					Inserire qui la denominazione dell'entità giuridica registrata							
Numero del documento: P01					Titolo del documento: **Politica per la sicurezza delle informazioni**							
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 definisce l'impegno complessivo dell'organizzazione in materia di sicurezza delle informazioni mediante l'istituzione di un Sistema di Gestione della Sicurezza delle Informazioni (SGSI) formalizzato.

1.2 Fornisce l'indirizzo strategico e i requisiti fondamentali per proteggere la riservatezza, l'integrità, la disponibilità e la resilienza di tutti gli asset informativi negli ambienti fisici, digitali e cloud.

1.3 La politica soddisfa i requisiti di cui alle Clausole 5.1 e 5.2 della ISO/IEC 27001:2022, esprimendo gli indirizzi della leadership, l'impegno dell'alta direzione e l'allineamento delle attività di sicurezza agli obiettivi dell'organizzazione.

1.4 Costituisce il riferimento ufficiale per tutte le politiche, gli standard e le procedure subordinate del SGSI ed è essenziale per abilitare un assetto di sicurezza basato sul rischio, orientato alla conformità e soggetto a miglioramento continuo.

2. Ambito di applicazione

2.1 La presente politica si applica a tutte le persone, agli asset e ai processi definiti nel campo di applicazione del SGSI, inclusi:

2.1.1 Tutte le unità organizzative, i dipartimenti, le controllate e le sedi

2.1.2 I dipendenti e i collaboratori esterni, il personale temporaneo, i consulenti, gli appaltatori e i fornitori di servizi terzi

2.1.3 Tutti i dati, i sistemi informativi, le applicazioni, le infrastrutture e i canali di comunicazione

2.1.4 Tutti gli ambienti fisici, cloud, remoti e ibridi in cui i dati aziendali sono trattati o ai quali si accede

2.2 La politica è vincolante per tutte le entità che trattano informazioni dell'organizzazione e si applica a tutte le fasi del ciclo di vita delle informazioni, dalla creazione e trasmissione fino all'archiviazione e allo smaltimento.

2.3 Eventuali esclusioni o limitazioni del presente ambito di applicazione devono essere documentate nella Dichiarazione di campo di applicazione del SGSI e giustificate con approvazione formale della Direzione esecutiva.

3. Obiettivi

3.1 Istituire un SGSI coerente con la ISO/IEC 27001:2022 e in grado di supportare il processo decisionale basato sul rischio in tutta l'organizzazione.

3.2 Assicurare che i principi di sicurezza di riservatezza, integrità e disponibilità siano integrati in tutte le attività, i sistemi e i rapporti di partnership dell'organizzazione.

3.3 Consentire la conformità normativa e contrattuale definendo obiettivi di sicurezza misurabili, guidati dalla politica e integrati nelle operazioni aziendali.

3.4 Ridurre al minimo la probabilità e l'impatto degli incidenti di sicurezza delle informazioni mediante controlli preventivi, controlli di rilevazione e azioni correttive efficaci.

3.5 Promuovere il miglioramento continuo del livello di maturità della sicurezza delle informazioni attraverso indicatori di prestazione definiti, risultanze degli audit e riesami della direzione del SGSI.

3.6 Promuovere una cultura di responsabilità, consapevolezza e resilienza in cui le responsabilità in materia di sicurezza siano comprese e attuate da tutto il personale.

4. Ruoli e responsabilità

4.1 Direzione esecutiva

4.1.1 Approva e sostiene la Politica per la sicurezza delle informazioni e il framework del SGSI.

4.1.2 Assicura l'allineamento tra gli obiettivi di sicurezza e la strategia aziendale.

4.1.3 Fornisce l'esempio e promuove una solida cultura della sicurezza delle informazioni.

4.1.4 Riesamina e approva le modifiche rilevanti al campo di applicazione del SGSI, al trattamento del rischio e all'assetto di governance.

4.2 Chief Information Security Officer (CISO) / Responsabile del SGSI

4.2.1 È titolare del SGSI e mantiene la presente politica in conformità alla ISO/IEC 27001.

4.2.2 Guida i processi di valutazione del rischio, attuazione dei controlli e miglioramento continuo.

4.2.3 Assicura il coordinamento trasversale delle attività di sicurezza e supervisiona le politiche subordinate.

4.2.4 Riferisce alla Direzione esecutiva sullo stato del SGSI, sugli incidenti, sui risultati degli audit e sulle metriche.

4.2.5 Assicura che i riesami e gli aggiornamenti della politica siano condotti in conformità alla Sezione 9 del presente documento.

[... 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 Frequenza di riesame

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

9.1.1.1 Modifiche significative degli obblighi legali, normativi o contrattuali

9.1.1.2 Cambiamenti sostanziali del profilo di rischio dell'organizzazione

9.1.1.3 Esiti di audit interni o esterni

9.1.1.4 Incidenti gravi o malfunzionamenti dei controlli

9.2 Autorità e processo di riesame

9.2.1 Il CISO o il Responsabile del SGSI designato deve guidare il processo di riesame.

9.2.2 Gli elementi in ingresso al riesame devono includere:

9.2.2.1 I risultati degli audit interni

9.2.2.2 Le tendenze delle valutazioni del rischio

9.2.2.3 I cambiamenti nei processi aziendali e nelle tecnologie

9.2.2.4 Le prestazioni rispetto agli indicatori chiave di prestazione e alle soglie di rischio

9.2.3 Tutti gli aggiornamenti devono:

9.2.3.1 Essere soggetti a controllo di versione ed essere documentati

9.2.3.2 Essere approvati dalla Direzione esecutiva

9.2.3.3 Essere distribuiti a tutte le parti interessate attraverso i canali ufficiali di comunicazione

9.2.3.4 Attivare i necessari aggiornamenti della documentazione subordinata e della formazione

10. Politiche correlate e collegamenti

10.1 La presente politica quadro è direttamente collegata alle seguenti politiche e ai seguenti framework di sicurezza dell'organizzazione:

10.1.1 P2 – Politica sui ruoli e le responsabilità di governance: definisce la struttura di governance e la gerarchia delle autorità richiamate nel presente documento.

10.1.2 P3 – Politica di uso accettabile: disciplina la conformità comportamentale e l'utilizzo accettabile degli asset informativi.

10.1.3 P4 – Politica di controllo degli accessi: rende operativi i controlli relativi agli accessi derivati dalla presente politica generale.

10.1.4 P6 – Politica di gestione del rischio: fornisce il contesto basato sul rischio per la selezione dei controlli e l'accettazione dei rischi residui.

10.1.5 P33 – Politica di monitoraggio dell'audit e della conformità: descrive in dettaglio come i meccanismi interni di assurance convalidano l'applicazione della politica.

10.2 Tali interdipendenze assicurano un allineamento completo e la tracciabilità nell'intero SGSI e supportano una governance unificata del rischio e della conformità.

11. Standard e quadri di riferimento

11.1 La presente Politica per la sicurezza delle informazioni è formalmente allineata ai seguenti standard e quadri di riferimento al fine di assicurare piena conformità, dimostrabilità in sede di audit e difendibilità sotto il profilo regolatorio:

11.2 ISO/IEC 27001

11.2.1 Clausola 5.1 – Leadership e impegno: la presente politica dimostra l'impegno dell'alta direzione verso la sicurezza delle informazioni e definisce responsabilità e allocazione delle risorse per il SGSI.

11.2.2 Clausola 5.2 – Politica per la sicurezza delle informazioni: il presente documento costituisce la politica formale di sicurezza dell'organizzazione, allineata agli obiettivi di sicurezza dichiarati, alla strategia aziendale e alla conformità alla ISO/IEC 27001.

11.2.3 Clausola 6.1 – Azioni per affrontare rischi e opportunità: l'approccio basato sul rischio riflesso nella presente politica assicura che le risorse di sicurezza siano applicate in misura proporzionata alle minacce.

11.2.4 Clausola 9.2 – Audit interno e Clausola 10 – Miglioramento: la presente politica è integrata nel ciclo di miglioramento continuo dell'organizzazione ed è soggetta a convalida da parte dell'audit interno.

11.2.5 ISO/IEC 27002:2022 – Controllo 5.1: specifica linee guida per l'istituzione e il mantenimento delle politiche di sicurezza. La presente politica riflette le raccomandazioni della ISO/IEC 27002 in materia di documentazione gerarchica, cicli di riesame e applicabilità.

11.3 NIST SP 800-53 Rev.5

11.3.1 PL-1 (Politica e procedure di pianificazione della sicurezza): la presente politica soddisfa il requisito di sviluppare, diffondere e riesaminare una politica formale di sicurezza delle informazioni valida per l'intera organizzazione.

11.3.2 PM-1–PM-5: affronta la governance a livello di programma, inclusi ruoli per la sicurezza delle informazioni, allocazione delle risorse, strategia di rischio e integrazione della pianificazione della sicurezza nelle operazioni aziendali.

11.4 GDPR UE (2016/679)

11.4.1 Articolo 5(2): dà attuazione al principio di accountability. La presente politica definisce i soggetti responsabili e le azioni applicative tracciabili.

11.4.2 Articolo 24: richiede l'attuazione di misure tecniche e organizzative, incluse politiche allineate al rischio.

11.4.3 Articolo 32: supporta l'attuazione di misure adeguate per garantire la sicurezza dei dati personali durante l'intero ciclo di vita.

11.5 Direttiva UE NIS2 (2022/2555)

11.5.1 Articolo 21(2)(a): impone ai soggetti obbligati di attuare una politica di sicurezza documentata che disciplini la gestione del rischio e la governance. La presente politica soddisfa tale requisito e supporta, più in generale, la preparazione in materia di cibersicurezza e la protezione delle infrastrutture critiche.

11.6 Regolamento UE DORA (2022/2554)

11.6.1 Articolo 5(2): richiede un framework di controllo interno documentato per la gestione del rischio ICT. La presente politica supporta la conformità del settore finanziario assegnando ruoli, controlli e funzioni di supervisione allineati alle aspettative di governance previste dal DORA.

11.7 COBIT 2019

11.7.1 EDM01 – Definizione del framework di governance: la presente politica supporta la governance aziendale definendo i ruoli del SGSI, gli impegni della leadership e gli obiettivi strategici.

11.7.2 APO01 – Framework di gestione: supporta l'istituzione e il funzionamento di un SGSI strutturato.

11.7.3 APO12 – Gestione del rischio: fornisce il fondamento per la governance dei rischi per la sicurezza delle informazioni.

11.7.4 MEA01/MEA03 – Monitorare, valutare e analizzare: rafforza la valutazione continua delle prestazioni e il monitoraggio dei controlli interni attraverso l'applicazione della conformità alla politica.