Document number: P22		Document Title: **Logging and Monitoring Policy**
Version: 1.0	Effective Date:	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 8.1	
ISO/IEC 27002:2022	Controls 8.15–8.17	
NIST SP 800-53 Rev.5	AU-2 to AU-12, SI-4, SC-45	
EU GDPR	Article 32	
EU NIS2	Article 21(2)(e)	
EU DORA	Articles 9, 11	
COBIT 2019	DSS01.05, DSS05.04, MEA03	

Document number: P22					Document Title: **Logging and Monitoring Policy**						
Version: 1.0		Effective Date:			Document Owner:						
X	Policy		Standard		Procedure		Form		Register		Other

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 environment.

1.2 Logging and monitoring are critical for anomaly detection, threat response, forensic investigation, 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 for supporting 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 SIEMs, firewalls, 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 Infrastructure and IT operations staff

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 investigations.

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 continuous improvement and compliance by integrating log monitoring with audit, risk, and incident 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 organizational 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 incident triage escalation paths.

[…..]

11. Reference Standards and Frameworks

This policy aligns with key international standards and regulatory frameworks requiring robust log generation, protection, monitoring, and correlation capabilities.

ISO/IEC 27001:2022

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

ISO/IEC 27002:2022 – Controls 8.15, 8.16, 8.17

Defines detailed logging requirements, including what events must be recorded, how to protect and analyze logs, and how to ensure timestamp reliability across systems.

NIST SP 800-53 Rev.5

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

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

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

EU GDPR (2016/679)

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

EU NIS2 Directive (2022/2555)

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

EU DORA (2022/2554)

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

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

COBIT 2019

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

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

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