					Inserire qui la denominazione dell'entità giuridica registrata							
Numero del documento: P06					Titolo del documento: **Politica di gestione del rischio**							
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**

Allineamento a standard e regolamenti

Standard/Regulation	Clause/Article	Comment
ISO/IEC 27001:2022	Clausole 6.1, 8.32, 10	Elementi fondamentali per l'identificazione e la gestione del rischio, integrazione nella gestione delle modifiche, miglioramento continuo
ISO/IEC 27005:2024	Metodologia completa del ciclo di vita del rischio	Processo completo di gestione del rischio in linea con lo standard
ISO 31000:2018	Principi e quadro di riferimento per la gestione del rischio	Principi di gestione del rischio adottati nel quadro di riferimento
NIST SP 800-30 Rev.1	SP 800-30, SP 800-39	Linee guida e struttura per le valutazioni del rischio, governance del rischio su più livelli
GDPR UE	Articoli 24, 25, 32	Processi e controlli per i rischi relativi alla protezione dei dati
Direttiva UE NIS2	Articolo 21(2)(a–d)	Obblighi di valutazione del rischio e della sicurezza
Regolamento UE DORA	Articoli 5, 6	Gestione del rischio ICT e resilienza operativa
COBIT 2019	APO12, MEA	Struttura e supervisione della gestione del rischio

1. Scopo

1.1 La presente politica definisce un quadro di riferimento unificato e formalizzato per identificare, analizzare, valutare, trattare, monitorare e riesaminare i rischi per la sicurezza delle informazioni nell'intera organizzazione.

1.2 Essa garantisce l'applicazione coerente di principi basati sul rischio a tutela della riservatezza, integrità e disponibilità (CIA) degli asset informativi, in conformità alla Clausola 6.1 della ISO/IEC 27001:2022 e alla ISO 31000:2018.

1.3 La politica integra la gestione del rischio per la sicurezza delle informazioni nei processi decisionali dell'organizzazione al fine di conseguire gli obiettivi strategici interni e soddisfare i requisiti normativi esterni.

2. Ambito di applicazione

2.1 La presente politica si applica a tutte le unità organizzative, ai processi aziendali, ai sistemi, al personale e ai rapporti con terze parti coinvolti nel trattamento, nello sviluppo, nella conservazione o nella gestione degli asset informativi.

2.2 L'ambito di applicazione si estende ai beni fisici e digitali, nonché agli asset ospitati in cloud, inclusi dati strutturati e non strutturati, applicazioni, infrastrutture, reti e servizi.

2.3 Essa copre i rischi per la sicurezza delle informazioni a livello strategico, operativo, progettuale e tecnico ed è obbligatoria per tutti i dipendenti, i collaboratori esterni e i fornitori di servizi coinvolti nelle attività del Sistema di gestione della sicurezza delle informazioni (SGSI).

2.4 La gestione del rischio deve essere applicata ai seguenti scenari:

2.4.1 Implementazione di un nuovo progetto o sistema

2.4.1.1 Modifiche significative (ad es. architettura, titolarità, processi)

2.4.1.2 Inserimento di fornitori e accordi con terze parti

2.4.1.3 Risposta agli incidenti e riesami post-incidente

2.4.1.4 Riesami periodici del rischio organizzativo o audit

3. Obiettivi

3.1 Stabilire e rendere operativo un processo di gestione del rischio ripetibile e applicabile all'intera organizzazione, basato sulle metodologie ISO/IEC 27005 e ISO 31000.

3.2 Garantire che i rischi siano identificati, analizzati, valutati e trattati mediante metodi strutturati e tracciabili, inclusa l'assegnazione della titolarità del rischio e il collegamento ai controlli.

3.3 Mantenere un registro dei rischi centralizzato e soggetto a controllo delle versioni, nonché un piano di trattamento del rischio, che riflettano lo stato corrente del rischio, la copertura dei controlli e lo stato di avanzamento della mitigazione.

3.4 Allineare le decisioni sul rischio ai livelli documentati di propensione al rischio e tolleranza al rischio, consentendo decisioni di governance informate in materia di accettazione, mitigazione, trasferimento o evitamento del rischio.

3.5 Monitorare continuamente le tendenze degli eventi di rischio e garantire l'efficacia dei trattamenti del rischio, consentendo al contempo adeguamenti proattivi in funzione dell'evoluzione delle minacce o dei cambiamenti aziendali.

4. Ruoli e responsabilità

4.1 Direzione aziendale / Consiglio di amministrazione

4.1.1 Approva il quadro di riferimento per la gestione del rischio e definisce la propensione al rischio accettabile e le soglie di tolleranza.

4.1.2 Autorizza le strategie di trattamento del rischio per i rischi residui che eccedono la tolleranza.

4.1.3 Assegna risorse e assicura la supervisione necessaria per l'efficace funzionamento del programma di gestione del rischio.

4.2 Responsabile del SGSI / Responsabile del rischio

4.2.1 È titolare della presente politica e ne garantisce l'allineamento con gli standard ISO/IEC 27001 e ISO/IEC 27005.

4.2.2 Coordina il processo aziendale di valutazione del rischio e mantiene il registro dei rischi e il piano di trattamento del rischio.

4.2.3 Garantisce riesami periodici ed escalation dei rischi principali verso la Direzione aziendale o il Comitato direttivo del SGSI.

[... 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 e il relativo quadro di riferimento devono essere riesaminati annualmente oppure:

9.1.1 Dopo un evento di rischio rilevante o un incidente di sicurezza

9.1.2 A seguito di una modifica organizzativa o tecnica significativa

9.1.3 In risposta alle risultanze dell'audit o a nuovi requisiti normativi

9.2 Il Responsabile del SGSI, il Responsabile del rischio e il Team di conformità sono congiuntamente responsabili di:

9.2.1 Avviare il ciclo di riesame

9.2.2 Raccogliere input dalle unità aziendali

9.2.3 Riesaminare procedure e soglie, se necessario

9.3 Tutte le revisioni devono essere:

9.3.1 Soggette a controllo delle versioni e registrate

9.3.2 Approvate dalla Direzione aziendale

9.3.3 Comunicate alle parti interessate

9.3.4 Conservate nel repository di audit per un periodo minimo di 5 anni

10. Politiche correlate e collegamenti

10.1 La presente politica è interdipendente con le seguenti politiche per la sicurezza delle informazioni:

10.1.1 P1 – Politica per la sicurezza delle informazioni: definisce il modello generale di governance della sicurezza nel cui ambito opera la presente politica di gestione del rischio.

10.1.2 P2 – Politica sui ruoli e sulle responsabilità di governance: definisce i soggetti responsabili e i livelli di governance richiamati nella matrice di escalation del rischio.

10.1.3 P5 – Politica di gestione delle modifiche: attiva la rivalutazione del rischio per le modifiche dell'infrastruttura e dell'organizzazione.

10.1.4 P13 – Politica di classificazione ed etichettatura dei dati: supporta la valutazione dell'impatto durante l'identificazione del rischio.

10.1.5 P33 – Politica di monitoraggio dell'audit e della conformità: convalida la conformità alle politiche, inclusa la completezza del registro dei rischi e le evidenze dei trattamenti.

11. Norme e quadri di riferimento

11.1 La presente politica è espressamente allineata ai seguenti standard e quadri di riferimento per garantire l'adozione delle migliori pratiche internazionali e la conformità alle aspettative normative in materia di gestione dei rischi per la sicurezza delle informazioni:

11.2 ISO/IEC 27001:

11.2.1 Clausola 6.1: stabilisce i requisiti per identificare rischi e opportunità, incluso l'intero ciclo di vita delle valutazioni e dei trattamenti del rischio per la sicurezza delle informazioni. La presente politica rende operative la Clausola 6.1.2 e la Clausola 6.1.3 mediante un quadro di riferimento strutturato che impone protocolli documentati per l'identificazione, l'analisi, la valutazione, il trattamento e l'accettazione del rischio residuo.

11.2.2 Clausola 8.32: l'integrazione di un approccio basato sul rischio nei processi di gestione delle modifiche garantisce che tutte le modifiche organizzative significative attivino rivalutazioni formali del rischio.

11.2.3 Clausola 10: il miglioramento continuo è integrato tramite riesami periodici della politica, analisi delle tendenze del rischio e aggiornamenti della SoA guidati dagli esiti delle valutazioni del rischio.

11.3 ISO/IEC 27005:

11.3.1 Fornisce linee guida specialistiche e dettagliate sulla gestione dei rischi per la sicurezza delle informazioni. La presente politica attua l'intero modello di processo del rischio ISO/IEC 27005: definizione del contesto, identificazione del rischio, analisi del rischio, valutazione del rischio, trattamento del rischio, accettazione del rischio, comunicazione del rischio, monitoraggio e riesame del rischio.

11.4 ISO 31000:

11.4.1 La presente politica integra i principi della ISO 31000, quali l'impegno della leadership, l'integrazione con il processo decisionale e il miglioramento continuo. Essa garantisce che la gestione del rischio sia integrata nella cultura e nelle operazioni dell'organizzazione.

11.5 NIST SP 800-30 Rev.1:

11.5.1 È allineata alla guida NIST per lo svolgimento delle valutazioni del rischio, inclusi identificazione delle minacce, analisi delle vulnerabilità, stima della probabilità e determinazione dell'impatto. La struttura della presente politica rispecchia le fasi di valutazione del rischio definite dal NIST e le adatta sia ai processi tecnici sia a quelli aziendali.

11.6 NIST SP 800-39:

11.6.1 Supporta la governance del rischio a livello aziendale, enfatizzando una gestione del rischio articolata per livelli organizzativi, missione/processo aziendale e sistema informativo. La politica garantisce che la titolarità del rischio sia chiaramente definita a tutti i livelli e includa strategie di trattamento a livello organizzativo.

11.7 GDPR UE:

11.7.1 Articolo 24: richiede l'attuazione di misure tecniche e organizzative appropriate per garantire che i rischi relativi alla protezione dei dati siano gestiti correttamente, aspetto affrontato tramite il processo di rischio strutturato previsto dalla presente politica.

11.7.2 Articolo 25: la "protezione dei dati fin dalla progettazione e per impostazione predefinita" è coerente con l'integrazione del trattamento del rischio nella progettazione di sistemi e processi.

11.7.3 Articolo 32: impone un approccio basato sul rischio alle misure di sicurezza, soddisfatto tramite valutazioni del rischio basate sull'impatto e selezione dei controlli.

11.8 Direttiva UE NIS2:

11.8.1 Articolo 21(2)(a–d): richiede che i soggetti effettuino valutazioni del rischio, adottino politiche sull'analisi del rischio e garantiscano misure di sicurezza proporzionate. La presente politica soddisfa tali obblighi attraverso l'applicazione continua del ciclo di vita del rischio e una governance documentata.

11.9 Regolamento UE DORA:

11.9.1 Articolo 5: richiede un quadro di riferimento documentato per la gestione del rischio ICT, pienamente coperto dall'architettura della presente politica, inclusa la mappatura con la SoA e i KRI.

11.9.2 Articolo 6: richiede l'integrazione della gestione del rischio nelle strategie di resilienza operativa, aspetto affrontato tramite matrici di escalation e tracciamento degli asset critici.

11.10 COBIT 2019:

11.10.1 APO12 – Manage Risk: corrisponde direttamente all'istituzione da parte dell'organizzazione di un approccio strutturato alla gestione del rischio, con assegnazione dei ruoli, tracciamento dei trattamenti e garanzia di responsabilità a livello di Consiglio di amministrazione.

11.10.2 MEA01 – Monitor, Evaluate and Assess Performance and Conformance: è riflesso nell'attenzione della presente politica all'analisi delle tendenze, al monitoraggio dei KRI e all'integrazione del feedback di audit nei cicli di miglioramento continuo.