					Inserire qui la denominazione dell'entità giuridica registrata							
Numero del documento: P15S					Titolo del documento: **Politica di backup e ripristino**							
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/Regolamento	Clausola/Articolo	Commento
ISO/IEC 27001:2022	Clausola 8	Controlli di backup in conformità ai requisiti del SGSI
ISO/IEC 27002:2022	Controlli 5.29, 8	Buone pratiche per il backup e integrazione con la continuità operativa
NIST SP 800-53 Rev.5	CP-9, MP-6	Backup e protezione dei supporti
Direttiva UE NIS2	Articolo 21(2)(c)	Resilienza e continuità mediante backup
Regolamento UE DORA	Articolo 10(1)	Continuità dei sistemi ICT - backup per le organizzazioni del settore finanziario
COBIT 2019	BAI04.05, DSS04	Documentazione e test dei backup, controllo dei processi
GDPR UE	Articoli 5(1)(f), 32(1)(c)	Integrità, disponibilità e tempestivo ripristino dei dati

1. Finalità

1.1 La presente politica definisce le modalità con cui l'organizzazione esegue e gestisce i backup al fine di garantire la continuità operativa, proteggere dalla perdita di dati e consentire il ripristino tempestivo a seguito di incidenti.

1.2 Essa stabilisce regole vincolanti per l'esecuzione del backup, l'archiviazione e il ripristino di sistemi e dati, in particolare nelle piccole e medie imprese (PMI) prive di un'infrastruttura IT complessa.

1.3 La presente politica supporta la capacità di dimostrare la conformità e conseguire la certificazione ISO/IEC 27001, assicurando che i controlli essenziali di backup siano definiti, applicati in modo coerente e riesaminati regolarmente.

1.4 La capacità dell'organizzazione di riprendersi da guasti tecnici, cancellazioni accidentali o incidenti informatici dipende dal rigoroso rispetto della presente politica.

2. Ambito di applicazione

2.1 La presente politica si applica a tutti i sistemi aziendali e ai dati, inclusi:

2.1.1 registrazioni finanziarie, informazioni sui clienti e dati HR

2.1.2 desktop, laptop, server e applicazioni cloud utilizzati nelle operazioni aziendali

2.1.3 supporti di backup quali unità USB, sistemi di archiviazione esterni o backup basati su cloud

2.2 Si applica inoltre a tutti i soggetti che hanno responsabilità nel trattamento o nella gestione dei processi di backup, inclusi:

2.2.1 il Direttore generale (GM) o il responsabile designato

2.2.2 il fornitore di supporto IT esterno o i consulenti, ove applicabile

2.2.3 tutti i dipendenti responsabili del salvataggio dei dati in posizioni approvate

3. Obiettivi

3.1 Garantire che tutti i dati e i sistemi aziendali critici siano sottoposti a backup in modo sicuro, con frequenze adeguate in funzione del rischio e delle esigenze operative.

3.2 Garantire che i dati possano essere ripristinati in modo tempestivo e completo a seguito di interruzioni.

3.3 Prevenire accessi non autorizzati, manomissioni o perdita dei dati di backup mediante efficaci controlli di archiviazione.

3.4 Assegnare in modo chiaro e attuare ruoli e responsabilità per l'esecuzione e il test delle procedure di backup.

3.5 Supportare la conformità a ISO/IEC 27001, al GDPR e ad altri obblighi normativi mediante pratiche di backup strutturate e documentate.

4. Ruoli e responsabilità

4.1 Direttore generale (GM)

4.1.1 Approva la presente politica e ne garantisce l'attuazione

4.1.2 Assegna le risorse e attribuisce le responsabilità per le attività di backup e ripristino

4.1.3 Riesamina i fallimenti dei backup, gli incidenti o le deviazioni dalla politica

4.1.4 Conduce il riesame annuale della politica e garantisce la capacità di dimostrare la conformità

4.2 Fornitore di supporto IT, ove applicabile

4.2.1 Implementa e gestisce le soluzioni di backup (on-premise o basate su cloud)

4.2.2 Monitora l'esito dei backup e pianifica i test di ripristino

4.2.3 Segnala direttamente al GM guasti e incidenti

4.2.4 Garantisce la cifratura, le restrizioni di accesso e la corretta gestione dei supporti di backup

[... 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 deve essere riesaminata dal GM almeno una volta l'anno. I fattori che attivano riesami intermedi includono:

9.1.1 modifiche rilevanti ai sistemi o ai metodi di archiviazione

9.1.2 introduzione di nuove piattaforme cloud o IT

9.1.3 modifiche legali o normative che incidono sul ripristino dei dati

9.1.4 risultanze dell'audit o incidenti

9.2 Il GM è responsabile dell'avvio del riesame, dell'approvazione delle modifiche e della comunicazione degli aggiornamenti.

9.3 Le versioni della politica devono essere tracciate e archiviate. L'accesso alle versioni sostituite deve essere limitato per evitare confusione durante gli audit o gli eventi di ripristino aziendale.

10. Politiche correlate e collegamenti

10.1 La presente politica è allineata alle seguenti politiche SME e dipende da esse:

10.1.1 P14S – Politica di conservazione e smaltimento dei dati: definisce per quanto tempo i dati di backup devono essere conservati e cancellati in modo sicuro.

10.1.2 P13S – Politica di classificazione ed etichettatura dei dati: aiuta a stabilire la priorità dei dati che devono essere sottoposti a backup in base ai livelli di classificazione.

10.1.3 P30S – Politica di risposta agli incidenti: disciplina le procedure da seguire in caso di fallimento dei backup o qualora sia necessario il ripristino dei dati a seguito di una violazione o di un'indisponibilità del servizio.

10.1.4 P2S – Politica sui ruoli e sulle responsabilità di governance: assegna in modo chiaro l'autorità per la supervisione dei backup e l'attuazione della politica.

10.1.5 P17S – Politica di protezione dei dati e privacy: garantisce che la gestione dei backup dei dati personali sia allineata ai requisiti legali e alla normativa in materia di privacy.

11. Standard e quadri di riferimento

11.1 ISO/IEC 27001

11.1.1 Clausola 8.1: pianificazione operativa e controllo dei sistemi di backup nell'ambito del SGSI

11.2 ISO/IEC 27002

11.2.1 Controllo 8.13: prescrive buone pratiche per la pianificazione, il monitoraggio e il ripristino dei backup

11.2.2 Allegato A, Controllo 5.29: integrazione del backup con la continuità operativa e la prontezza al ripristino

11.3 NIST SP 800-53 Rev.5

11.3.1 CP-9 (Contingency Planning): definisce strategie di backup strutturate per la resilienza aziendale

11.3.2 MP-6 (Media Protection): richiede la gestione sicura e la distruzione dei supporti di backup

11.4 GDPR UE

11.4.1 Articolo 5(1)(f): impone l'integrità e la disponibilità dei dati personali

11.4.2 Articolo 32(1)(c): richiede la capacità di ripristinare tempestivamente l'accesso ai dati personali

11.5 Direttiva UE NIS2

11.5.1 Articolo 21(2)(c): richiede backup e ripristino nell'ambito della pianificazione della resilienza e della continuità

11.6 Regolamento UE DORA

11.6.1 Articolo 10(1): le organizzazioni del settore finanziario devono garantire il backup nell'ambito delle misure di continuità dei sistemi ICT

11.7 COBIT 2019

11.7.1 BAI04.05: richiede strategie di backup documentate

11.7.2 DSS04.07: pone l'accento sul test periodico e sul controllo dei processi di backup e ripristino dei dati