					Inserire qui la denominazione dell'entità giuridica registrata							
Numero del documento: P13S					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**

Allineamento a standard e normative

Standard/Regolamento	Clausola/Articolo	Commento
ISO/IEC 27001:2022	Clausole 5.3, 8	
ISO/IEC 27002:2022	Controlli 5.12, 5	
NIST SP 800-53 Rev.5	AC-16, MP-3, MP-5	
Direttiva UE NIS2	Articolo 21(2)(a)	
Regolamento UE DORA	Articolo 5(8)	
COBIT 2019	BAI03.05, DSS05	
Regolamento UE GDPR	Articolo 5, 32	

1. Finalità

1.1 La presente politica definisce le modalità con cui tutte le informazioni trattate dall'organizzazione devono essere classificate ed etichettate al fine di garantirne la riservatezza, l'integrità e la disponibilità (CIA) durante l'intero ciclo di vita.

1.2 Essa consente una gestione coerente dei dati, assegnando alle informazioni livelli di protezione adeguati in funzione della sensibilità, dell'impatto sul business o degli obblighi di conformità.

1.3 La classificazione e l'etichettatura contribuiscono a ridurre il rischio di divulgazione accidentale, accesso non autorizzato o trattamento improprio di dati sensibili, in particolare nelle piccole e medie imprese (PMI), che possono fare affidamento su sistemi più semplici e su controlli meno formalizzati.

1.4 La presente politica è essenziale ai fini della certificazione ISO/IEC 27001 e della conformità normativa, in particolare rispetto a normative in materia di protezione dei dati quali il GDPR e a quadri di riferimento per la cibersicurezza quali NIS2 e DORA.

2. Ambito di applicazione

2.1 La presente politica si applica a tutti i dati dell'organizzazione, indipendentemente dal formato o dall'ubicazione, inclusi:

2.1.1 Documenti elettronici, fogli di calcolo, e-mail, moduli, immagini e file acquisiti tramite scansione

2.1.2 Documenti fisici quali registrazioni cartacee, report, fatture e note

2.1.3 Dati archiviati o trattati in servizi cloud, su server locali, supporti portatili o dispositivi personali utilizzati per finalità lavorative

2.1.4 Dati temporanei o transitori generati nel corso delle operazioni aziendali (ad es. log, file di cache, e-mail)

2.2 Tutto il personale, i collaboratori esterni, i lavoratori temporanei e i fornitori terzi con accesso ai dati dell'organizzazione sono tenuti a rispettare la presente politica.

2.3 La presente politica si applica all'intero ciclo di vita dei dati: dalla creazione e archiviazione, passando per l'accesso e il trasferimento, fino alla conservazione a lungo termine o alla cancellazione.

3. Obiettivi

3.1 Definire uno schema di classificazione semplice e applicabile, facilmente comprensibile e utilizzabile in tutta l'organizzazione.

3.2 Richiedere che ogni asset informativo sia classificato in base alla propria sensibilità e opportunamente etichettato per orientarne la corretta gestione, archiviazione e accesso.

3.3 Garantire che le prassi di etichettatura dei dati siano integrate nei processi aziendali, quali onboarding, avvio di progetto e configurazione dei sistemi.

3.4 Ridurre il rischio di violazione dei dati applicando controlli di protezione appropriati al livello di classificazione (ad es. cifratura, restrizione degli accessi).

3.5 Garantire la conformità alle normative in materia di privacy e sicurezza delle informazioni, dimostrando che i dati sensibili (ad es. dati personali, finanziari o proprietari) sono correttamente etichettati e gestiti.

3.6 Stabilire la responsabilità per le decisioni di classificazione e garantire riesami e aggiornamenti periodici sulla base dell'evoluzione delle esigenze aziendali e degli obblighi normativi.

4. Ruoli e responsabilità

4.1 Direttore Generale (GM)

4.1.1 È il titolare della politica e approva lo schema di classificazione.

4.1.2 Esercita la supervisione necessaria a garantire che le responsabilità di classificazione siano assegnate e applicate.

4.1.3 Riesamina e autorizza eventuali eccezioni ai requisiti di classificazione o etichettatura.

4.1.4 Garantisce che le prassi di gestione dei dati soddisfino gli obblighi di conformità previsti da normative quali GDPR e DORA.

4.2 Titolare delle informazioni / Responsabile dei dati

4.2.1 Assegna una classificazione iniziale a ogni nuovo insieme di dati o asset informativo al momento della creazione o acquisizione.

4.2.2 Garantisce l'apposizione di etichette visibili, ove applicabile (ad es. intestazioni, piè di pagina, filigrane, nomi delle cartelle).

4.2.3 Riesamina periodicamente le classificazioni per verificarne pertinenza, accuratezza ed eventuali modifiche necessarie (ad es. a seguito di declassificazione o pubblicazione).

4.2.4 Collabora con il responsabile IT per applicare misure di protezione tecniche basate sulla classificazione (ad es. diritti di accesso, cifratura).

[... 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 dal GM e dal Responsabile dei dati per garantire che rifletta:

9.1.1 cambiamenti nelle operazioni aziendali o nelle tipologie di dati

9.1.2 nuovi requisiti normativi (ad es. in materia di protezione dei dati o vigilanza finanziaria)

9.1.3 evoluzioni tecnologiche che incidono sulle capacità di etichettatura o classificazione

9.2 Il riesame deve includere aggiornamenti alle categorie di classificazione, agli strumenti o alle prassi di etichettatura e ai contenuti di sensibilizzazione e formazione.

9.3 Le revisioni della politica devono essere approvate dal GM e comunicate a tutto il personale. Deve essere conservata una registrazione delle modifiche di versione ai fini di audit.

10. Politiche correlate e collegamenti

10.1 P2S – Politica su ruoli e responsabilità di governance: assegna la responsabilità per la titolarità e l'attuazione della politica.

10.2 P4S – Politica di controllo degli accessi: allinea l'accesso ai sistemi ai livelli di classificazione dei dati.

10.3 P12S – Politica di gestione degli asset: consente il tracciamento dei beni fisici e digitali che archiviano dati classificati.

10.4 P17S – Politica di protezione dei dati e privacy: disciplina la protezione dei dati personali, molti dei quali sono classificati come "Riservato".

10.5 P30S – Politica di risposta agli incidenti: definisce i percorsi di escalation e le procedure di risposta in caso di violazioni della classificazione o esposizione dei dati.

11. Standard e quadri di riferimento

11.1 ISO/IEC 27001

11.1.1 Clausola 5.3: richiede responsabilità chiaramente definite per la gestione e la protezione dei dati.

11.1.2 Clausola 8.1: richiede pianificazione e controlli operativi, inclusi quelli collegati alla classificazione dei dati.

11.2 ISO/IEC 27002

11.2.1 Controllo 5.12: fornisce indicazioni sulla classificazione delle informazioni in base al rischio e ai requisiti normativi.

11.2.2 Controllo 5.13: definisce i meccanismi pratici di etichettatura e le relative regole di gestione.

11.3 NIST SP 800-53 Rev.5

11.3.1 AC-16: richiede la marcatura delle informazioni per garantire che le misure di protezione siano allineate alla classificazione.

11.3.2 MP-3 / MP-5: forniscono indicazioni sull'etichettatura e sul controllo dei supporti e degli output.

11.4 Regolamento UE GDPR

11.4.1 Articoli 5 e 32: impongono la minimizzazione dei dati e la tutela dell'integrità mediante classificazione appropriata e misure di sicurezza per la gestione.

11.5 Direttiva UE NIS2

11.5.1 Articolo 21(2)(a): impone controlli tecnici e organizzativi per la protezione dei dati basata sul rischio.

11.6 Regolamento UE DORA

11.6.1 Articolo 5(8): richiede alle organizzazioni di classificare gli asset di dati come parte del proprio programma di gestione del rischio ICT.

11.7 COBIT 2019

11.7.1 BAI03.05: richiede la classificazione delle informazioni e una protezione adeguata al rischio.

11.7.2 DSS05.02: riguarda l'applicazione di controlli basati sulla classificazione e il monitoraggio.