees organization-wide incident coordination.

4.1.2 Acts as the primary liaison with regulators, executive management, and external legal counsel during major incidents.

4.2 Incident Response Coordinator

4.2.1 Coordinates cross-functional response teams, manages response workflows, and tracks containment and recovery status.

4.2.2 Initiates and leads Post-Incident Reviews (PIRs) and ensures corrective actions are recorded and implemented.

[... 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 This policy must be reviewed at least annually and revised as necessary to incorporate:

9.1.1 Changes in the threat landscape, incident types, or attack vectors

9.1.2 Lessons learned from major incidents, near misses, or regulatory findings

9.1.3 Updates to applicable laws and regulations (e.g., GDPR, DORA, NIS2)

9.1.4 Feedback from incident response exercises and post-incident reviews

9.2 The CISO is responsible for initiating and coordinating the review process, in consultation with:

9.2.1.1 Legal Counsel and the DPO

9.2.1.2 SOC and IT Operations

9.2.1.3 Business Continuity and Risk Management teams

9.2.1.4 Executive Management

9.3 Policy changes must be:

9.3.1 Documented in a version-controlled repository

9.3.2 Communicated to all affected teams and reflected in awareness training

9.3.3 Validated through tabletop exercises or live incident response exercises within three months of approval

9.4 Urgent updates triggered by emerging threats, audit findings, or newly issued legal obligations must be implemented immediately and recorded in the policy revision history.

10. Related Policies and Linkages

10.1 This policy is supported by, and dependent upon, the following organizational policies:

10.1.1 P1 – Information Security Policy: Establishes the overarching requirement for risk-based, incident-ready operations.

10.1.2 P5 – Change Management Policy: Ensures that containment and recovery activities involving infrastructure or services follow formal procedures.

10.1.3 P13 – Data Classification and Labeling Policy: Supports incident severity classification based on data sensitivity.

10.1.4 P15 – Backup and Restore Policy: Enables recovery from ransomware or destructive attacks with assurance of integrity.

10.1.5 P18 – Cryptographic Controls Policy: Defines encryption measures that reduce incident impact and data exposure risk.

10.1.6 P22 – Logging and Monitoring Policy: Provides the foundational event visibility, alerting, and log retention required for effective detection and forensic investigation.

10.1.7 P29 – Test Data and Test Environment Policy: Ensures that incidents affecting non-production systems are also handled in a structured and secure manner.

10.1.8 P33 – Audit and Compliance Monitoring Policy: Validates incident readiness and response effectiveness through structured audits and compliance assessments.

11. Reference Standards and Frameworks

11.1 ISO/IEC 27001: Clause 8.1 – Operational Planning and Control: Structured processes to manage risks and plan incident response.

11.2 ISO/IEC 27002:2022 – Controls 5.25–5.27: Responsibilities for incident management, reporting, response, communication, and improvement.

11.3 NIST SP 800-53 Rev.5: IR-1 through IR-9, AU-6, PL-2: Comprehensive requirements for the incident response lifecycle, audit, and security planning.

11.4 EU GDPR: Articles 33 and 34: Reporting obligations to supervisory authorities and notification requirements for data subjects, including defined exceptions.

11.5 EU NIS2 Directive (2022/2555): Article 23: Mandatory national reporting, including intermediate and final reporting obligations.

11.6 EU DORA (2022/2554): Article 17: ICT incident reporting requirements for financial institutions to competent authorities.

11.7 COBIT 2019: DSS02, DSS04, MEA01: Service incident and continuity management, together with performance and conformance monitoring.