					Inserire qui la denominazione dell'entità giuridica registrata							
Numero del documento: P22S					Titolo del documento: **Politica di registrazione e monitoraggio**							
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 norme e regolamenti

Norma/Regolamento	Clausola/Articolo	Commento
ISO/IEC 27001:2022	Clausola 8	Controlli operativi, inclusa la registrazione degli eventi
ISO/IEC 27002:2022	Controlli 8.15, 8.16, 8.17	Registrazione degli eventi, protezione dei log e monitoraggio
NIST SP 800-53 Rev.5	AU-2 to AU-12, SI-4	Contenuto e riesame dei log di audit, conservazione, rilevamento delle anomalie, allerta
GDPR UE	Articoli 5(1)(f), 32, 33	Riservatezza e integrità dei dati, misure tecniche e notifica delle violazioni
NIS2 UE	Articoli 21(2)(d), 23	Meccanismi di registrazione delle anomalie e segnalazione degli incidenti entro 24 ore
DORA UE	Articoli 10, 15	Resilienza operativa, monitoraggio e registrazione dei fornitori di servizi
COBIT 2019	DSS01.03, DSS05.02	Tracciabilità delle attività e protezione mediante registrazione e monitoraggio

1. Finalità

1.1 La presente politica stabilisce controlli obbligatori di registrazione e monitoraggio al fine di garantire la sicurezza, la responsabilità e l'integrità operativa dei sistemi IT dell'organizzazione.

1.2 Definisce le tipologie di eventi che devono essere registrati, le modalità di archiviazione dei log, le modalità di riesame e le responsabilità del personale e dei fornitori di servizi.

1.3 La registrazione e il monitoraggio supportano il rilevamento delle minacce, la conformità normativa, la risposta agli incidenti e l'analisi forense.

1.4 La presente politica consente all'organizzazione di soddisfare i requisiti di controllo operativo della norma ISO/IEC 27001 e supporta in modo continuativo la capacità di dimostrare la conformità, rafforzare la fiducia dei clienti e assicurare l'aderenza a GDPR, NIS2 e DORA.

2. Ambito di applicazione

2.1 La presente politica si applica a tutti i sistemi e a tutti gli utenti dell'organizzazione, inclusi:

2.1.1 Workstation, laptop, server, firewall, switch, router e punti di accesso wireless

2.1.2 Servizi cloud utilizzati per le operazioni aziendali, ad esempio posta elettronica, archiviazione file, backup e strumenti di collaborazione

2.1.3 Funzioni di audit logging presenti in software antivirus, applicazioni, sistemi operativi e apparati di rete

2.1.4 Tutti i dipendenti, i collaboratori esterni e i fornitori di servizi gestiti che utilizzano o amministrano i sistemi

2.1.5 Qualsiasi contesto in cui vengano utilizzati sistemi IT aziendali, inclusi ambienti remoti, ibridi o BYOD

2.2 La politica si applica anche ai log generati da servizi di terze parti laddove l'organizzazione disponga di accesso amministrativo o di clausole contrattuali sul diritto di audit.

3. Obiettivi

3.1 Garantire la registrazione delle attività di sistema, incluse l'autenticazione, le modifiche di configurazione, l'accesso ai dati sensibili e gli allarmi tecnici

3.2 Mantenere log sicuri e accurati per rilevare violazioni della politica, errori di sistema o azioni non autorizzate

3.3 Consentire un tempestivo riesame dei log durante incidenti, indagini e audit

3.4 Supportare la sincronizzazione temporale per garantire l'integrità e la correlazione dei dati di log

3.5 Proteggere i log da manomissioni, perdita o cancellazione prematura

3.6 Soddisfare gli obblighi legali e normativi in materia di responsabilità dei sistemi, tracciabilità e risposta alle violazioni

4. Ruoli e responsabilità

4.1 Direttore generale (GM)

4.1.1 Approva la presente politica e ne garantisce l'applicazione in tutti i sistemi aziendali

4.1.2 Riesamina gli allarmi ad alta gravità e le risultanze di audit significative segnalati dalle funzioni IT o privacy

4.1.3 Approva le eccezioni nei casi in cui la registrazione o la conservazione non possano essere applicate per motivi tecnici

4.2 Fornitore di supporto IT / Funzione IT interna

4.2.1 Implementa e configura la registrazione per sistemi operativi, dispositivi di rete, strumenti antivirus e applicazioni critiche

4.2.2 Garantisce che i log siano conservati, sottoposti a backup e protetti da alterazioni

4.2.3 Riesamina i log secondo una pianificazione definita e indaga attività sospette o non autorizzate

4.2.4 Mantiene sistemi di allerta che segnalano comportamenti anomali o indicatori di compromissione

[... 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 annuale

9.1.1 La presente politica deve essere riesaminata almeno una volta all'anno dal Direttore generale con il supporto del Fornitore di supporto IT e del Coordinatore privacy.

9.2 Eventi che attivano il riesame

9.2.1 Devono essere effettuati riesami non pianificati in risposta a:

9.2.1.1 Risultanze relative ai log emerse da audit interni o esterni

9.2.1.2 Incidenti di sicurezza nei quali i log erano mancanti, corrotti o insufficienti

9.2.1.3 Modifiche rilevanti all'infrastruttura IT, ad esempio migrazione a piattaforme cloud per la registrazione

9.2.1.4 Aggiornamenti degli obblighi legali o normativi, ad esempio GDPR, NIS2 e DORA

9.3 Controllo delle versioni

9.3.1 Tutte le modifiche alla presente politica devono essere registrate con numero di versione, data e sintesi delle revisioni

9.3.2 Le versioni precedenti devono essere archiviate e conservate per almeno 3 anni

9.3.3 Le politiche aggiornate devono essere comunicate alle parti interessate coinvolte, in particolare a quelle con accesso a livello di sistema

10. Politiche correlate e collegamenti

10.1 La presente politica supporta direttamente ed è supportata dalle seguenti politiche SME in materia di sicurezza delle informazioni:

10.1.1 P17S – Politica di protezione dei dati e privacy: garantisce che i dati di log contenenti informazioni personali siano gestiti con integrità, conservazione e misure di controllo degli accessi in linea con i requisiti del GDPR.

10.1.2 P21S – Politica di sicurezza della rete: fornisce la base per acquisire log relativi a firewall, accesso wireless, VPN e monitoraggio della segmentazione.

10.1.3 P24S – Politica di sviluppo sicuro: garantisce che i log applicativi, ad esempio relativi a tentativi di accesso, errori ed eccezioni, siano integrati nella progettazione e nelle operazioni del software.

10.1.4 P30S – Politica di risposta agli incidenti: si basa su dati di log accurati e completi per rilevare, analizzare e gestire eventi di sicurezza delle informazioni.

10.1.5 P23S – Politica di sincronizzazione temporale: garantisce marcature temporali coerenti e tracciabili su tutti i sistemi, consentendo la correlazione dei log durante le indagini.

11. Standard e quadri di riferimento

11.1 ISO/IEC 27001

11.1.1 Clausola 8.1 – Richiede l'implementazione di controlli operativi per mitigare i rischi per la sicurezza delle informazioni, inclusa la registrazione.

11.2 ISO/IEC 27002

11.2.1 Controllo 8.15 – Richiede la registrazione degli eventi a supporto del rilevamento delle anomalie e della responsabilità.

11.2.2 Controllo 8.16 – Richiede la protezione dei log da manomissioni e accessi non autorizzati.

11.2.3 Controllo 8.17 – Richiede il monitoraggio dei sistemi per attività anomale e la conferma dell'efficacia dei controlli di monitoraggio.

11.3 NIST SP 800-53 Rev.5

11.3.1 AU-2 to AU-12 – Coprono contenuto dei log di audit, riesame, conservazione e allerta automatizzata.

11.3.2 SI-4 – Richiede il rilevamento delle anomalie di sistema e la segnalazione di eventi sospetti.

11.4 GDPR UE

11.4.1 Articolo 5(1)(f) – Richiede integrità e riservatezza dei dati personali, inclusa la registrazione degli accessi.

11.4.2 Articolo 32 – Impone misure tecniche e organizzative per garantire la sicurezza, inclusi registrazione e monitoraggio.

11.4.3 Articolo 33 – Richiede la notifica tempestiva delle violazioni, supportata da log che consentano l'analisi della causa radice.

11.5 Direttiva NIS2 UE

11.5.1 Articolo 21(2)(d) – Richiede meccanismi di registrazione che rilevino anomalie e forniscano supporto durante le indagini sugli incidenti.

11.5.2 Articolo 23 – Impone la segnalazione degli incidenti entro 24 ore, che dipende da dati di log accurati e tempestivi.

11.6 DORA UE

11.6.1 Articolo 10 – Richiede la resilienza operativa digitale, inclusa la tracciabilità degli incidenti relativi ai sistemi ICT mediante registrazione.

11.6.2 Articolo 15 – Impone il monitoraggio dei fornitori di servizi, inclusi i diritti di accesso ai log e di riesame.

11.7 COBIT 2019

11.7.1 DSS01.03 – Richiede la tracciabilità delle attività di sistema tramite registrazione e monitoraggio.

11.7.2 DSS05.02 – Riguarda la registrazione come controllo chiave nella protezione contro malware e altre attività non autorizzate.