					Inserire qui la denominazione dell'entità giuridica registrata							
Numero del documento: P23S					Titolo del documento: **Politica di sincronizzazione temporale**							
Versione: 1.0		Data di entrata in vigore: 01.01.2025			Proprietario del documento:							
X	Politica		Standard		Procedura		Modulo		Registro		Altro	

Cronologia delle revisioni				
Numero di revisione	**Data di revisione**	**Modifiche**	**Riesaminato da**	**Proprietario del processo**

Approvazioni			
Nome	**Ruolo**	**Data**	**Firma**

Allineata a standard e regolamenti

Standard/Regolamento	Clausola/Articolo	Commento
ISO/IEC 27001:2022	Clausola 8	Requisiti di controllo pertinenti
ISO/IEC 27002:2022	Controllo 8	Operatività sincronizzata dei sistemi
NIST SP 800-53 Rev.5	SC-45, AU-8	NTP attendibile e accuratezza della marcatura temporale dei log
GDPR UE	Articoli 5(1)(d), 32	Accuratezza, accountability e integrità dei dati personali mediante marcature temporali sincronizzate
NIS2 UE	Articolo 21(2)(d)	Capacità di monitoraggio e rilevazione supportate da log sincronizzati
DORA UE	Articoli 10, 15	Resilienza operativa e registrazioni tecniche accurate
COBIT 2019	DSS05.02, MEA03	Eventi con marcatura temporale ed evidenze basate sul monitoraggio

1. Finalità

1.1 La presente politica stabilisce controlli obbligatori per mantenere un orario accurato e sincronizzato in tutti i sistemi che archiviano, trasmettono o trattano dati dell'organizzazione.

1.2 La sincronizzazione temporale è essenziale per garantire la tracciabilità dei log di sistema, la corretta correlazione degli incidenti di sicurezza e l'affidabilità delle evidenze durante le analisi forensi o i riesami legali.

1.3 L'organizzazione adotta la sincronizzazione temporale automatizzata quale requisito fondamentale per l'integrità degli audit, la risposta agli incidenti e la conformità normativa ai sensi di ISO 27001, GDPR, DORA e NIS2.

1.4 La presente politica garantisce che tutti i sistemi utilizzino fonti temporali attendibili, vieta la modifica manuale delle impostazioni dell'ora e richiede la correzione tempestiva della deriva temporale.

2. Ambito di applicazione

2.1 La presente politica si applica a:

2.1.1 Tutti i sistemi e dispositivi di proprietà aziendale, inclusi server, desktop, laptop, dispositivi mobili, firewall, router e macchine virtuali

2.1.2 L'infrastruttura remota e gli asset ospitati nel cloud utilizzati nelle operazioni (ad es. AWS, Microsoft 365, piattaforme SaaS)

2.1.3 I sistemi che generano o archiviano log di evento, registrazioni di autenticazione o audit trail

2.1.4 Qualsiasi dipendente, collaboratore esterno, fornitore o fornitore di supporto IT responsabile della configurazione o della manutenzione di tali sistemi

2.2 La politica si applica anche agli endpoint BYOD (Bring Your Own Device) utilizzati per accedere ai sistemi aziendali, a condizione che tali endpoint archivino o generino dati rilevanti ai fini di audit.

3. Obiettivi

3.1 Garantire che tutti i sistemi critici sincronizzino automaticamente l'orario utilizzando server Network Time Protocol (NTP) attendibili o meccanismi equivalenti del provider cloud

3.2 Prevenire discrepanze temporali che possano compromettere l'affidabilità o la correlazione dei log di sistema durante gli audit o le indagini di sicurezza

3.3 Consentire il rilevamento e la correzione tempestivi della deriva temporale oltre le soglie accettabili

3.4 Mantenere una marcatura temporale coerente in tutti gli ambienti (on-premise, cloud e remoti)

3.5 Soddisfare i requisiti tecnici e legali relativi a integrità, tracciabilità e non ripudio delle registrazioni e degli eventi

4. Ruoli e responsabilità

4.1 Direttore generale (GM)

4.1.1 Approva la presente politica e assicura la conformità organizzativa

4.1.2 Sovrintende ai riesami periodici dell'accuratezza temporale a livello di sistema e delle eventuali lacune di attuazione

4.1.3 Approva le eccezioni alla sincronizzazione temporale automatizzata, se giustificate e documentate

4.2 Fornitore di supporto IT / Referente IT interno

4.2.1 Configura la sincronizzazione temporale per tutti i sistemi aziendali o gestiti

4.2.2 Verifica quotidianamente o secondo pianificazione che la sincronizzazione funzioni correttamente

4.2.3 Analizza e corregge gli eventi di deriva temporale, i guasti di sincronizzazione o i problemi di accesso al servizio NTP

4.2.4 Documenta lo stato della sincronizzazione temporale nell'ambito dei controlli mensili sullo stato di salute dei sistemi

[... Le sezioni 4.3–8 non sono incluse in questa anteprima. Acquistare il documento completo per accedere all'intero contenuto. ...]

9. Requisiti di riesame e aggiornamento

9.1 Riesame pianificato

9.1.1 La presente politica deve essere riesaminata annualmente dal Direttore generale, dal fornitore di supporto IT e dal Coordinatore privacy

9.1.2 Nel riesame devono essere considerati tutti i log e i report sullo stato di conformità della sincronizzazione temporale

9.2 Aggiornamenti basati su trigger

9.2.1 La presente politica deve essere aggiornata se:

9.2.1.1 Un guasto di sistema provoca una deriva temporale significativa

9.2.1.2 Un audit rileva carenze nella sincronizzazione temporale

9.2.1.3 L'organizzazione adotta nuovi ambienti cloud, ibridi o virtualizzati

9.2.1.4 Modifiche legali o normative introducono nuovi requisiti di integrità temporale

9.3 Controllo delle versioni e comunicazione

9.3.1 Tutti gli aggiornamenti devono essere sottoposti a controllo delle versioni e datati

9.3.2 Le modifiche rilevanti devono essere comunicate a tutto il personale tecnico

9.3.3 Le versioni precedenti devono essere conservate per 3 anni a supporto degli audit

10. Politiche correlate e collegamenti

10.1 La presente politica deve essere applicata congiuntamente alle seguenti politiche SME:

10.1.1 P22S – Politica di registrazione e monitoraggio: garantisce una marcatura temporale coerente nei log ai fini della tracciabilità e della correlazione forense.

10.1.2 P30S – Politica di risposta agli incidenti: si basa sull'accuratezza della marcatura temporale per ricostruire gli incidenti, definire le cronologie e supportare le decisioni di notifica.

10.1.3 P17S – Politica di protezione dei dati e privacy: garantisce che i log di accesso e le tempistiche di trattamento dei dati personali siano accurati e difendibili ai sensi del GDPR.

10.1.4 P12S – Politica di gestione degli asset: supporta l'identificazione dei sistemi che richiedono sincronizzazione, in particolare i dispositivi mobili e remoti.

10.1.5 P26S – Politica di sicurezza delle terze parti e dei fornitori: garantisce che i fornitori che accedono ai dati dell'organizzazione o li registrano adottino contrattualmente pratiche di sincronizzazione temporale.

11. Standard e quadri di riferimento

11.1 ISO/IEC 27001:

11.1.1 Clausola 8.1 – Richiede l'attuazione dei controlli necessari per operazioni sicure, inclusi registrazione e marcatura temporale.

11.2 ISO/IEC 27002:

11.2.1 Controllo 8.17 – Raccomanda la sincronizzazione temporale per tutti i sistemi che producono log o operano in modo interconnesso.

11.3 NIST SP 800-53 Rev.5:

11.3.1 AU-8 – Richiede l'uso di fonti temporali interne o esterne per garantire l'accuratezza della marcatura temporale dei log.

11.3.2 SC-45 – Specifica l'uso di fonti NTP attendibili e la prevenzione delle modifiche manuali dell'ora nei sistemi critici.

11.4 GDPR UE:

11.4.1 Articolo 5(1)(d) – Richiede accuratezza e accountability nel trattamento dei dati personali, supportate da marcature temporali sincronizzate.

11.4.2 Articolo 32 – Richiede misure di sicurezza che garantiscano l'integrità dei dati, inclusa la coerenza dei tempi di registrazione.

11.5 Direttiva UE NIS2:

11.5.1 Articolo 21(2)(d) – Richiede capacità di monitoraggio e rilevazione, supportate da log di sistema sincronizzati.

11.6 DORA UE:

11.6.1 Articolo 10 – Richiede resilienza operativa, imponendo log degli incidenti ICT tracciabili e con marcatura temporale.

11.6.2 Articolo 15 – Richiede ai fornitori di servizi di mantenere registrazioni tecniche accurate, incluse audit trail con marcatura temporale.

11.7 COBIT 2019:

11.7.1 DSS05.02 – Sottolinea l'integrità della marcatura temporale per rilevare gli eventi e rispondere agli stessi.

11.7.2 MEA03.01 – Richiede il monitoraggio delle prestazioni basato su evidenze, supportato da dati accurati e sincronizzati temporalmente.