					Insert Registered Legal Entity Name Here							
Document number: P22					Document Title: **Logging and Monitoring 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**

1. Purpose

1.1 The purpose of this policy is to establish clear and enforceable requirements for the generation, protection, review, and analysis of logs that capture key system and security events across the organization's IT infrastructure.

1.2 Audit logging, monitoring, and threat detection are critical for anomaly detection, threat response, forensic review, audit readiness, and legal compliance. This policy ensures that all system-generated events are properly recorded, retained, and correlated with time-synchronized accuracy.

1.3 This policy is essential to support ISO/IEC 27001 Clause 8.1 and Annex A Controls 8.15 (Logging), 8.16 (Monitoring), and 8.17 (Clock Synchronization), and is directly mapped to regulatory obligations under GDPR, NIS2, DORA, and COBIT 2019.

2. Scope

2.1 This policy applies to all systems, services, and environments that store, process, or transmit data covered under the Information Security Management System (ISMS), including:

2.1.1 On-premises infrastructure, cloud-based services (e.g., IaaS, PaaS, SaaS), and hybrid environments

2.1.2 Operating systems, databases, applications, and network appliances

2.1.3 Security systems such as SIEM platforms, firewalls, endpoint protection (AV/EDR) platforms, VPN concentrators, and identity providers

2.2 The following stakeholders are within scope:

2.2.1 Internal users with system or administrative privileges

2.2.2 IT infrastructure and IT operations personnel

2.2.3 Security Operations Center (SOC) and threat detection teams

2.2.4 Software developers and application owners

2.2.5 Third-party service providers managing log-producing systems

3. Objectives

3.1 Ensure that all critical systems generate security event logs and system activity records that are retained in accordance with regulatory, legal, and contractual requirements.

3.2 Define the minimum event types and log content required to detect unauthorized activities, trace user actions, and support forensic review.

3.3 Enforce protections to prevent log tampering, unauthorized deletion, or uncontrolled access to log data.

3.4 Establish centralized logging and alerting systems (e.g., SIEM) to aggregate, correlate, and escalate suspicious activity in near real time.

3.5 Ensure synchronization of system clocks to enable accurate cross-system correlation and incident analysis.

3.6 Enable continual improvement and compliance by integrating log monitoring with audit and compliance, risk management, and incident reporting and management processes.

4. Roles and Responsibilities

4.1 Chief Information Security Officer (CISO)

4.1.1 Owns this policy and ensures it is aligned with the organization's risk posture, audit requirements, and ISMS obligations.

4.1.2 Approves the logging scope for regulated or high-risk systems and oversees compliance reporting.

4.2 Security Operations Center (SOC) Manager

4.2.1 Operates and maintains centralized log management platforms (e.g., SIEM).

4.2.2 Defines log aggregation rules, alert thresholds, and escalation paths for incident triage.

4.2.3 Reviews daily reports and ensures anomalies are analyzed, documented, and escalated as needed.

[... 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 annually, or sooner in response to:

9.1.1 Major changes in system architecture or logging infrastructure (e.g., SIEM migration)

9.1.2 Revisions to regulatory logging requirements (e.g., NIS2, DORA logging mandates)

9.1.3 Audit findings or incident post-mortems

9.1.4 Emerging threats requiring enhanced monitoring (e.g., insider threats, supply chain compromise)

9.2 The review process shall be led by the Security Operations Center (SOC) Manager in coordination with the CISO, Risk Management, compliance teams, and IT infrastructure teams.

9.3 Approved changes must be version-controlled in the ISMS Document Control Register and communicated to:

9.3.1 All stakeholders responsible for logging system maintenance

9.3.2 Application owners and system owners

9.3.3 Third-party providers with telemetry or SIEM integration responsibilities

9.4 All superseded versions must be securely archived, with access restricted to authorized ISMS custodians for audit and legal purposes.

10. Related Policies and Linkages

10.1 P1 – Information Security Policy. Establishes the foundational commitment to protect systems and data, under which logging and monitoring serve as critical detective and response capabilities.

10.2 P4 – Access Control Policy. Ensures that privileged access, user logins, and authorization events are captured in logs and monitored for misuse or anomalous behavior.

10.3 P5 – Change Management Policy. Requires logging of system changes, patch deployments, and configuration updates that may introduce risk or unauthorized modifications.

10.4 P21 – Network Security Policy. Requires network-level logging (e.g., firewall logs, IDS/IPS alerts, VPN activity) and integration with SIEM to provide visibility into traffic anomalies and boundary protection.

10.5 P23 – Time Synchronization Policy. Enforces clock consistency across systems, which is essential for reliable logging and correlation of security events across multiple environments.

10.6 P30 – Incident Response Policy. Relies on log data and alerting mechanisms to identify, investigate, and respond to security incidents, while also preserving forensic artifacts for post-incident review.

11. Reference Standards and Frameworks

11.1 ISO/IEC 27001

11.1.1 Clause 8.1 – Operational Planning and Control: Requires controls for monitoring operations and safeguarding against unauthorized access and system misuse.

11.2 ISO/IEC 27002:2022 – Controls 8.15, 8.16, 8

11.2.1 Defines detailed logging requirements, including which events must be recorded, how logs must be protected and analyzed, and how timestamp reliability must be ensured across systems.

11.3 NIST SP 800-53 Rev.5

11.3.1 AU-2 to AU-12: Covers event selection, logging, protection, audit review, response to audit failures, and audit record retention.

11.3.2 SI-4 – System Monitoring: Requires active monitoring with alerts based on anomalous activity.

11.3.3 SC-45 – System Time Synchronization: Reinforces time accuracy for event traceability and incident correlation.

11.4 EU GDPR (2016/679)

11.4.1 Article 32 – Security of Processing: Requires technical controls such as logging and monitoring to ensure security and accountability, particularly for access to personal data (PII).

11.5 EU NIS2 Directive (2022/2555)

11.5.1 Article 21(2)(e): Requires event logging and monitoring systems for rapid detection of and response to security incidents.

11.6 EU DORA (2022/2554)

11.6.1 Article 9 – ICT Risk Management: Requires mechanisms to detect anomalous activity, log incidents, and retain forensic data.

11.6.2 Article 11 – Testing of ICT Business Continuity Plans: Emphasizes continuity of monitoring and validation of log availability during operational disruptions.

11.7 COBIT 2019

11.7.1 DSS01.05 – Manage Security Logs: Requires implementation of logging capabilities for all critical infrastructure.

11.7.2 DSS05.04 – Monitor Security Events: Requires real-time monitoring and analysis of logs to detect and respond to events.

11.7.3 MEA03 – Monitor, Evaluate, and Assess Compliance: Requires regular review of logging practices and alignment with control objectives.