Document number: P22S					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**

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	
EU GDPR	Articles 5(1)(f), 32, 33	
EU NIS2	Articles 21(2)(d), 23	
EU DORA	Articles 10, 15	
COBIT 2019	DSS01.03, DSS05.02	

Document number: P22S					Document Title: **Logging and Monitoring Policy**								
Version: 1.0		Effective Date: **01.01.2025**			Document Owner:								
X	Policy		Standard		Procedure		Form		Register		Other		

1. **Purpose**
   1.1. This policy establishes mandatory logging and monitoring controls to ensure the security, accountability, and operational integrity of the organization's IT systems.
   1.2. It defines the types of events that must be logged, how logs are stored, how they are reviewed, and the responsibilities of staff and service providers.
   1.3. Logging and monitoring support threat detection, regulatory compliance, incident response, and forensic analysis.
   1.4. This policy enables the organization to meet the operational control requirements of ISO/IEC 27001:2022 and supports ongoing audit-readiness, customer trust, and compliance with GDPR, NIS2, and DORA.
2. **Scope**
   2.1. This policy applies to all systems and users within the organization, including:
      2.1.1. Workstations, laptops, servers, firewalls, switches, routers, and wireless access points
      2.1.2. Cloud services used for business operations (e.g., email, file storage, backups, collaboration tools)
      2.1.3. Logging functions on antivirus software, applications, operating systems, and network equipment
      2.1.4. All employees, contractors, and managed service providers (MSPs) who use or administer systems
      2.1.5. Any location where company IT systems are used, including remote, hybrid, or BYOD environments
   2.2. The policy also applies to logs generated by third-party services where the organization has administrative access or contractual audit rights.
3. **Objectives**
   3.1. Ensure logging of system activity, including authentication, configuration changes, access to sensitive data, and security alerts
   3.2. Maintain secure and accurate logs to detect policy violations, system errors, or unauthorized actions
   3.3. Enable rapid review of logs during incidents, investigations, and audits
   3.4. Support time synchronization to ensure integrity and correlation of log data
   3.5. Protect logs from tampering, loss, or premature deletion
   3.6. Fulfill legal and regulatory obligations for system accountability, traceability, and breach response
4. **Roles and Responsibilities**
   4.1. **General Manager (GM)**
      4.1.1. Approves this policy and ensures implementation across all business systems
      4.1.2. Reviews high-severity alerts and serious audit findings reported by IT or privacy functions
      4.1.3. Signs off on exceptions where logging or retention cannot be technically enforced
   4.2. **IT Support Provider / Internal IT Role**
      4.2.1. Implements and configures logging for operating systems, network devices, antivirus tools, and key applications
      4.2.2. Ensures logs are retained, backed up, and protected from alteration
      4.2.3. Reviews logs on a scheduled basis and investigates suspicious or unauthorized activity
      4.2.4. Maintains alerting systems that flag anomalous behavior or intrusion indicators
   4.3. **Privacy Coordinator / Data Protection Lead**

4.3.1. Verifies that log data relating to personal or sensitive information is handled in line with GDPR and other data protection laws

4.3.2. Supports investigations involving access to personal data or security events affecting user confidentiality

4.3.3. Ensures logs are used in incident response, breach notification analysis, and internal reviews

4.4. **All Staff and Contractors**

4.4.1. Must not disable or interfere with system logging or alert mechanisms

4.4.2. Must promptly report system error messages, failed login attempts, or other anomalies

[……]

11. Reference Standards and Frameworks

ISO/IEC 27001:2022

Clause 8.1 – Requires implementation of operational controls to mitigate information security risks, including logging.

ISO/IEC 27002:2022

Control 8.15 – Requires event logging to support anomaly detection and accountability.

Control 8.16 – Requires protection of logs from tampering and unauthorized access.

Control 8.17 – Requires monitoring systems for unusual activity and confirming the effectiveness of

NIST SP 800-53 Rev.5

AU-2 to AU-12 – Cover audit log content, review, retention, and automated alerting.

SI-4 – Requires detection of system anomalies and reporting of suspicious events.

EU GDPR

Article 5(1)(f) – Requires integrity and confidentiality of personal data, which includes logging of access.

Article 32 – Mandates technical and organizational measures to ensure security, including logging and monitoring.

Article 33 – Requires timely breach notification, supported by logs that enable root cause analysis.

EU NIS2 Directive

Article 21(2)(d) – Requires logging mechanisms that detect anomalies and provide support during incident investigations.

Article 23 – Mandates reporting of incidents within 24 hours, which depends on accurate and timely log data.

EU DORA

Article 10 – Requires digital operational resilience, including traceability of ICT-related incidents through logging.

Article 15 – Obligates monitoring of service providers, including log access and review rights.

COBIT 2019

DSS01.03 – Requires traceability of system activity through logging and monitoring.

DSS05.02 – Addresses logging as a key control in protecting against malware and other unauthorized activity.