					Inserire qui la denominazione dell'entità giuridica registrata							
Numero del documento: P14					Titolo del documento: **Politica di conservazione e smaltimento dei dati**							
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 norme e regolamenti

Norma/Regolamento	Clausola/Articolo	Commento
ISO/IEC 27001:2022	Clausole 6.1.3, 8.1	
ISO/IEC 27002:2022	Controlli 5.10, 5.12, 5.30, 5	
NIST SP 800-53 Rev. 5	AU-11, MP-6, SI-12, PL-2	
GDPR UE	Articoli 5(1)(e), 17, 32	
NIS2 UE	Articolo 21(2)(a-e)	
DORA UE	Articoli 5, 9	
COBIT 2019	DSS01, DSS05, MEA	

1. Finalità

1.1 La finalità della presente politica è definire i requisiti organizzativi per la conservazione dei dati e il loro smaltimento sicuro in tutte le fasi del ciclo di vita delle informazioni. Essa garantisce la conformità agli obblighi legali, normativi e contrattuali applicabili e previene l'accumulo non necessario o rischioso di dati.

1.2 La presente politica supporta l'attuazione della ISO/IEC 27001:2022 imponendo il controllo sui tempi di conservazione dei dati e sulle pratiche di smaltimento irreversibile. Consente una documentazione tracciabile delle registrazioni, impone periodi di conservazione allineati alla sensibilità e alla classificazione delle informazioni e assicura la disponibilità delle evidenze richieste in sede di audit, ispezione regolatoria e attività istruttorie legali.

1.3 Essa mira inoltre a tutelare la riservatezza, l'integrità e la disponibilità (CIA) dei dati, riducendo al minimo il rischio aziendale, le inefficienze operative e l'esposizione a violazioni della privacy derivanti da conservazione o distruzione improprie dei dati.

2. Ambito di applicazione

2.1 La presente politica si applica a tutti gli asset informativi fisici e digitali posseduti, trattati o conservati dall'organizzazione, inclusi quelli sotto il controllo di terze parti, società controllate o fornitori in outsourcing.

2.2 L'ambito di applicazione include, a titolo esemplificativo e non esaustivo:

2.2.1 Documenti, file e registrazioni, in formato digitale e cartaceo

2.2.2 Database e archivi

2.2.3 E-mail e log di messaggistica istantanea

2.2.4 Backup, log di sistema e tracce di audit

2.2.5 Codice sorgente, dati applicativi e asset ospitati in cloud

2.2.6 Supporti rimovibili e hardware obsoleto contenenti dati

2.3 La politica disciplina sia le registrazioni operative sia i set di dati regolamentati, ad esempio contenuti finanziari, legali, HR, relativi ai clienti e rilevanti ai fini di audit, indipendentemente dall'ubicazione di archiviazione o dal sistema utilizzato.

2.4 Si applica a tutti i dipartimenti dell'organizzazione e a tutti i dipendenti, collaboratori esterni e fornitori coinvolti nella creazione, conservazione, gestione o smaltimento dei dati.

3. Obiettivi

3.1 Assicurare che i dati siano conservati solo per il tempo necessario sotto il profilo legale, contrattuale o operativo e che siano smaltiti in modo sicuro quando non più necessari.

3.2 Prevenire la cancellazione prematura, non autorizzata o accidentale di registrazioni necessarie per operazioni in corso, conformità, contenzioso o finalità di audit.

3.3 Stabilire e applicare piani di conservazione coerenti basati sulla classificazione delle informazioni, sul tipo di asset, sulle leggi applicabili e sull'esposizione al rischio.

3.4 Tutelare la privacy e la riservatezza dei dati durante il periodo di conservazione e al momento dello smaltimento, incluso il soddisfacimento dei diritti degli interessati, ad esempio la cancellazione ai sensi dell'articolo 17 del GDPR.

3.5 Assicurare che tutti i metodi di smaltimento dei dati siano irreversibili, adeguatamente documentati e conformi a standard riconosciuti quali il NIST SP 800-88.

3.6 Ridurre al minimo le inefficienze operative, i costi aggiuntivi e l'esposizione legale causati da conservazione eccessiva o da dati legacy non tracciati.

3.7 Supportare gli obiettivi di continuità operativa e di ripristino in caso di disastro mediante una governance integrata della conservazione dei backup e pratiche di archiviazione dei dati difendibili.

4. Ruoli e responsabilità

4.1 Direzione esecutiva

4.1.1 Approva la presente politica e assicura finanziamenti, risorse e adeguata integrazione nei programmi di gestione del rischio aziendale e di conformità.

4.1.2 Mantiene la responsabilità complessiva della conformità legale e regolatoria relativa alla conservazione dei dati e al loro smaltimento sicuro.

4.2 Chief Information Security Officer (CISO)

4.2.1 È il titolare della politica ed è responsabile della definizione e del riesame della governance della conservazione e dello smaltimento in allineamento con il SGSI.

4.2.2 Assicura che i requisiti di conservazione e smaltimento basati sulla classificazione siano applicati nelle unità aziendali e nei sistemi tecnici.

4.2.3 Monitora la conformità alla politica e dispone azioni correttive ove necessario.

[... 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 annualmente o al ricorrere di una delle seguenti condizioni:

9.1.1 Modifiche alle leggi o ai regolamenti applicabili che incidono sulla conservazione dei dati, ad esempio aggiornamenti del GDPR, dei codici tributari o del DORA

9.1.2 Revisioni del quadro di classificazione o dei processi aziendali che incidono sulle fasi del ciclo di vita dei dati

9.1.3 Introduzione di nuovi sistemi IT, piattaforme di archiviazione o tecnologie di smaltimento dei supporti

9.1.4 Risultanze dell'audit interno o raccomandazioni regolatorie che evidenziano carenze nelle pratiche di conservazione o smaltimento

9.2 Il riesame deve essere condotto dal CISO e dal Responsabile della protezione dei dati (DPO), con il contributo della funzione legale e compliance, dell'IT e delle unità aziendali.

9.3 Il piano generale di conservazione dei dati (MDRS) e il registro di smaltimento devono essere riesaminati in parallelo per assicurare che:

9.3.1 I piani rimangano accurati e riflettano esigenze operative, legali e regolatorie

9.3.2 La documentazione di smaltimento sia completa e verificabile in sede di audit

9.3.3 Le registrazioni di conservazione legale e sospensione della cancellazione siano convalidate e rilasciate quando appropriato

9.4 Qualsiasi aggiornamento della politica deve:

9.4.1 Essere formalmente sottoposto a controllo di versione e conservato nel repository documentale del SGSI

9.4.2 Includere una cronologia delle versioni e la motivazione della modifica

9.4.3 Essere approvato dalla Direzione esecutiva

9.4.4 Essere comunicato al personale interessato con materiali formativi o linee guida aggiornati

9.5 In presenza di modifiche rilevanti alla politica, i dipendenti interessati devono completare una formazione mirata entro 30 giorni dal rilascio per garantire la continua conformità.

9.6 Politiche correlate e collegamenti

10. Politiche correlate e collegamenti

10.1.1 P4 - Politica di controllo degli accessi: assicura che solo i soggetti autorizzati accedano ai dati durante il loro periodo di conservazione e che i dati scaduti siano soggetti a restrizioni in attesa dello smaltimento.

10.1.2 P12 - Politica di gestione degli asset: identifica quali asset contengono dati che richiedono smaltimento programmato e ne traccia il ciclo di vita dall'acquisizione alla distruzione.

10.1.3 P13 - Politica di classificazione ed etichettatura dei dati: guida le decisioni di classificazione che influenzano direttamente la durata di conservazione dei dati e il metodo di smaltimento richiesto.

10.1.4 P15 - Politica di backup e ripristino: definisce i periodi di conservazione e le procedure di smaltimento per i supporti di backup e gli asset di dati replicati.

10.1.5 P18 - Politica sui controlli crittografici: supporta la cancellazione crittografica ai fini dello smaltimento e impone la cifratura durante l'archiviazione dei dati fino alla distruzione.

10.1.6 P30 - Politica di risposta agli incidenti: viene attivata nei casi in cui uno smaltimento improprio comporti potenziale perdita di dati, violazione dei dati o violazione normativa.

10.2 Ciascuna politica collegata contribuisce all'applicazione di un modello di governance dei dati coerente tra classificazione, controllo del ciclo di vita, accessi e capacità di dimostrare la conformità.

11. Standard e quadri di riferimento

11.1 La presente politica è allineata a standard e quadri normativi riconosciuti a livello globale che definiscono pratiche sicure, conformi ed efficienti per il ciclo di vita dei dati.

11.2 ISO/IEC 27001:

11.2.1 Clausola 6.1.3 - Piano di trattamento del rischio: supporta la mitigazione dei rischi associati a conservazione eccessiva, violazioni dei dati o mancato smaltimento.

11.2.2 Clausola 8.1 - Pianificazione e controllo operativi: stabilisce controlli sul ciclo di vita che disciplinano memorizzazione, archiviazione e distruzione.

11.3 ISO/IEC 27002:2022 - Controlli 5.10, 5.12, 5.30, 5: forniscono indicazioni pratiche su uso accettabile dei dati, giustificazione della conservazione, cancellazione controllata e tenuta delle registrazioni difendibile in linea con la tolleranza al rischio dell'organizzazione.

11.4 NIST SP 800-53 Rev. 5:

11.4.1 AU-11 - Conservazione delle registrazioni di audit: assicura una conservazione sufficiente dei log di audit e delle evidenze di conformità.

11.4.2 MP-6 - Sanitizzazione dei supporti: richiede metodi di distruzione sicuri e documentati per supporti fisici ed elettronici.

11.4.3 SI-12 - Gestione delle informazioni: impone un trattamento appropriato dei dati in linea con i controlli di conservazione e smaltimento.

11.4.4 PL-2 - Piano di sicurezza e privacy del sistema: richiede documentazione specifica per sistema sul trattamento del ciclo di vita dei dati e sulle disposizioni per lo smaltimento sicuro.

11.5 GDPR UE (2016/679):

11.5.1 Articolo 5(1)(e) - Minimizzazione dei dati e limitazione della conservazione: richiede che i dati non siano conservati più a lungo del necessario.

11.5.2 Articolo 17 - Diritto alla cancellazione ("diritto all'oblio"): richiede la cancellazione tempestiva e permanente dei dati personali a fronte di una richiesta valida.

11.5.3 Articolo 32 - Sicurezza del trattamento: rafforza la protezione dei dati durante la conservazione e impone la distruzione sicura delle registrazioni scadute.

11.6 Direttiva NIS2 UE (2022/2555):

11.6.1 Articolo 21(2)(a-e): richiede che i soggetti adottino politiche e misure tecniche per la gestione sicura dei dati, comprese limitazioni di conservazione e metodi di smaltimento.

11.7 DORA UE (2022/2554):

11.7.1 Articolo 5 - Governance e controllo: impone una gestione strutturata del rischio ICT, inclusa la gestione sicura del ciclo di vita delle informazioni.

11.7.2 Articolo 9 - Quadro di riferimento per la gestione del rischio ICT: richiede politiche per la conservazione dei dati, la distruzione e la conformità legale e regolatoria delle operazioni digitali.

11.8 COBIT 2019:

11.8.1 DSS01 - Managed Operations: supporta il tracciamento della conservazione e la coerenza tra i sistemi di dati.

11.8.2 DSS05 - Managed Security Services: assicura la protezione dei dati memorizzati e archiviati fino allo smaltimento sicuro.

11.8.3 MEA03 - Monitor, Evaluate, and Assess Compliance: consente l'audit dell'applicazione dei periodi di conservazione, delle procedure di cancellazione e dell'adempimento normativo.