					Inserire qui la denominazione dell'entità giuridica registrata							
Numero del documento: P02S					Titolo del documento: **Politica P02S su ruoli e responsabilità di governance**							
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 normative

Standard/Regulation	Clause/Article	Comment
ISO/IEC 27001:2022	Clausola 5	
ISO/IEC 27002:2022	Controlli: 5.2, 5.3, 5	
NIST SP 800-53 Rev.5	PM-1, PL-1, PL-4, CA-1, AC-1	
GDPR UE	Articoli 5(2), 32	

1. Finalità

1.1 La presente politica definisce le modalità con cui le responsabilità di governance per la sicurezza delle informazioni sono assegnate, delegate e gestite all'interno dell'organizzazione, al fine di garantire la piena conformità alla ISO/IEC 27001:2022 e agli altri obblighi normativi applicabili.

1.2 Garantisce l'attribuzione delle responsabilità a ogni livello e supporta l'efficacia operativa, identificando chiaramente il soggetto responsabile di ciascuna funzione relativa alla sicurezza.

1.3 La presente politica rafforza la capacità di dimostrare la conformità e accresce la fiducia dei clienti, dimostrando una governance della sicurezza formalizzata, anche nelle organizzazioni con personale tecnico limitato o con servizi IT esternalizzati.

2. Ambito di applicazione

2.1 La presente politica si applica a tutte le persone che utilizzano o gestiscono sistemi o dati dell'organizzazione, inclusi:

2.1.1 titolari dell'attività e direttori generali

2.1.2 dipendenti e collaboratori esterni

2.1.3 fornitori esterni di supporto IT o consulenti

2.2 Essa si applica a tutti i sistemi, ambienti e servizi utilizzati per elaborare, trasmettere o archiviare informazioni aziendali o dei clienti, inclusi:

2.2.1 infrastruttura IT d'ufficio e dispositivi per il lavoro da remoto

2.2.2 piattaforme cloud e servizi di posta elettronica

2.2.3 archivi cartacei e unità condivise

2.3 L'ambito di applicazione comprende sia le attività interne sia quelle esternalizzate che coinvolgono la governance della sicurezza.

3. Obiettivi

3.1 Stabilire responsabilità chiare per tutti i compiti relativi alla sicurezza, inclusi la gestione delle politiche, il controllo degli accessi, la gestione degli incidenti e il monitoraggio.

3.2 Consentire un'efficace segregazione dei compiti (SoD) per ridurre conflitti di interesse e rischi di frode.

3.3 Garantire che compiti e ruoli di sicurezza siano documentati chiaramente e sottoposti a riesame periodico.

3.4 Consentire decisioni informate, escalation e adeguata supervisione dei rischi IT e di sicurezza.

3.5 Supportare la certificazione ISO/IEC 27001:2022 e rafforzare la fiducia di clienti, partner e auditor.

4. Ruoli e responsabilità

4.1 Direttore generale (GM) / Titolare dell'attività

4.1.1 Ha la responsabilità complessiva dell'attuazione e della supervisione della presente politica.

4.1.2 Approva tutti i ruoli di sicurezza, le relative responsabilità e le decisioni di delega.

4.1.3 Monitora la conformità e adotta le decisioni finali in merito alle eccezioni alla politica e alle escalation.

4.2 Coordinatore della sicurezza designato (se nominato)

4.2.1 Può essere un membro del personale o un consulente di fiducia.

4.2.2 Nelle microimprese, tale ruolo può essere ricoperto dal Direttore generale (GM) o da un fornitore esterno.

4.2.3 Supporta la gestione operativa quotidiana del controllo degli accessi, della risposta agli incidenti e delle attività tecniche di sicurezza di base.

4.2.4 Riferisce direttamente al Direttore generale (GM) in merito a eventuali problematiche o rischi di sicurezza.

[... 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 sottoposta a riesame dal Direttore generale (GM) ogni 12 mesi, per garantire che continui a riflettere gli obblighi legali, le esigenze operative e i requisiti di certificazione ISO/IEC 27001.

9.2 Riesami intermedi

9.2.1 I riesami devono essere effettuati anche quando:

9.2.1.1 si verificano cambiamenti organizzativi rilevanti

9.2.1.2 viene avviato l’onboarding di un nuovo fornitore

9.2.1.3 si verifica un grave incidente di sicurezza

9.2.1.4 normative quali GDPR, NIS2 o DORA vengono aggiornate

9.3 Controllo delle versioni e documentazione

9.3.1 Tutti i riesami devono includere:

9.3.1.1 data del riesame

9.3.1.2 sintesi delle eventuali modifiche

9.3.1.3 firma o approvazione documentata del Direttore generale (GM)

9.3.1.4 versioni precedenti archiviate come riferimento ai fini di audit

9.4 Comunicazione delle modifiche

9.4.1 Tutti gli aggiornamenti della politica devono essere comunicati tempestivamente al personale e ai fornitori tramite e-mail, portali interni o comunicazioni formali.

10. Politiche correlate e collegamenti

10.1 Per garantirne la piena efficacia, la presente politica deve essere applicata congiuntamente alle seguenti politiche SME:

10.1.1 P4S – Politica sul controllo degli accessi: definisce le modalità con cui l’accesso viene concesso, gestito e revocato, in collegamento diretto con i ruoli assegnati e la supervisione.

10.1.2 P8S – Politica sulla consapevolezza e la formazione in materia di sicurezza delle informazioni: rafforza le responsabilità e le aspettative specifiche per ruolo.

10.1.3 P17S – Politica sulla protezione dei dati e sulla privacy: definisce gli obblighi di legge ai sensi del GDPR, assegnati ai ruoli definiti nella presente politica di governance.

10.1.4 P30S – Politica di risposta agli incidenti: richiede responsabilità definite per la segnalazione, l’escalation e la risoluzione degli incidenti.

10.2 Nel loro insieme, queste politiche consentono un'applicazione coerente, la responsabilizzazione interna e la conformità verso l'esterno.

11. Standard e quadri di riferimento

11.1 ISO/IEC 27001

11.1.1 Clausola 5.3 – Ruoli organizzativi, responsabilità e autorità: richiede che i ruoli siano chiaramente assegnati e supportati dall'alta direzione.

11.2 ISO/IEC 27002

11.2.1 Controlli 5.2–5.4: richiedono una chiara documentazione dei ruoli per la sicurezza delle informazioni, la segregazione dei compiti e la supervisione manageriale.

11.3 NIST SP 800-53 Rev.5

11.3.1 PM-1: stabilisce un programma generale per la sicurezza delle informazioni con responsabilità definite.

11.3.2 Da PL-1 a PL-4: richiedono controlli di pianificazione, inclusi la definizione delle politiche e l'assegnazione documentata dei ruoli.

11.3.3 CA-1: richiede ruoli definiti per la valutazione e l'autorizzazione.

11.3.4 AC-1: collega il controllo degli accessi basato sui ruoli (RBAC) alle responsabilità di governance assegnate.

11.4 GDPR UE

11.4.1 Articolo 5(2) – Responsabilizzazione: richiede alle organizzazioni di dimostrare la conformità attraverso ruoli e responsabilità definiti.

11.4.2 Articolo 32 – Sicurezza del trattamento: enfatizza la chiara assegnazione dei compiti per proteggere i dati personali.

11.5 NIS UE

11.5.1 Articolo 21(2)(a): richiede strutture di governance che includano ruoli formalizzati per la gestione del rischio cyber e degli incidenti.

11.6 DORA UE

11.6.1 Articoli 9 e 10: richiedono agli enti finanziari di assegnare chiaramente e supervisionare le responsabilità relative ai sistemi ICT e alla sicurezza.

11.7 COBIT 2019

11.7.1 EDM03 – Ensure Risk Optimization: richiede ruoli ben definiti e percorsi di escalation per la gestione del rischio di sicurezza.

11.7.2 APO13 – Manage Security: assegna compiti strategici e operativi di sicurezza a persone e ruoli.

11.7.3 DSS05 – Gestire i servizi di sicurezza: richiede struttura e tracciabilità nelle responsabilità dei servizi di sicurezza interni ed esterni.