					Inserire qui la denominazione dell'entità giuridica registrata							
Numero del documento: P02					Titolo del documento: **Politica sui ruoli e sulle 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 regolamenti applicabili

Standard/Regulation	Clause/Article	Comment
ISO/IEC 27001:2022	Clause 5.3; Annex A Control 5	
ISO/IEC 27002:2022	Control 5	
NIST SP 800-53 Rev.5	PL-1 through PL-4, PM-1 through PM-13	
EU GDPR	Articles 5(1)(f), 24, 37	
EU NIS2	Article 21(2)(a)	
EU DORA	Article 5	
COBIT 2019	EDM01, EDM02, APO01, APO12, MEA	

1. Finalità

1.1 La presente politica definisce il modello di governance, i ruoli organizzativi e le responsabilità necessari a gestire un Sistema di Gestione della Sicurezza delle Informazioni (SGSI) efficace.

1.2 Stabilisce chiare linee di responsabilità, autorità decisionale e percorsi di escalation per garantire che la sicurezza delle informazioni sia integrata a tutti i livelli dell'organizzazione e allineata agli obiettivi strategici aziendali.

1.3 La politica attua i requisiti della Clause 5.3 e del controllo A.5.2 della ISO/IEC 27001:2022, assicurando che le responsabilità relative alle attività di sicurezza siano chiaramente assegnate, documentate, comunicate e riesaminate periodicamente.

1.4 La presente politica fornisce inoltre una base per una governance integrata con altre discipline, quali gestione del rischio, conformità, operazioni IT e funzione legale.

2. Ambito di applicazione

2.1 La presente politica si applica a tutte le persone e a tutte le entità coinvolte nella governance, nella gestione operativa e nella supervisione della sicurezza delle informazioni all'interno del campo di applicazione del SGSI. Ciò include:

2.1.1 Direzione esecutiva, alta direzione e membri del Consiglio di Amministrazione

2.1.2 Responsabili del SGSI, CISO e titolari dei controlli

2.1.3 Titolari di processo e titolari degli asset

2.1.4 Appaltatori e fornitori di servizi terzi con responsabilità di sicurezza delegate

2.2 Essa copre sia le funzioni interne sia quelle esternalizzate (ad esempio, SOC esternalizzato, amministratori della piattaforma cloud) nei casi in cui i ruoli di governance siano formalmente assegnati o definiti contrattualmente.

2.3 La politica si applica inoltre alle unità organizzative, ai dipartimenti e ai gruppi di progetto che gestiscono o influenzano asset, sistemi o servizi rilevanti per la sicurezza.

3. Obiettivi

3.1 Garantire che i ruoli e le responsabilità in materia di sicurezza delle informazioni siano formalmente definiti, assegnati, comunicati e documentati.

3.2 Mantenere un modello di governance che assicuri la segregazione dei compiti (SoD), elimini i conflitti di interesse e consenta l'escalation delle questioni di sicurezza non risolte.

3.3 Garantire che la responsabilità e l'autorità per le decisioni di sicurezza siano distribuite in coerenza con l'impatto aziendale e con la struttura organizzativa.

3.4 Stabilire un quadro di riferimento per la gestione della delega di responsabilità, delle modifiche dei ruoli e del riesame delle responsabilità assegnate.

3.5 Fornire assurance alle parti interessate, inclusi regolatori, auditor e clienti, che la sicurezza delle informazioni sia governata in modo efficace e in conformità con gli standard applicabili.

4. Ruoli e responsabilità

4.1 Direzione esecutiva (alta direzione)

4.1.1 Fornisce supervisione strategica, assegna risorse e garantisce l'allineamento tra gli obiettivi del SGSI e gli obiettivi aziendali.

4.1.2 Approva la documentazione principale del SGSI, inclusa la Politica per la sicurezza delle informazioni, i piani di trattamento del rischio e le decisioni di remediation degli audit.

4.1.3 Partecipa ai riesami della direzione del SGSI ed effettua l'escalation delle decisioni che richiedono l'approvazione del Consiglio di Amministrazione.

4.1.4 Promuove una cultura della sicurezza e favorisce la conformità dell'organizzazione ai principi della governance della sicurezza.

4.2 Comitato di indirizzo per la sicurezza delle informazioni

4.2.1 Agisce quale organo di governance interfunzionale per la supervisione del SGSI.

4.2.2 Riesamina la postura di rischio, le prestazioni dei controlli, le risultanze degli audit e le iniziative strategiche di sicurezza.

4.2.3 Favorisce il coordinamento tra dipartimenti (ad esempio IT, funzione legale e compliance, Risorse Umane (HR), rischio, conformità, operazioni).

4.2.4 Approva soglie di escalation, allocazioni di budget e modifiche alle politiche che richiedono il contributo della Direzione esecutiva.

[... 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 Pianificazione del riesame

9.1.1 La presente politica deve essere riesaminata almeno annualmente oppure al verificarsi di uno dei seguenti eventi:

9.1.1.1 modifiche alla struttura organizzativa o al team esecutivo

9.1.1.2 ampliamento o ridefinizione del campo di applicazione del SGSI

9.1.1.3 modifiche normative che incidono sull'assegnazione dei ruoli o sulla supervisione

9.1.1.4 risultanze di audit significative o incidenti che comportino un fallimento della governance

9.2 Processo di riesame e approvazione

9.2.1 Il Responsabile del SGSI deve avviare e guidare il processo di riesame, inclusa la raccolta dei contributi delle parti interessate e del feedback di audit.

9.2.2 Gli aggiornamenti proposti devono essere riesaminati dall'ISSC e formalmente approvati dalla Direzione esecutiva.

9.2.3 Ogni versione deve essere tracciata nel Registro documentale del SGSI e includere i seguenti metadati:

9.2.3.1 ID e titolo della politica

9.2.3.2 Numero di versione e sintesi delle modifiche

9.2.3.3 Data di entrata in vigore e data del successivo riesame

9.2.3.4 Titolare della politica e approvatore

9.2.3.5 Livello di classificazione del documento

9.2.3.6 Storico di conservazione e archiviazione

10. Politiche correlate e collegamenti

10.1 La presente politica deve essere interpretata congiuntamente alle seguenti politiche:

10.1.1 P1 – Politica per la sicurezza delle informazioni: stabilisce il programma generale di sicurezza e definisce le responsabilità della leadership per l'approvazione delle politiche e la supervisione strategica.

10.1.2 P5 – Politica di gestione delle modifiche: assicura che le modifiche alle strutture di governance, ai ruoli o alle responsabilità siano soggette ad approvazione documentata e a riesame del rischio.

10.1.3 P6 – Politica di gestione del rischio: identifica e tratta i rischi di governance derivanti da conflitti di ruolo, compiti non assegnati o mancanza di escalation.

10.1.4 P7 – Politica di onboarding e cessazione del personale: applica i processi di assegnazione dei controlli e di revoca durante i cambiamenti del ciclo di vita del personale.

10.1.5 P33 – Politica di monitoraggio degli audit e della conformità: supporta il riesame indipendente dell'efficacia della governance e assicura l'attuazione di azioni correttive in caso di non conformità.

10.2 Tali politiche supportano congiuntamente un quadro di governance del SGSI unitario e applicabile.

11. Standard e quadri di riferimento

11.1 La presente politica è allineata a standard e quadri di riferimento riconosciuti a livello globale per la governance della sicurezza delle informazioni e per l'attribuzione delle responsabilità di ruolo. Essa assicura la tracciabilità rispetto ai requisiti normativi e di certificazione e supporta una struttura del SGSI solida e difendibile.

11.2 ISO/IEC 27001

11.2.1 Clause 5.3 – Ruoli, responsabilità e autorità organizzative: la presente politica soddisfa il requisito secondo cui i ruoli rilevanti per la sicurezza delle informazioni devono essere chiaramente assegnati, comunicati e documentati.

11.2.2 Clause 9.3 – Riesame della direzione: la presente politica assicura la supervisione esecutiva dei ruoli e della governance del SGSI mediante riesami trimestrali e annuali.

11.2.3 Annex A Control 5.2 – Ruoli e responsabilità per la sicurezza delle informazioni: definisce i ruoli a livello tecnico, operativo e strategico per garantire segregazione dei compiti (SoD), titolarità del rischio e responsabilità tracciabile.

11.3 ISO/IEC 27002:2022 – Controllo 5

11.3.1 Fornisce indicazioni di attuazione per l'assegnazione delle responsabilità di sicurezza delle informazioni all'interno dell'organizzazione. La presente politica adotta tali indicazioni definendo tipologie di ruolo, regole di delega, procedure di escalation e meccanismi di riesame.

11.4 NIST SP 800-53 Rev.5

11.4.1 PL-1 fino a PL-4: impongono l'esigenza di documentazione formale di pianificazione, incluse politiche che definiscono la governance e assegnano responsabilità di sicurezza.

11.4.2 PM-1 (Piano del programma di sicurezza delle informazioni) e PM-2 (Responsabile senior della sicurezza delle informazioni): trovano attuazione nella presente politica tramite l'assegnazione del CISO/Responsabile del SGSI e di ruoli formali di governance.

11.4.3 PM-5 fino a PM-13: la presente politica soddisfa i requisiti relativi alla documentazione dei ruoli, ai ruoli di rischio a livello aziendale, alla supervisione della gestione della configurazione e all'integrazione con le funzioni mission/business.

11.5 GDPR UE (2016/679)

11.5.1 Articolo 5(1)(f): richiede che i dati personali siano protetti contro trattamenti non autorizzati o illeciti. La presente politica assicura che le persone responsabili della protezione dei dati siano chiaramente designate e monitorate.

11.5.2 Articolo 24: richiede misure organizzative adeguate, incluse strutture di governance.

11.5.3 Articolo 37: richiede la designazione di un Responsabile della protezione dei dati (DPO), che deve essere riportata nel quadro di governance dell'organizzazione e nel registro delle responsabilità.

11.6 Direttiva UE NIS2 (2022/2555)

11.6.1 Articolo 21(2)(a): impone che i soggetti adottino politiche in materia di analisi del rischio e sicurezza dei sistemi informativi, incluse responsabilità specifiche per ruolo. La presente politica definisce tali ruoli e i relativi meccanismi di governance.

11.7 DORA UE (2022/2554)

11.7.1 Articolo 5 – Quadro di governance e controllo interno: richiede l'assegnazione formale delle responsabilità di gestione del rischio ICT, dei ruoli decisionali e dei canali di reporting. La presente politica fornisce la base per la governance dei ruoli relativi alla sicurezza negli ambienti ICT.

11.8 COBIT 2019

11.8.1 EDM01 – Impostazione del framework di governance assicurata: la presente politica assicura che il SGSI disponga di una struttura di governance chiaramente definita e allineata alle esigenze aziendali.

11.8.2 EDM02 – Erogazione dei benefici assicurata: allinea le attività di sicurezza basate sui ruoli agli obiettivi strategici e operativi, assicurando responsabilità ed esiti misurabili.

11.8.3 APO01 – Managed I&T Management Framework e APO12 – Managed Risk: la presente politica supporta una gestione strutturata dei ruoli di sicurezza delle informazioni all'interno di un più ampio quadro di governance IT e di gestione del rischio.

11.8.4 MEA01 – Monitorare, valutare e analizzare le prestazioni: integra meccanismi di riesame per verificare che i ruoli di governance siano efficaci, aggiornati e applicati.