					[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 where applicable		
Standard/Regulation	**Clause/Article**	**Comment**
ISO/IEC 27001:2022	Clause 8.1	
ISO/IEC 27002:2022	Control 8.17	
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, MEA03	

					[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			

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 response, and forensic investigation. Misaligned time can 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 estate.
2. **Scope**
   2.1 This policy applies to:
      2.1.1 All infrastructure components including servers, workstations, network devices, firewalls, and 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 with responsibility over time-sensitive systems
   2.2 Systems generating or consuming 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 response
      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, exception handling procedures, and audit mechanisms to maintain policy enforcement.
   3.5 Ensure that time-related anomalies are logged, alerted upon, and escalated when exceeding tolerances.
4. **Roles and Responsibilities**
   4.1 **Chief Information Security Officer (CISO)**
      4.1.1 Owns this policy and ensures alignment with 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.

[.....]

11. Reference Standards and Frameworks

ISO/IEC 27001:2022

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

ISO/IEC 27002:2022 – Control 8.17

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

NIST SP 800-53 Rev.5

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

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

EU GDPR (2016/679)

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

EU NIS2 Directive (2022/2555)

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

EU DORA (2022/2554)

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

Article 10 – ICT Business Continuity: Enforces controls ensuring system integrity during disruptions, including time-aligned event records.

COBIT 2019

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

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