					Inserire qui la denominazione dell'entità giuridica registrata							
Numero del documento: P14S					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**

Nota legale (diritti d'autore e limitazioni d'uso)

(C) 2025 Clarysec LLC. All rights reserved.

Il presente documento è proprietà intellettuale di Clarysec LLC. Nessuna parte del presente documento può essere copiata, riutilizzata, distribuita o modificata per finalità commerciali o di implementazione senza previa autorizzazione scritta espressa.

L'uso non autorizzato è severamente vietato e può comportare azioni legali.

Per richieste di licenza, contattare: info@clarysec.com

Allineata a standard e regolamenti

Standard/Regolamento	Clausola/Articolo	Commento
ISO/IEC 27001:2022	Clausole 6.1.3, 8	Copre il trattamento del rischio, i controlli operativi e i requisiti di conservazione
ISO/IEC 27002:2022	Controllo 5	Fornisce linee guida sui periodi di conservazione e sui metodi di distruzione sicura
NIST SP 800-53 Rev.5	AU-11, MP-6, SI-12	Conservazione dei log di audit, sanitizzazione dei supporti, limiti di conservazione dei dati e relativa applicazione
Direttiva UE NIS2	Articolo 21(2)(a)	Richiede una politica di gestione del ciclo di vita proporzionata al rischio
Regolamento UE DORA	Articolo 5(1)	Gestione del rischio ICT: disponibilità e rimozione dei dati
COBIT 2019	BAI03.04, DSS01	Controlli sul ciclo di vita delle informazioni, smaltimento sicuro
Regolamento UE GDPR	Articolo 5(1)(e), 17	I dati non devono essere conservati più a lungo del necessario; diritto alla cancellazione

1. Finalità

1.1 La presente politica definisce le regole applicabili alla conservazione e allo smaltimento sicuro delle informazioni in un contesto di piccole e medie imprese (PMI). Garantisce che le registrazioni siano conservate solo per il periodo richiesto dalla legge, da obblighi contrattuali o da esigenze aziendali e che siano successivamente distrutte in modo sicuro.

1.2 La presente politica è volta a ridurre il rischio informativo, gestire l'esposizione legale e limitare la conservazione di dati ridondanti o obsoleti. Contribuisce a garantire la conformità alla ISO/IEC 27001 e ai quadri normativi in materia di protezione dei dati personali, quali il GDPR, minimizzando la conservazione non autorizzata di informazioni personali o dati sensibili.

1.3 Un quadro di conservazione e smaltimento ben strutturato riduce i costi operativi, migliora le prestazioni dei sistemi e aumenta la capacità di dimostrare la conformità. Per le PMI con capacità IT limitata, fornisce un approccio pratico per gestire responsabilmente gli asset informativi digitali e fisici.

2. Ambito di applicazione

2.1 La presente politica si applica a:

2.1.1 tutte le registrazioni, i file, i log, le comunicazioni e i set di dati creati, raccolti, trattati o archiviati dall'organizzazione

2.1.2 tutti i dipendenti, i collaboratori esterni e i fornitori che trattano dati dell'organizzazione

2.1.3 tutti i formati di dati (ad es. cartaceo, elettronico, immagine, audio o log) e tutti i supporti di memorizzazione (ad es. unità locali, servizi cloud, server di posta elettronica, backup)

2.2 L'ambito di applicazione comprende:

2.2.1 documenti aziendali (ad es. fatture, contratti, relazioni di progetto)

2.2.2 registrazioni operative (ad es. log, cronologia degli accessi, snapshot di backup)

2.2.3 dati personali (ad es. fascicoli HR, comunicazioni con i clienti, registrazioni di assistenza)

2.2.4 dati ospitati internamente, esternamente o in sistemi ibridi

2.2.5 dati archiviati e di backup, sia attivi sia inattivi

2.3 Rientrano nell'ambito di applicazione tutte le fasi del ciclo di vita dei dati, dalla creazione allo smaltimento autorizzato.

3. Obiettivi

3.1 Definire regole di conservazione coerenti sulla base di criteri legali, operativi e regolamentari.

3.2 Prevenire la cancellazione prematura di registrazioni critiche ed eliminare l'accumulo non necessario di dati.

3.3 Garantire lo smaltimento sicuro e irreversibile dei dati quando la conservazione non è più richiesta.

3.4 Assegnare chiaramente le responsabilità per l'attuazione delle decisioni di conservazione e cancellazione, tenendo conto dei vincoli di organico tipici delle PMI.

3.5 Fornire documentazione idonea a dimostrare la dovuta diligenza ai sensi della ISO 27001, del GDPR, della NIS2 e di altri quadri di riferimento.

3.6 Promuovere una gestione sicura del ciclo di vita dei dati senza imporre un onere tecnico non necessario al personale non specializzato.

4. Ruoli e responsabilità

4.1 Direttore generale (GM)

4.1.1 Approva la presente politica e ne assume la responsabilità.

4.1.2 Garantisce che le procedure di conservazione e smaltimento siano applicate in modo coerente con il rischio legale e aziendale.

4.1.3 Autorizza eccezioni e misure di conservazione legale e sospensione della cancellazione quando necessario.

4.1.4 Avvia i riesami della politica e approva gli aggiornamenti sulla base di cambiamenti aziendali o normativi.

4.2 Responsabile designato dei dati

4.2.1 È designato per ciascuna categoria di dati (ad es. dati finanziari, HR, registrazioni dei clienti).

4.2.2 Classifica le registrazioni e determina il periodo di conservazione appropriato sulla base della politica e delle indicazioni legali.

4.2.3 Autorizza la cancellazione quando i requisiti di conservazione sono stati soddisfatti.

4.2.4 Supporta gli audit interni fornendo il contesto relativo alla logica di conservazione e agli eventi di smaltimento.

[... 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 almeno una volta all'anno, oppure in caso di:

9.1.1 modifiche della normativa applicabile (ad es. protezione dei dati personali, rendicontazione finanziaria)

9.1.2 adozione di nuovi sistemi o processi che incidono sul ciclo di vita dei dati

9.1.3 risultanze dell'audit o incidenti che evidenzino lacune nelle pratiche di conservazione

9.2 I riesami devono garantire che il Registro di conservazione rimanga completo e rifletta tutte le principali categorie di registrazioni.

9.3 Gli aggiornamenti della politica devono essere approvati dal GM e comunicati al personale interessato. La versione più recente deve essere accessibile e soggetta a controllo delle versioni.

10. Politiche correlate e collegamenti

10.1 P2S – Politica sui ruoli e sulle responsabilità di governance: definisce la responsabilità della politica e l'autorità per le eccezioni.

10.2 P13S – Politica di classificazione ed etichettatura dei dati: determina come le regole di conservazione si allineano alla classificazione dei dati.

10.3 P12S – Politica di gestione degli asset: disciplina i supporti di memorizzazione che contengono dati soggetti a conservazione e smaltimento.

10.4 P17S – Politica di protezione dei dati e privacy: garantisce la minimizzazione dei dati e supporta il trattamento lecito delle informazioni ai sensi del GDPR.

10.5 P30S – Politica di risposta agli incidenti: è attivata quando carenze nello smaltimento o nella conservazione determinano una potenziale esposizione dei dati.

11. Standard e quadri di riferimento

11.1 ISO/IEC 27001

11.1.1 Clausola 6.1.3: richiede il trattamento dei rischi connessi alle informazioni, inclusi i rischi di conservazione.

11.1.2 Clausola 8.1: definisce i controlli operativi del ciclo di vita.

11.2 ISO/IEC 27002

11.2.1 Controllo 5.33: fornisce linee guida per definire i periodi di conservazione e i metodi di distruzione sicura.

11.3 NIST SP 800-53 Rev. 5

11.3.1 AU-11: richiede la conservazione dei log di audit.

11.3.2 MP-6: definisce le procedure di sanitizzazione dei supporti.

11.3.3 SI-12: tratta i limiti di conservazione dei dati e la relativa applicazione.

11.4 Regolamento UE GDPR

11.4.1 Articolo 5(1)(e): i dati non devono essere conservati più a lungo del necessario.

11.4.2 Articolo 17: il diritto alla cancellazione si applica quando i dati non sono più conservati lecitamente.

11.5 Direttiva UE NIS2

11.5.1 Articolo 21(2)(a): richiede politiche organizzative proporzionate al rischio, inclusa la gestione del ciclo di vita.

11.6 Regolamento UE DORA

11.6.1 Articolo 5(1): la gestione del rischio ICT include la disponibilità e la rimozione dei dati.

11.7 COBIT 2019

11.7.1 BAI03.04: richiede controlli sul ciclo di vita delle informazioni.

11.7.2 DSS01.06: richiede procedure di smaltimento sicuro come parte della protezione degli asset informativi.