					Insert Registered Legal Entity Name Here							
Document number: P23					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	-
ISO/IEC 27002:2022	Control 8	-
NIST SP 800-53 Rev.5	SC-45, AU-8	-
EU GDPR	Article 32	-
EU NIS2	Article 21(2)(e)	-
EU DORA	Articles 9, 10	-
COBIT 2019	DSS05.04, MEA	-

1. Purpose

1.1 The purpose of this policy is to ensure that all organizational systems, applications, devices, and cloud services maintain consistent and accurate time settings by synchronizing with designated trusted time sources.

1.2 Accurate time synchronization is essential for reliable logging, secure communications, audit traceability, incident reporting and management, and forensic investigation. Misaligned time may result in uncorrelated logs, failed authentication, and incomplete regulatory reporting.

1.3 This policy supports ISO/IEC 27001 Annex A control 8.17 and related international standards by enforcing time accuracy and clock drift detection across the organization's IT infrastructure.

2. Scope

2.1 This policy applies to:

2.1.1 All IT infrastructure components, including servers, workstations, network devices, firewalls, and Internet of Things (IoT) systems

2.1.2 Virtual and cloud environments (e.g., AWS, Azure, Google Cloud)

2.1.3 All systems participating in logging, authentication, transaction processing, or security event correlation

2.1.4 Internal employees, contractors, and third-party service providers responsible for time-sensitive systems

2.2 Systems that generate or consume timestamped records—such as log entries, alerts, user activity records, or forensic evidence—are considered in scope.

3. Objectives

3.1 Define a consistent, centralized time synchronization architecture using approved NTP sources or equivalent.

3.2 Ensure that all systems synchronize their clocks at defined intervals and that any drift is detected and corrected automatically or with minimal intervention.

3.3 Maintain clock accuracy across hybrid, on-premises, and cloud environments to enable:

3.3.1 Reliable event correlation and incident reporting and management

3.3.2 Regulatory compliance with standards such as ISO 27001, GDPR, NIS2, and DORA

3.3.3 Protection against replay attacks and time-based authentication failures

3.4 Establish clear roles and responsibilities, exception handling procedures, and audit mechanisms to maintain policy enforcement.

3.5 Ensure that time-related anomalies are logged, alerted on, and escalated when they exceed defined tolerances.

4. Roles and Responsibilities

4.1 Chief Information Security Officer (CISO)

4.1.1 Owns this policy and ensures alignment with Information Security Management System (ISMS) operational controls and regulatory requirements.

4.1.2 Approves enterprise time source selection and validates time synchronization reporting processes.

4.2 Infrastructure Services Manager / Network Engineering Lead

4.2.1 Maintains the organization's primary and secondary NTP servers or designated time source configuration.

4.2.2 Ensures that all network-connected devices and virtual instances synchronize time at appropriate intervals.

4.2.3 Monitors time synchronization logs, clock drift alerts, and fault conditions.

[... 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 earlier under the following conditions:

9.1.1 Detection of time-based exploits or logging failures

9.1.2 Changes to core time infrastructure (e.g., new enterprise NTP servers or protocol updates)

9.1.3 Cloud platform time drift discrepancies or regional service changes

9.1.4 Post-incident findings identifying time misalignment as a contributing factor

9.2 The review shall be coordinated by the Infrastructure Lead, with required input from the Security Operations Center (SOC), application security, and compliance stakeholders.

9.3 Revisions must be documented in the ISMS Document Register and communicated to affected internal and third-party stakeholders.

9.4 Historical versions of the policy must be securely archived, version-controlled, and made available for compliance or legal audit requests.

10. Related Policies and Linkages

10.1 P1 – Information Security Policy. Establishes the overarching requirement to ensure the integrity and traceability of all information systems, for which time accuracy is foundational.

10.2 P5 – Change Management Policy. Governs changes to system configurations, including time source adjustments, ensuring proper documentation, testing, and rollback planning.

10.3 P22 – Logging and Monitoring Policy. Directly depends on synchronized time to ensure event sequencing, log correlation, and the integrity of incident investigations across diverse systems.

10.4 P30 – Incident Response Policy. Relies on accurate timestamps for forensic investigations, incident timelines, and chain-of-custody evidence. Inaccurate time undermines the credibility of incident reports.

10.5 P20 – Endpoint Protection / Malware Policy. Requires time-accurate alerting and behavioral analytics to detect malware spread, lateral movement, and access anomalies.

10.6 P6 – Risk Management Policy. Defines the treatment of desynchronization as a potential operational and forensic risk, requiring the controls defined in this policy to mitigate impact.

11. Reference Standards and Frameworks

11.1 ISO/IEC 27001

11.1.1 Clause 8.1 – Operational Planning and Control: Requires integration of accurate technical controls, such as synchronized system clocks, for reliable operational execution.

11.2 ISO/IEC 27002:2022 – Control 8

11.2.1 Reinforces clock accuracy and requires organizational consistency of system time to facilitate log comparison, investigation, and secure transaction validation.

11.3 NIST SP 800-53 Rev.5

11.3.1 SC-45 – System Time Synchronization: Requires time synchronization using authoritative sources across all components within a system boundary.

11.3.2 AU-8 – Time Stamps: Ensures events are accurately timestamped and provides traceability for audit and incident response.

11.4 EU GDPR (2016/679)

11.4.1 Article 32 – Security of Processing: While not explicitly referring to time, it mandates appropriate technical measures—including audit trails and logs—that inherently depend on synchronized timestamps for validity and integrity.

11.5 EU NIS2 Directive (2022/2555)

11.5.1 Article 21(2)(e): Requires logging and detection capabilities that presuppose accurate time synchronization for cross-system correlation and timely response.

11.6 EU DORA (2022/2554)

11.6.1 Article 9 – ICT Risk Management: Mandates accurate system telemetry for risk monitoring and anomaly detection, which depends on precise clock synchronization.

11.6.2 Article 10 – ICT Business Continuity: Requires controls to ensure system integrity during disruptions, including time-aligned event records.

11.7 COBIT 2019

11.7.1 DSS05.04 – Monitor Security Events: Requires timestamp integrity for effective log analysis and threat intelligence detection.

11.7.2 MEA03 – Monitor, Evaluate, and Assess Compliance: Time synchronization supports accurate compliance auditing and reporting cycles.