					Insert Registered Legal Entity Name Here							
Document number: P23S					Document Title: **Time Synchronization 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	Relevant control requirements
ISO/IEC 27002:2022	Control 8	Synchronized system operation
NIST SP 800-53 Rev.5	SC-45, AU-8	Trusted NTP and log timestamp accuracy
EU GDPR	Articles 5(1)(d), 32	Accuracy, accountability, and integrity in personal data with synchronized timestamps
EU NIS2	Article 21(2)(d)	Monitoring and detection capabilities supported by synchronized logs
EU DORA	Articles 10, 15	Operational resilience and accurate technical records
COBIT 2019	DSS05.02, MEA03	Timestamped events and evidence-based monitoring

1. Purpose

1.1 This policy establishes mandatory controls to maintain accurate, synchronized time across all systems that store, transmit, or process organizational data.

1.2 Time synchronization is essential to ensure that system logs are traceable, security incidents can be accurately correlated, and evidence is reliable for forensic analysis or legal review.

1.3 The organization mandates automated time synchronization as a foundational requirement for audit integrity, incident response, and regulatory compliance under ISO 27001, GDPR, DORA, and NIS2.

1.4 This policy ensures that all systems use trusted time sources, prohibits manual override of time settings, and requires timely correction of clock drift.

2. Scope

2.1 This policy applies to:

2.1.1 All company-owned systems and devices, including servers, desktops, laptops, mobile devices, firewalls, routers, and virtual machines

2.1.2 Remote and cloud-hosted systems used in operations (e.g., AWS, Microsoft 365, SaaS platforms)

2.1.3 Systems that generate or store event logs, authentication records, or audit trails

2.1.4 Any employee, contractor, vendor, or IT support provider responsible for configuring or maintaining these systems

2.2 This policy also applies to BYOD (Bring Your Own Device) endpoints used to access business systems, where those endpoints store or generate audit-relevant data.

3. Objectives

3.1 Ensure that all critical systems automatically synchronize time using trusted Network Time Protocol (NTP) servers or equivalent cloud-provider mechanisms

3.2 Prevent time discrepancies that could undermine the reliability or correlation of system logs during audits or security investigations

3.3 Enable timely detection and correction of time drift beyond acceptable thresholds

3.4 Maintain consistent timestamping across on-premises, cloud, and remote environments

3.5 Meet technical and legal requirements for the integrity, traceability, and non-repudiation of records and events

4. Roles and Responsibilities

4.1 General Manager (GM)

4.1.1 Approves this policy and ensures organizational compliance

4.1.2 Oversees periodic reviews of system-level time accuracy and implementation gaps

4.1.3 Approves exceptions to automated time synchronization where justified and documented

4.2 IT Support Provider / Internal IT Role

4.2.1 Configures time synchronization for all company-owned or managed systems

4.2.2 Verifies that daily or scheduled synchronization is functioning correctly

4.2.3 Investigates and remediates time drift events, synchronization failures, or NTP access issues

4.2.4 Documents time synchronization status as part of monthly system health checks

[... 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 Scheduled Review

9.1.1 This policy must be reviewed annually by the General Manager, IT Support Provider, and Privacy Coordinator

9.1.2 All logs and time synchronization compliance status reports must be considered during the review

9.2 Trigger-Based Updates

9.2.1 This policy must be updated if:

9.2.1.1 A system failure results in significant time drift

9.2.1.2 An audit identifies deficiencies in time synchronization

9.2.1.3 The organization adopts new cloud, hybrid, or virtualized environments

9.2.1.4 Legal or regulatory changes introduce new time integrity requirements

9.3 Version Control and Communication

9.3.1 All updates must be version-controlled and dated

9.3.2 Major changes must be communicated to all technical staff

9.3.3 Previous versions must be retained for 3 years to support audits

10. Related Policies and Linkages

10.1 This policy must be applied together with the following SME policies:

10.1.1 P22S – Logging and Monitoring Policy: Ensures consistent timestamping across logs for traceability and forensic correlation.

10.1.2 P30S – Incident Response Policy: Relies on timestamp accuracy to reconstruct incidents, establish timelines, and support notification decisions.

10.1.3 P17S – Data Protection and Privacy Policy: Ensures that access logs and data handling timelines involving personal data are accurate and defensible under GDPR.

10.1.4 P12S – Asset Management Policy: Supports identification of systems requiring synchronization, particularly mobile and remote devices.

10.1.5 P26S – Third-Party and Supplier Security Policy: Ensures that vendors accessing or logging organizational data contractually follow synchronized time practices.

11. Reference Standards and Frameworks

11.1 ISO/IEC 27001:

11.1.1 Clause 8.1 – Requires implementation of controls necessary for secure operations, including logging and timestamping.

11.2 ISO/IEC 27002:

11.2.1 Control 8.17 – Recommends synchronized time for all systems that produce logs or operate in coordination.

11.3 NIST SP 800-53 Rev.5:

11.3.1 AU-8 – Requires the use of internal or external time sources to ensure log timestamp accuracy.

11.3.2 SC-45 – Specifies the use of trusted NTP sources and the prevention of manual time changes in critical systems.

11.4 EU GDPR:

11.4.1 Article 5(1)(d) – Requires accuracy and accountability in personal data processing, supported by synchronized timestamps.

11.4.2 Article 32 – Requires security measures to ensure data integrity, including consistent logging timeframes.

11.5 EU NIS2 Directive:

11.5.1 Article 21(2)(d) – Requires monitoring and detection capabilities supported by synchronized system logs.

11.6 EU DORA:

11.6.1 Article 10 – Requires operational resilience, including traceable and timestamped ICT incident logs.

11.6.2 Article 15 – Requires service providers to maintain accurate technical records, including timestamped audit trails.

11.7 COBIT 2019:

11.7.1 DSS05.02 – Emphasizes timestamp integrity for detecting and responding to events.

11.7.2 MEA03.01 – Requires evidence-based performance monitoring supported by accurate, time-synchronized data.