					Inserire qui la denominazione dell'entità giuridica registrata							
Numero del documento: P22					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**

1. Finalità

1.1 La presente politica stabilisce requisiti chiari e applicabili per la generazione, la protezione, il riesame e l'analisi dei log che registrano i principali eventi di sistema e di sicurezza nell'intero ambiente IT dell'organizzazione.

1.2 La registrazione e il monitoraggio sono essenziali per il rilevamento delle anomalie, la risposta alle minacce, le indagini forensi, la dimostrazione della conformità e l'adempimento degli obblighi di legge. La presente politica garantisce che tutti gli eventi generati dai sistemi siano correttamente registrati, conservati e correlati con precisione mediante marcatura temporale sincronizzata.

1.3 La presente politica è essenziale a supporto della Clausola 8.1 della ISO/IEC 27001 e dei controlli dell'Allegato A 8.15 (logging), 8.16 (monitoraggio) e 8.17 (sincronizzazione degli orologi), ed è direttamente collegata agli obblighi normativi previsti da GDPR, NIS2, DORA e COBIT 2019.

2. Ambito di applicazione

2.1 La presente politica si applica a tutti i sistemi, servizi e ambienti che archiviano, trattano o trasmettono dati compresi nel campo di applicazione del SGSI, inclusi:

2.1.1 infrastrutture on-premises, servizi cloud (ad es. IaaS, PaaS, SaaS) e ambienti ibridi

2.1.2 sistemi operativi, database, applicazioni e apparati di rete

2.1.3 sistemi di sicurezza quali SIEM, firewall, piattaforme EDR, concentratori VPN e identity provider

2.2 Rientrano nel presente ambito di applicazione i seguenti soggetti interessati:

2.2.1 utenti interni con privilegi di sistema o amministrativi

2.2.2 personale dell'infrastruttura e delle operations IT

2.2.3 Security Operations Center (SOC) e team di rilevamento delle minacce

2.2.4 sviluppatori software e proprietari delle applicazioni

2.2.5 fornitori terzi che gestiscono sistemi che producono log

3. Obiettivi

3.1 Garantire che tutti i sistemi critici generino log degli eventi di sicurezza e registrazioni delle attività di sistema, conservati in conformità ai requisiti normativi, legali e contrattuali.

3.2 Definire le tipologie minime di evento e il contenuto minimo dei log necessari per rilevare attività non autorizzate, tracciare le azioni degli utenti e supportare le indagini forensi.

3.3 Applicare misure di protezione per prevenire la manomissione dei log, la cancellazione non autorizzata o l'accesso non controllato ai dati di log.

3.4 Istituire sistemi centralizzati di logging e allertamento (ad es. SIEM) per aggregare, correlare ed escalare le attività sospette in tempo quasi reale.

3.5 Garantire la sincronizzazione degli orologi di sistema per consentire una correlazione accurata tra sistemi e l'analisi degli incidenti.

3.6 Supportare il miglioramento continuo e la conformità integrando il monitoraggio dei log con i processi di audit, gestione del rischio e gestione degli incidenti.

4. Ruoli e responsabilità

4.1 Chief Information Security Officer (CISO)

4.1.1 È il proprietario della politica e ne garantisce l'allineamento con la postura di rischio dell'organizzazione, i requisiti di audit e gli obblighi del SGSI.

4.1.2 Approva l'ambito del logging per i sistemi regolamentati o ad alto rischio e supervisiona la reportistica di conformità.

4.2 Responsabile del Security Operations Center (SOC)

4.2.1 Gestisce e mantiene le piattaforme centralizzate di gestione dei log (ad es. SIEM).

4.2.2 Definisce le regole di aggregazione dei log, le soglie di allerta e i percorsi di escalation per il triage degli incidenti.

4.2.3 Riesamina i report giornalieri e garantisce che le anomalie siano analizzate, documentate ed escalate quando necessario.

[... 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 La presente politica deve essere riesaminata annualmente, o prima in risposta a:

9.1.1 modifiche rilevanti nell'architettura dei sistemi o nell'infrastruttura di logging (ad es. migrazione del SIEM)

9.1.2 revisioni dei requisiti normativi di registrazione (ad es. obblighi di logging previsti da NIS2, DORA)

9.1.3 risultanze di audit o analisi post-incidente

9.1.4 minacce emergenti che richiedano un monitoraggio rafforzato (ad es. minacce interne, compromissione della supply chain)

9.2 Il processo di riesame deve essere guidato dal Responsabile del Security Operations Center (SOC) in coordinamento con il CISO, la funzione Risk Management, la funzione compliance e i team dell'infrastruttura IT.

9.3 Le modifiche approvate devono essere sottoposte a controllo di versione nel registro di controllo documentale del SGSI e comunicate a:

9.3.1 tutti i soggetti interessati responsabili della manutenzione dei sistemi di logging

9.3.2 proprietari delle applicazioni e dei sistemi

9.3.3 fornitori terzi con responsabilità di telemetria o integrazione SIEM

9.4 Tutte le versioni superate devono essere archiviate in modo sicuro, con accesso limitato ai custodi autorizzati del SGSI per finalità di audit e legali.

10. Politiche correlate e collegamenti

10.1 P1 – Politica per la sicurezza delle informazioni. Stabilisce l'impegno fondamentale a proteggere sistemi e dati, nell'ambito del quale la registrazione e il monitoraggio operano come elementi abilitanti essenziali per i controlli di rilevamento e la risposta.

10.2 P4 – Politica di controllo degli accessi. Garantisce che l'uso di accessi privilegiati, gli accessi degli utenti e gli eventi di autorizzazione siano registrati nei log e monitorati per rilevare abusi o comportamenti anomali.

10.3 P5 – Politica di gestione delle modifiche. Impone la registrazione delle modifiche di sistema, dei deployment di patch e degli aggiornamenti di configurazione che possono introdurre rischio o modifiche non autorizzate.

10.4 P21 – Politica di sicurezza della rete. Richiede il logging a livello di rete (ad es. log del firewall, allerte IDS/IPS, attività VPN) e l'integrazione con il SIEM per assicurare visibilità sulle anomalie del traffico e sulla protezione del perimetro.

10.5 P23 – Politica di sincronizzazione temporale. Impone la coerenza temporale tra i sistemi, elemento essenziale per un logging affidabile e per la correlazione degli eventi di sicurezza in ambienti multipli.

10.6 P30 – Politica di risposta agli incidenti (P30). Si basa sui dati di log e sui meccanismi di allerta per identificare, indagare e gestire gli incidenti di sicurezza, preservando al contempo gli artefatti forensi per il riesame post-incidente.

11. Standard e quadri di riferimento

11.1 ISO/IEC 27001

11.1.1 Clausola 8.1 – Pianificazione e controllo operativi: richiede controlli per il monitoraggio delle operazioni e la protezione contro accessi non autorizzati e uso improprio dei sistemi.

11.2 ISO/IEC 27002:2022 – Controlli 8.15, 8.16, 8.17

11.2.1 Definisce requisiti dettagliati di logging, inclusi gli eventi da registrare, le modalità di protezione e analisi dei log e le misure per garantire l'affidabilità dei timestamp tra sistemi.

11.3 NIST SP 800-53 Rev.5

11.3.1 AU-2 to AU-12: copre la selezione degli eventi, la registrazione, la protezione, il riesame degli audit trail, la risposta ai guasti dei meccanismi di audit e la conservazione delle registrazioni di audit.

11.3.2 SI-4 – Monitoraggio dei sistemi: richiede il monitoraggio attivo dei sistemi con allerte basate su attività anomale.

11.3.3 SC-45 – Sincronizzazione temporale dei sistemi: rafforza l'accuratezza temporale ai fini della tracciabilità degli eventi e della correlazione degli incidenti.

11.4 GDPR UE (2016/679)

11.4.1 Articolo 32 – Sicurezza del trattamento: richiede controlli tecnici quali registrazione e monitoraggio per garantire sicurezza e accountability, in particolare per l'accesso ai dati personali.

11.5 Direttiva NIS2 UE (2022/2555)

11.5.1 Articolo 21(2)(e): impone sistemi di registrazione degli eventi e monitoraggio per il rilevamento rapido e la risposta agli incidenti di sicurezza.

11.6 DORA UE (2022/2554)

11.6.1 Articolo 9 – Gestione del rischio ICT: richiede meccanismi per rilevare attività anomale, registrare gli incidenti e conservare dati forensi.

11.6.2 Articolo 11 – Test dei piani di continuità operativa ICT: pone l'accento sulla continuità del monitoraggio e sulla convalida della disponibilità dei log durante le interruzioni operative.

11.7 COBIT 2019

11.7.1 DSS01.05 – Gestire i log di sicurezza: richiede l'implementazione di capacità di logging in tutta l'infrastruttura critica.

11.7.2 DSS05.04 – Monitorare gli eventi di sicurezza: impone il monitoraggio e l'analisi in tempo reale dei log per rilevare gli eventi e rispondere agli stessi.

11.7.3 MEA03 – Monitorare, valutare e verificare la conformità: richiede il riesame regolare delle pratiche di registrazione e il relativo allineamento con gli obiettivi di controllo.