					Inserire qui la denominazione dell'entità giuridica registrata							
Numero del documento: P06S					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**

Allineata a standard e regolamenti

Standard/Regulation	Clause/Article	Comment
ISO/IEC 27001:2022	Clausole 6.1, 6.1.3	
ISO/IEC 27002:2022	5.4, 5.25	
NIST SP 800-53 Rev. 5	RA-1 a RA-7, PM-9	
Direttiva UE NIS2	Articolo 21(2)(a–d)	
Regolamento UE DORA	Articolo 5	
COBIT 2019	APO12, MEA01	

1. Scopo

1.1 La presente politica definisce le modalità con cui l'organizzazione identifica, valuta e gestisce i rischi relativi alla sicurezza delle informazioni, alle operazioni, alla tecnologia e ai servizi erogati da terze parti.

1.2 Garantisce che la gestione del rischio sia parte integrante della pianificazione, dell'esecuzione dei progetti, della selezione dei fornitori e della risposta agli incidenti, in conformità alla ISO 27001, alla ISO 31000 e ai requisiti normativi applicabili.

1.3 La politica supporta decisioni consapevoli, la protezione degli asset informativi e la resilienza delle principali operazioni aziendali.

2. Ambito di applicazione

2.1 La presente politica si applica a:

2.1.1 Tutti i dipartimenti, i sistemi e gli utenti dell'organizzazione

2.1.2 Tutte le informazioni, i servizi e gli asset gestiti internamente o tramite terze parti

2.1.3 Tutte le attività correlate al rischio, inclusi riesami di progetto, aggiornamenti dei sistemi, esternalizzazione e conformità normativa

2.2 Include tutte le tipologie di rischio, quali:

2.2.1 Minacce di cybersicurezza e vulnerabilità dei sistemi

2.2.2 Interruzioni operative e indisponibilità dei servizi

2.2.3 Esposizioni legali, di conformità o reputazionali

2.2.4 Rischi relativi alle terze parti e alla catena di fornitura

2.3 Tutti i dipendenti, i collaboratori esterni e i fornitori di servizi devono rispettare la presente politica nell'identificazione e nella segnalazione dei rischi.

3. Obiettivi

3.1 Integrare nelle normali operazioni aziendali procedure di valutazione del rischio semplici e ripetibili.

3.2 Identificare e attribuire priorità ai rischi che potrebbero incidere su riservatezza, integrità e disponibilità (CIA) o sulla conformità normativa.

3.3 Assegnare la responsabilità e definire azioni di trattamento per tutti i rischi significativi.

3.4 Mantenere un Registro dei rischi accurato e aggiornato a supporto della dimostrabilità della conformità e del monitoraggio dei rischi.

3.5 Assicurare il coinvolgimento della direzione nell'approvazione della tolleranza al rischio e dei principali piani di trattamento.

4. Ruoli e responsabilità

4.1 Direttore generale

4.1.1 Definisce la propensione al rischio dell'organizzazione e approva il quadro di gestione del rischio.

4.1.2 Approva le principali decisioni di trattamento del rischio e le risorse necessarie.

4.1.3 Riesamina trimestralmente i principali rischi con il Coordinatore del rischio.

4.2 Coordinatore del rischio (o Responsabile del SGSI)

4.2.1 Facilita le valutazioni del rischio e mantiene il Registro dei rischi.

4.2.2 Garantisce che il punteggio di rischio, la titolarità e le azioni di trattamento siano documentati.

4.2.3 Organizza almeno un riesame formale del rischio all'anno.

[... 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 della politica

9.1.1 La presente politica deve essere riesaminata almeno una volta all'anno dal Direttore generale e dal Coordinatore del rischio per assicurarne la pertinenza e la completezza.

9.2 Trigger di aggiornamento

9.2.1 Il riesame e l'aggiornamento anticipati devono avvenire se:

9.2.1.1 Un incidente rilevante o una risultanza di audit evidenzia lacune nei controlli di gestione del rischio

9.2.1.2 Vengono introdotte nuove unità aziendali, tecnologie o partnership

9.2.1.3 Cambia un requisito normativo o contrattuale

9.3 Controllo delle versioni

9.3.1 Tutti gli aggiornamenti alla presente politica devono essere soggetti a controllo delle versioni con i seguenti metadati:

9.3.1.1 Numero di versione e data di entrata in vigore

9.3.1.2 Sintesi delle modifiche

9.3.1.3 Soggetto approvante (Direttore generale)

9.3.1.4 Versioni precedenti archiviate ai fini dell'audit

9.4 Comunicazione e sensibilizzazione delle parti interessate

9.4.1 Le versioni aggiornate della politica e i principali piani di trattamento del rischio devono essere comunicati al personale interessato. La formazione annuale di sensibilizzazione deve includere i principi di base della consapevolezza del rischio.

10. Politiche correlate e collegamenti

10.1 La presente politica opera in coordinamento con altre politiche al fine di garantire una governance della sicurezza completa:

10.1.1 P2S – Politica sui ruoli e sulle responsabilità di governance: definisce chi è responsabile della titolarità del rischio e del processo decisionale.

10.1.2 P5S – Politica di gestione delle modifiche: richiede una valutazione del rischio prima dell'attuazione di modifiche tecniche o procedurali.

10.1.3 P17S – Politica di protezione dei dati e privacy: tratta il rischio normativo associato al trattamento dei dati personali.

10.1.4 P30S – Politica di risposta agli incidenti: assicura che il trattamento del rischio prosegua durante e dopo gli incidenti di sicurezza.

10.1.5 P33S – Politica di continuità operativa: identifica i rischi residui e le misure di ripristino per i servizi critici.

11. Norme e quadri di riferimento

11.1 ISO/IEC 27001:

11.1.1 Clausola 6.1 – Definisce un processo formale di gestione del rischio e la pianificazione del trattamento.

11.1.2 Clausola 6.1.3 – Richiede alle organizzazioni di conservare piani di trattamento e approvazioni documentati.

11.2 ISO/IEC 27002:

11.2.1 Controlli 5.4, 5.25 – Forniscono indicazioni applicative per la titolarità del rischio, la prioritizzazione e la gestione del ciclo di vita.

11.3 NIST SP 800-53 Rev. 5:

11.3.1 RA-1 a RA-7 – Definiscono la valutazione del rischio, le strategie di risposta, la documentazione e i meccanismi di riesame.

11.4 PM-9 – Richiede una vigilanza coerente da parte della direzione sui rischi dei sistemi informativi dell'organizzazione.

11.5 Direttiva UE NIS2

11.5.1 Articolo 21(2)(a–d) – Impone ai soggetti essenziali e importanti controlli obbligatori di valutazione del rischio, mitigazione e governance.

11.6 Regolamento UE DORA

11.6.1 Articolo 5 – Richiede ai soggetti regolamentati di definire e gestire quadri di gestione del rischio ICT, inclusi identificazione, classificazione e risposta.

11.7 COBIT 2019

11.7.1 APO12 – Gestire il rischio: integra il rischio nella pianificazione strategica e operativa.

11.7.2 MEA01 – Monitorare, valutare e analizzare: garantisce l'efficacia e la conformità dei processi e delle azioni di trattamento del rischio.