					Inserire qui la denominazione dell'entità giuridica registrata							
Numero del documento: P18S					Titolo del documento: **Politica sui controlli crittografici**							
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	Clausola 8	
ISO/IEC 27002:2022	Controlli 8.24, 8.25	
NIST SP 800-53 Rev. 5	SC-12–SC-17	
Direttiva UE NIS2	Articoli 21(2)(d), 21(2)(e)	
Regolamento UE DORA	Articoli 6(2)(d), 9(2)(f)	
COBIT 2019	DSS05.01, APO13	
Regolamento generale sulla protezione dei dati (GDPR)	Articoli 32(1)(a), 34	

1. Finalità

1.1 La presente politica definisce i requisiti obbligatori per l'uso della cifratura e dei controlli crittografici al fine di proteggere la riservatezza, l'integrità e l'autenticità dei dati aziendali e dei dati personali.

1.2 Garantisce che gli strumenti crittografici siano utilizzati in modo appropriato su sistemi, dispositivi e servizi cloud nel contesto di una piccola impresa.

1.3 La presente politica supporta direttamente la certificazione ISO/IEC 27001:2022 e contribuisce a garantire la conformità agli obblighi di legge previsti dal Regolamento generale sulla protezione dei dati (GDPR), dalla Direttiva UE NIS2 e dal Regolamento sulla resilienza operativa digitale (DORA).

1.4 I controlli crittografici disciplinati includono la cifratura dei dati, la gestione dei certificati, la gestione sicura delle chiavi e i backup cifrati.

2. Ambito di applicazione

2.1 La presente politica si applica a:

2.1.1 tutti i dipendenti, i collaboratori esterni e le terze parti che trattano dati aziendali;

2.1.2 tutti i sistemi aziendali, gli endpoint e le piattaforme cloud utilizzati per archiviare, trasmettere o accedere a informazioni riservate;

2.1.3 tutti i dati personali, finanziari, legali o sensibili classificati ai sensi della politica di classificazione dei dati dell'organizzazione;

2.1.4 tutti i controlli crittografici, inclusi metodi di cifratura, chiavi, password, certificati e moduli di sicurezza.

2.2 La politica si applica ai dati a riposo, ai dati in transito e ai dati in uso. Disciplina inoltre la cifratura utilizzata per i backup, la posta elettronica, i trasferimenti esterni di dati e i siti web esposti pubblicamente.

3. Obiettivi

3.1 Garantire che i dati sensibili e regolamentati siano protetti in ogni momento mediante misure crittografiche adeguate.

3.2 Definire le responsabilità relative alla selezione degli strumenti di cifratura, alla configurazione e alla gestione delle chiavi.

3.3 Prevenire accessi non autorizzati, manomissioni o perdite di dati mediante l'applicazione di controlli sicuri per la trasmissione e l'archiviazione.

3.4 Garantire il rispetto dei requisiti legali e normativi che impongono la cifratura dei dati personali e aziendali.

3.5 Mantenere la sicurezza operativa e la disponibilità attraverso una gestione efficace dei certificati e delle chiavi crittografiche.

4. Ruoli e responsabilità

4.1 Direttore generale (GM)

4.1.1 Approva la presente politica e garantisce l'attuazione dei requisiti crittografici.

4.1.2 Riesamina le eccezioni, le notifiche di violazione e la conformità dei fornitori ai requisiti di cifratura.

4.1.3 Verifica che i servizi esternalizzati o cloud soddisfino gli standard di cifratura.

4.2 Fornitore di supporto IT / Amministratore IT interno

4.2.1 Implementa e mantiene le soluzioni di cifratura (ad es. cifratura completa del disco, certificati SSL/TLS, VPN).

4.2.2 Gestisce il ciclo di vita delle chiavi crittografiche e gli strumenti di archiviazione sicura.

4.2.3 Configura e monitora la cifratura a protezione di backup, siti web e dispositivi.

[... 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

9.1.1 La presente politica deve essere riesaminata almeno una volta all'anno dal Direttore generale, in coordinamento con il Fornitore di supporto IT e il Coordinatore privacy.

9.2 Attivatori del riesame intermedio

9.2.1 Il riesame deve essere effettuato anche nei seguenti casi:

9.2.1.1 modifica degli standard o dei protocolli crittografici (ad es. deprecazione di un algoritmo);

9.2.1.2 introduzione di nuovi sistemi o servizi cloud;

9.2.1.3 violazione o incidente che coinvolga una chiave o un certificato compromesso;

9.2.1.4 aggiornamenti legali o normativi che incidano sui requisiti di cifratura.

9.3 Controllo delle versioni e comunicazione

9.3.1 Tutte le modifiche alla politica devono essere documentate in un registro delle modifiche.

9.3.2 Il personale deve essere informato degli aggiornamenti e le versioni precedenti devono essere archiviate.

9.3.3 L'ultima versione approvata deve essere conservata nel repository centrale delle politiche.

10. Politiche correlate e collegamenti

10.1 La presente politica deve essere applicata congiuntamente alle seguenti politiche PMI:

10.1.1 P12S – Politica di gestione degli asset: garantisce che la cifratura sia applicata agli asset classificati durante l'archiviazione, il trasferimento e lo smaltimento.

10.1.2 P14S – Politica di conservazione e smaltimento dei dati: definisce i periodi di conservazione e richiede l'archiviazione cifrata dei dati fino alla loro cancellazione sicura.

10.1.3 P17S – Politica di protezione dei dati e privacy: allinea la cifratura ai principi di protezione dei dati e alle aspettative normative ai sensi dell'articolo 32 del GDPR.

10.1.4 P22S – Politica di registrazione e monitoraggio: richiede la registrazione dell'uso delle chiavi, dei guasti della cifratura e delle scadenze dei certificati ai fini di audit.

10.1.5 P30S – Politica di risposta agli incidenti: definisce le procedure di escalation, contenimento e notifica quando la cifratura non funziona o le chiavi sono compromesse.

11. Standard e quadri di riferimento

11.1 ISO/IEC 27001

11.1.1 Clausola 8.1 – Richiede l'implementazione di controlli operativi, inclusa la cifratura, per gestire i rischi di sicurezza.

11.2 ISO/IEC 27002

11.2.1 Controllo 8.24 – Descrive i requisiti per applicare la cifratura a tutela della riservatezza e dell'integrità.

11.2.2 Controllo 8.25 – Definisce la gestione sicura delle chiavi crittografiche e dei certificati.

11.3 NIST SP 800-53 Rev. 5

11.3.1 SC-12 – Stabilisce i requisiti per la definizione e la convalida delle chiavi crittografiche.

11.3.2 SC-13 – Definisce gli standard per la generazione delle chiavi crittografiche.

11.3.3 SC-17 – Copre l'infrastruttura a chiave pubblica (PKI) e la gestione del ciclo di vita dei certificati.

11.3.4 SC-28 – Richiede la cifratura dei dati a riposo.

11.3.5 Famiglia SC-12–SC-17 – Garantisce che le protezioni crittografiche siano correttamente implementate nei sistemi.

11.4 GDPR

11.4.1 Articolo 32(1)(a) – Richiede alle organizzazioni di implementare misure tecniche quali la cifratura per garantire la riservatezza dei dati.

11.4.2 Articolo 34 – Stabilisce che la cifratura può esentare le organizzazioni dagli obblighi di notifica di una violazione qualora i dati risultino incomprensibili a soggetti non autorizzati.

11.5 Direttiva UE NIS2

11.5.1 Articolo 21(2)(d) – Richiede una cifratura efficace per proteggere sistemi e comunicazioni.

11.5.2 Articolo 21(2)(e) – Sottolinea la protezione dei dati e la mitigazione delle minacce informatiche mediante cifratura.

11.6 Regolamento UE DORA

11.6.1 Articolo 6(2)(d) – Richiede che i sistemi ICT mantengano canali di comunicazione sicuri e cifrati.

11.6.2 Articolo 9(2)(f) – Impone ai soggetti finanziari di utilizzare una cifratura forte per proteggere le comunicazioni digitali e gli scambi di dati.

11.7 COBIT 2019

11.7.1 DSS05.01 – Richiede la protezione delle informazioni sensibili mediante cifratura e protocolli crittografici.

11.7.2 APO13.02 – Richiede l'implementazione efficace dei controlli di sicurezza, comprese le misure di protezione crittografiche, nell'ambito della pianificazione della sicurezza delle informazioni.