| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | Insert Registered Legal Entity Name Here | | | | | | | |
| Document number:<br>P22S | | | | | Document Title:<br>**Logging and Monitoring Policy** | | | | | | | |
| Version:<br>1.0 | | Effective Date:<br>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 | Operational controls, including logging |
| ISO/IEC 27002:2022 | Controls 8.15, 8.16, 8.17 | Event logging, log protection, and monitoring |
| NIST SP 800-53 Rev.5 | AU-2 to AU-12, SI-4 | Audit log content and review, retention, anomaly detection, and alerting |
| EU GDPR | Articles 5(1)(f), 32, 33 | Data confidentiality and integrity, technical measures, and breach notification |
| EU NIS2 | Articles 21(2)(d), 23 | Logging mechanisms for anomaly detection and incident reporting within 24 hours |
| EU DORA | Articles 10, 15 | Operational resilience and service provider monitoring/logging |
| COBIT 2019 | DSS01.03, DSS05.02 | Traceability of activity and protection through logging/monitoring |

**1. Purpose**

1.1 This policy establishes mandatory audit logging, monitoring, and threat detection 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 must be stored, how they must be reviewed, and the responsibilities of personnel and service providers.

1.3 Logging and monitoring support threat detection, regulatory compliance, incident reporting and management, and forensic analysis.

1.4 This policy enables the organization to meet the operational control requirements of ISO/IEC 27001 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 access, hybrid, or BYOD environments

2.2 This 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 timely review of logs during incidents, investigations, and audits

3.4 Support time synchronization to ensure the 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 its implementation across all business systems

4.1.2 Reviews high-severity alerts and significant audit findings reported by IT or privacy functions

4.1.3 Approves 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 against alteration

4.2.3 Reviews logs according to schedule and investigates suspicious or unauthorized activity

4.2.4 Maintains alerting systems that identify anomalous behavior or indicators of compromise

[ ... 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 Annual Review

9.1.1 This policy must be reviewed at least annually by the General Manager, with support from the IT Support Provider and the Privacy Coordinator.

### 9.2 Review Triggers

#### 9.2.1 Unscheduled reviews must be conducted in response to:

9.2.1.1 Log-related findings from internal or external audits

9.2.1.2 Security incidents where logs were missing, corrupted, or insufficient

9.2.1.3 Material changes to IT infrastructure (e.g., migration to cloud logging platforms)

9.2.1.4 Updates to legal or regulatory obligations (e.g., GDPR, NIS2, DORA)

### 9.3 Version Control

9.3.1 All changes to this policy must be recorded with the version number, date, and summary of revisions

9.3.2 Previous versions must be archived and retained for at least 3 years

9.3.3 Updated policies must be communicated to affected stakeholders, especially those with system-level access

## 10. Related Policies and Linkages

### 10.1 This policy directly supports, and is supported by, the following SME information security policies:

10.1.1 P17S – Data Protection and Privacy Policy: Ensures that log data containing personal information (PII) is managed with appropriate integrity, retention, and access controls in line with GDPR requirements.

10.1.2 P21S – Network Security Policy: Provides the foundation for capturing logs related to firewalls, wireless access, VPNs, and network segmentation monitoring.

10.1.3 P24S – Secure Development Policy: Ensures that application logging (e.g., login attempts, errors, and exceptions) is incorporated into software design and operations.

10.1.4 P30S – Incident Response Policy: Relies on accurate and complete log data to detect, analyze, and respond to information security events.

10.1.5 P23S – Time Synchronization Policy: Ensures consistent and traceable timestamps across all systems, enabling log correlation during investigations.

## 11. Reference Standards and Frameworks

### 11.1 ISO/IEC 27001

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

### 11.2 ISO/IEC 27002

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

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

11.2.3 Control 8.17 – Requires monitoring for unusual activity and confirmation of the effectiveness of monitoring controls.

### 11.3 NIST SP 800-53 Rev.5

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

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

### 11.4 EU GDPR

11.4.1 Article 5(1)(f) – Requires the integrity and confidentiality of personal data, including logging of access.

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

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

### 11.5 EU NIS2 Directive

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

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

### 11.6 EU DORA

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

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

### 11.7 COBIT 2019

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

11.7.2 DSS05.02 – Addresses logging as a key control for protection against malware and other unauthorized activity.