					Inserire qui la denominazione dell'entità giuridica registrata							
Numero del documento: P13					Titolo del documento: **Politica di classificazione ed etichettatura 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**

1. Finalità

1.1 La presente politica definisce il quadro di riferimento formale per la classificazione e l'etichettatura degli asset informativi dell'organizzazione in base alla sensibilità, all'esposizione al rischio e agli obblighi normativi.

1.2 Essa garantisce che tutte le informazioni, indipendentemente dal fatto che siano archiviate, trasmesse o trattate, siano chiaramente classificate ed etichettate in modo da comunicarne il livello di protezione e le modalità di gestione richieste.

1.3 La politica prescrive una classificazione strutturata, allineata alle prassi di gestione del rischio dell'organizzazione, a supporto degli obiettivi di riservatezza, integrità e disponibilità (CIA) dei dati, sia digitali sia fisici.

1.4 Questo controllo è essenziale per abilitare il controllo degli accessi basato sui ruoli, la dimostrabilità della conformità in sede di audit, la condivisione appropriata dei dati e l'efficace applicazione di misure di sicurezza tecniche quali cifratura, backup e monitoraggio.

2. Ambito di applicazione

2.1 La presente politica si applica a:

2.1.1 Tutti gli asset informativi dell'organizzazione, inclusi documenti, basi di dati, registrazioni e comunicazioni

2.1.2 Tutti i formati dei dati, inclusi quelli digitali, stampati, scritti o verbali

2.1.3 Tutti gli ambienti: on-premise, remoti, mobili e cloud

2.1.4 Tutti i dipendenti, i collaboratori esterni, i fornitori di servizi e i responsabili del trattamento di terze parti che creano, gestiscono o archiviano informazioni dell'organizzazione

2.2 L'ambito di applicazione comprende contenuti sviluppati internamente, dati acquisiti da fonti esterne, dati personali soggetti agli obblighi previsti dalla normativa privacy (ad es. GDPR) e informazioni scambiate con clienti, partner e autorità di regolamentazione.

2.3 Si applica a tutti i sistemi utilizzati per archiviare o trasmettere dati, incluse applicazioni aziendali, file server, sistemi di posta elettronica, piattaforme cloud e repository di backup.

3. Obiettivi

3.1 Definire uno schema di classificazione standardizzato a livello di organizzazione, basato sull'impatto dell'esposizione o della compromissione dei dati.

3.2 Garantire che tutte le informazioni siano etichettate in modo visibile e persistente, così da riflettere il relativo livello di classificazione e i requisiti di gestione.

3.3 Applicare misure di trattamento dei dati e controlli di accesso allineati alla classificazione, inclusi cifratura, logging di audit, protezione della trasmissione e pianificazione della conservazione.

3.4 Supportare la conformità agli standard internazionali (ISO/IEC 27001, 27002), ai quadri normativi (GDPR, NIS2, DORA) e alle politiche interne di gestione del rischio.

3.5 Garantire che tutti gli utenti comprendano le proprie responsabilità nella protezione dei dati, nell'applicazione delle etichette e nella corretta gestione delle informazioni classificate.

3.6 Mantenere la tracciabilità tra stato della classificazione, controlli associati e inventario degli asset dell'organizzazione ai fini di audit e conformità.

4. Ruoli e responsabilità

4.1 Responsabile della sicurezza delle informazioni (CISO)

4.1.1 È il titolare della politica di classificazione ed etichettatura delle informazioni e ne garantisce l'allineamento ai requisiti normativi, contrattuali e operativi.

4.1.2 Approva i livelli di classificazione, gli standard di etichettatura e le modifiche alla politica.

4.1.3 Sovrintende alla conformità alla politica mediante audit, metriche e riesame delle eccezioni.

4.1.4 Coordina la governance interfunzionale con la funzione legale e compliance, la funzione privacy e i team di rischio.

4.2 Titolari delle informazioni

4.2.1 Sono responsabili della classificazione degli asset informativi sotto il proprio controllo utilizzando lo schema di classificazione dell'organizzazione.

4.2.2 Applicano le etichette di classificazione al momento della creazione, dell'aggiornamento o dell'acquisizione.

4.2.3 Riesaminano periodicamente la classificazione degli asset, in particolare a seguito di variazioni della sensibilità, dell'ambito normativo o del valore aziendale.

4.2.4 Garantiscono che i dati sensibili siano gestiti ed etichettati in modo appropriato durante tutto il loro ciclo di vita.

[... 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 annualmente per garantirne l'allineamento con:

9.1.1 L'evoluzione dei requisiti normativi (ad es. GDPR, NIS2, DORA)

9.1.2 Gli aggiornamenti alle linee guida di classificazione ISO/IEC 27001 o 27002

9.1.3 I cambiamenti organizzativi che incidono sulla sensibilità dei dati o sulla titolarità

9.1.4 I cambiamenti tecnologici, incluse nuove piattaforme di gestione documentale o dei dati

9.2 Il Responsabile della sicurezza delle informazioni (CISO) deve avviare il riesame in collaborazione con il Comitato per la sicurezza delle informazioni, la funzione legale e le unità aziendali interessate.

9.3 I riesami devono includere:

9.3.1 L'efficacia dell'applicazione della classificazione e la conformità degli utenti

9.3.2 L'analisi di incidenti o eccezioni connessi a errori di classificazione

9.3.3 Il feedback degli utenti sugli strumenti di etichettatura o sui materiali di indirizzo

9.3.4 Benchmarking rispetto agli standard di classificazione di settore

9.4 Gli aggiornamenti della politica devono essere soggetti a controllo di versione, documentati nel repository documentale del SGSI e comunicati a tutto il personale interessato, con particolare attenzione a nuove responsabilità o modifiche degli strumenti.

9.5 I nuovi assunti devono essere informati della versione corrente della politica durante l'onboarding. Tutti i dipendenti devono completare la formazione di aggiornamento a seguito di modifiche significative della politica.

10. Politiche correlate e collegamenti

10.1 La presente politica è direttamente supportata da, e dà attuazione ai controlli descritti nelle seguenti politiche correlate:

10.1.1 P4 - Politica di controllo degli accessi: l'accesso alle informazioni è regolato dai livelli di classificazione; i dati più sensibili richiedono controlli di accesso e meccanismi di autorizzazione più rigorosi.

10.1.2 P11 - Politica di gestione degli account utente e dei privilegi: rafforza l'assegnazione dei privilegi in base al principio del need-to-know, determinato dai livelli di classificazione.

10.1.3 P12 - Politica di gestione degli asset: garantisce che ogni asset nell'inventario includa classificazione ed etichetta, a supporto di tracciabilità e responsabilità.

10.1.4 P14 - Politica di conservazione e smaltimento dei dati: le regole di conservazione e smaltimento sono determinate dal livello di classificazione dei dati e dagli obblighi normativi di conservazione.

10.1.5 P18 - Politica sui controlli crittografici: applica standard di cifratura appropriati in base alla classificazione dell'asset informativo.

10.1.6 P22 - Politica di registrazione e monitoraggio: consente il monitoraggio dell'accesso alle informazioni classificate e del loro trasferimento, assicurando verificabilità e rilevazione di errori di etichettatura o uso improprio.

10.2 Ciascun collegamento garantisce una protezione coerente delle informazioni lungo tutto il loro ciclo di vita, dalla creazione e classificazione fino alla gestione sicura, all'archiviazione, alla trasmissione e alla distruzione finale.

11. Standard e quadri di riferimento

11.1 La presente politica è allineata a standard riconosciuti a livello internazionale e a quadri normativi che disciplinano la classificazione e l'etichettatura delle informazioni sensibili.

11.2 ISO/IEC 27001

11.2.1 Clausola 4.2 - Comprendere le esigenze e le aspettative delle parti interessate. I requisiti di classificazione derivano spesso da obblighi legali, normativi o contrattuali imposti dalle parti interessate (ad es. GDPR, accordi di riservatezza con i clienti), che devono essere recepiti nella politica.

11.2.2 Clausola 6.1.3 - Trattamento dei rischi per la sicurezza delle informazioni. La classificazione incide direttamente sulla selezione dei controlli di trattamento del rischio, inclusi controllo degli accessi, cifratura e conservazione, in base alla sensibilità dei dati.

11.2.3 Clausola 7.2 - Competenza. La politica richiede che il personale responsabile della classificazione e dell'etichettatura riceva una formazione adeguata, in linea con i requisiti di competenza.

11.2.4 Clausola 7.3 - Consapevolezza. La politica richiede che tutti gli utenti siano consapevoli dei livelli di classificazione e delle proprie responsabilità nella gestione delle informazioni, in allineamento con gli obblighi di sensibilizzazione.

11.2.5 Clausola 7.5 - Informazioni documentate. La politica di classificazione stessa è un documento controllato e le procedure, le registrazioni della formazione e le etichette di classificazione fanno parte delle informazioni documentate.

11.2.6 Clausola 8.1 - Pianificazione e controllo operativi. La classificazione e l'etichettatura sono processi operativi integrati nella gestione del ciclo di vita dei dati e questa clausola garantisce che tali attività siano pianificate, attuate e controllate.

11.2.7 Clausola 9.1 - Monitoraggio, misurazione, analisi e valutazione. La politica include disposizioni per monitorare la conformità della classificazione, le tendenze degli incidenti e l'efficacia dello schema di etichettatura.

11.2.8 Clausola 10.1 - Non conformità e azione correttiva. La politica definisce le risposte agli errori di classificazione, incluse azioni correttive quali formazione aggiuntiva, aggiornamenti e gestione delle eccezioni.

11.3 ISO/IEC 27002:2022

11.3.1 Controllo 5.12 - Classificazione delle informazioni. Questo controllo garantisce che le informazioni siano classificate in base a sensibilità, valore e criticità, come formalizzato dalla presente politica.

11.3.2 Controllo 5.13 - Etichettatura delle informazioni. Questo controllo richiede un'etichettatura appropriata delle informazioni in conformità al relativo livello di classificazione, aspetto pienamente disciplinato dalla politica.

11.3.3 Controllo 5.10 - Uso accettabile delle informazioni e degli altri asset associati. La politica definisce le modalità con cui gli utenti devono gestire i dati classificati, supportando direttamente l'uso accettabile e prevenendo usi impropri.

11.3.4 Controllo 5.11 - Restituzione degli asset. La classificazione contribuisce a garantire che i dati sensibili siano identificati e restituiti o sanitizzati in modo sicuro quando un dipendente o un fornitore cessa il rapporto.

11.3.5 Controllo 5.9 - Inventario degli asset informativi e degli altri asset associati. La classificazione è spesso collegata all'inventario degli asset, che deve riflettere il livello di classificazione di ciascun elemento per supportare la corretta assegnazione dei controlli.

11.3.6 Controllo 5.14 - Trasferimento delle informazioni. I livelli di classificazione influenzano i controlli sui trasferimenti di dati interni ed esterni (ad es. cifratura, approvazione, restrizioni di accesso).

11.3.7 Controllo 8.12 - Prevenzione della perdita di dati. L'applicazione della classificazione e dell'etichettatura supporta la prevenzione della divulgazione non autorizzata e della perdita di dati.

11.3.8 Controllo 8.11 - Mascheramento dei dati. Determinati livelli di classificazione (ad es. Riservato, Strettamente riservato) possono imporre il mascheramento quando i dati sono utilizzati in ambienti di test/sviluppo o nei sistemi di analisi.

11.4 NIST SP 800-53 Rev.5

11.4.1 PL-2 - Politica e procedure di protezione del sistema e delle comunicazioni: supporta le politiche di classificazione nell'ambito della protezione complessiva dei dati.

11.4.2 AC-16 - Attributi di sicurezza: applica il controllo degli accessi sulla base dei metadati di classificazione e delle autorizzazioni utente.

11.4.3 MP-3 / MP-5 - Marcatura dei supporti e protezione durante il trasporto: impone l'etichettatura e la protezione dei dati a riposo e in transito in base alla classificazione.

11.5 GDPR UE (2016/679)

11.5.1 Articolo 5 - Principi applicabili al trattamento dei dati: richiede che i dati personali siano trattati in modo sicuro e proporzionato alla loro sensibilità.

11.5.2 Articolo 32 - Sicurezza del trattamento: rafforza la classificazione come meccanismo per la protezione dei dati basata sul rischio e per l'adozione di misure tecniche appropriate.

11.6 Direttiva NIS2 UE (2022/2555)

11.6.1 Articolo 21(2)(a): richiede politiche per la gestione dei rischi per la sicurezza delle informazioni, inclusi controlli sulla classificazione degli asset e dei dati.

11.6.2 Articolo 21(3): promuove l'adozione di misure per applicare una gestione appropriata dei dati, supportata dall'etichettatura basata sulla classificazione.

11.7 DORA UE (2022/2554)

11.7.1 Articolo 5 - Governance e controllo: richiede quadri di governance che classifichino gli asset di dati ai fini del controllo del rischio ICT.

11.7.2 Articolo 9 - Gestione del rischio ICT: impone misure tecniche e organizzative per gli asset ICT critici, incluse classificazione ed etichettatura.

11.8 COBIT 2019

11.8.1 DSS05.02 - Gestire i servizi di sicurezza: applica classificazioni di sicurezza delle informazioni per garantire la protezione dei dati aziendali.

11.8.2 MEA03 - Monitor, Evaluate, and Assess Compliance: supporta audit e riesami regolari delle pratiche di classificazione per garantire conformità alla politica e maturità.