					[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 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	Articles 5(1)(d), 3	
EU NIS2	Article 21(2)(d)	
EU DORA	Articles 10, 15	
COBIT 2019	DSS05.02, MEA03.01	

<table>
<tr><td colspan="4"></td><td colspan="10">[Insert Registered Legal Entity Name Here]</td></tr>
<tr><td colspan="4">Document number:
P23S</td><td colspan="10">Document Title:
Time Synchronization Policy</td></tr>
<tr><td colspan="2">Version:
1.0</td><td colspan="2">Effective Date:
01.01.2025</td><td colspan="10">Document Owner:</td></tr>
<tr><td>X</td><td>Policy</td><td></td><td>Standard</td><td></td><td>Procedure</td><td></td><td>Form</td><td></td><td>Register</td><td></td><td>Other</td></tr>
</table>

1. **Purpose**
   1.1. This policy establishes mandatory controls for maintaining accurate, synchronized time across all systems that store, transmit, or process organizational data.
   1.2. Time synchronization is essential for ensuring that system logs are traceable, security incidents are correlated accurately, and evidence can be relied upon during forensic analysis or legal review.
   1.3. The organization enforces 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, prevents 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 infrastructure 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. The policy also applies to BYOD (Bring Your Own Device) endpoints used to access business systems, provided those endpoints store or generate audit-relevant data.
3. **Objectives**
   3.1. Ensure 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 environments (on-premise, cloud, and remote)
   3.5. Satisfy technical and legal requirements for 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

   [……]

Reference Standards and Frameworks

ISO/IEC 27001:2022

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

ISO/IEC 27002:2022

Control 8.17 – Recommends synchronized time for all systems that produce logs or operate collaboratively.

NIST SP 800-53 Rev.5

AU-8 – Requires use of internal or external time sources for log timestamp accuracy.

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

EU GDPR

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

Article 32 – Requires security measures ensuring data integrity, which includes consistent logging timeframes.

EU NIS2 Directive

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

EU DORA

Article 10 – Demands operational resilience, requiring traceable and timestamped ICT incident logs.

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

COBIT 2019

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

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

<table>
<tr><td colspan="3"></td><td colspan="9">[Insert Registered Legal Entity Name Here]</td></tr>
<tr><td colspan="3">Document number:
P23S</td><td colspan="9">Document Title:
Time Synchronization Policy</td></tr>
<tr><td colspan="2">Version:
1.0</td><td colspan="2">Effective Date:
01.01.2025</td><td colspan="9">Document Owner:</td></tr>
<tr><td>X</td><td>Policy</td><td></td><td>Standard</td><td></td><td>Procedure</td><td></td><td>Form</td><td></td><td>Register</td><td></td><td>Other</td></tr>
</table>