					Inserire qui la denominazione dell'entità giuridica registrata							
Numero del documento: P12					Titolo del documento: **Politica di gestione degli asset**							
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 i requisiti organizzativi obbligatori per identificare, classificare, gestire e proteggere gli asset informativi lungo il loro ciclo di vita. Supporta la governance aziendale degli asset hardware, software, dati, cloud e degli asset informativi immateriali, inclusi gli ambienti mobili, remoti e gestiti da terze parti.

1.2 La finalità della presente politica è garantire piena visibilità sul parco degli asset informativi dell'organizzazione, consentendo l'applicazione efficace dei controlli di sicurezza, l'assegnazione delle responsabilità di proprietà, l'allineamento agli obblighi di conformità e il corretto ritiro o smaltimento degli asset.

1.3 La politica è allineata al controllo A.5.9 della ISO/IEC 27001:2022 e richiede il mantenimento di un inventario centralizzato delle informazioni e degli asset associati. Garantisce la responsabilizzazione associando ciascun asset a un proprietario e applicando misure di protezione determinate dalla classificazione, in base alla sensibilità aziendale e ai requisiti normativi.

2. Ambito di applicazione

2.1 La presente politica si applica a tutti i dipendenti, collaboratori esterni, fornitori terzi e prestatori di servizi che gestiscono, utilizzano, accedono, archiviano o trattano asset informativi di proprietà dell'organizzazione o da essa controllati.

2.2 L'ambito di applicazione include tutte le categorie di asset, quali:

2.2.1 Beni fisici: laptop, desktop, dispositivi mobili, supporti rimovibili, stampanti, apparati di rete

2.2.2 Asset digitali: software, applicazioni, immagini di sistema, basi di dati, dati di backup, chiavi crittografiche

2.2.3 Asset informativi: dati strutturati e non strutturati, report, e-mail, proprietà intellettuale

2.2.4 Asset cloud e virtuali: ambienti IaaS, SaaS e PaaS, macchine virtuali, container

2.2.5 Asset logici: nomi di dominio, licenze, account utente, configurazioni baseline

2.3 La politica disciplina inoltre gli asset utilizzati in ambienti di lavoro remoti, ibridi o esternalizzati, garantendo protezione e visibilità anche quando gli asset non sono fisicamente ubicati presso le sedi dell'organizzazione.

3. Obiettivi

3.1 Mantenere un inventario completo, accurato e aggiornato di tutti gli asset informativi dell'organizzazione, con attributi definiti di proprietà, classificazione e ubicazione.

3.2 Assegnare Proprietari degli asset responsabili della classificazione, della gestione e della protezione degli asset sotto il loro controllo, in conformità alle politiche di governance dei dati e di sicurezza.

3.3 Applicare classificazione ed etichettatura appropriate a tutti gli asset sulla base di sensibilità, criticità e considerazioni normative.

3.4 Proteggere gli asset in funzione della loro classificazione e della relativa esposizione al rischio, inclusi archiviazione, accesso, trasmissione e smaltimento.

3.5 Applicare procedure di restituzione degli asset e di smaltimento sicuro durante l'offboarding del personale, la cessazione del contratto o la conclusione del ciclo di vita dell'asset.

3.6 Supportare la conformità normativa rispetto a quadri di riferimento quali ISO/IEC 27001, GDPR, NIS2, DORA e COBIT 2019 tramite una gestione strutturata degli asset e la relativa verificabilità.

4. Ruoli e responsabilità

4.1 Direzione aziendale

4.1.1 Approva la Politica di gestione degli asset e assicura l'assegnazione delle risorse necessarie alla sua piena attuazione.

4.1.2 Mantiene la responsabilità ultima di garantire che gli asset dell'organizzazione siano protetti e gestiti in conformità agli obblighi normativi e contrattuali.

4.2 Responsabile della sicurezza delle informazioni (CISO)

4.2.1 È il proprietario della Politica di gestione degli asset e ne garantisce l'integrazione con il Sistema di gestione della sicurezza delle informazioni (SGSI) dell'organizzazione.

4.2.2 Riesamina le eccezioni e gli scostamenti rispetto alla presente politica e impone strategie di mitigazione basate sul rischio.

4.2.3 Supervisiona audit periodici sulla classificazione degli asset, sull'integrità dell'inventario degli asset e sulla conformità del ciclo di vita degli asset.

[... 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 oppure in risposta a:

9.1.1 Modifiche degli obblighi di legge o normativi che incidono sulla classificazione degli asset o sui requisiti di inventario

9.1.2 Introduzione di nuove categorie di asset o piattaforme di gestione (ad esempio CMDB cloud-native)

9.1.3 Risultanze dell'audit interno o incidenti di sicurezza che coinvolgono una gestione inadeguata degli asset

9.1.4 Riorganizzazioni aziendali che incidono sulla proprietà o sui controlli del ciclo di vita

9.2 Il processo di riesame deve essere avviato dal Responsabile IT Asset e coordinato con il CISO, Approvvigionamenti, Funzione Legale e Compliance e i responsabili delle funzioni interessate.

9.3 Riesami intermedi possono inoltre essere attivati da:

9.3.1 Acquisizione o cessione di unità aziendali

9.3.2 Cambiamenti dei fornitori che incidono sugli asset gestiti da terze parti

9.3.3 Rinnovi tecnologici che comportano dismissioni o provisioning in blocco

9.4 Tutte le revisioni della presente politica devono:

9.4.1 Essere soggette a controllo delle versioni e archiviate nel repository del SGSI

9.4.2 Essere approvate dalla Direzione aziendale

9.4.3 Includere una sintesi delle modifiche e la relativa motivazione

9.4.4 Essere comunicate a tutte le parti interessate coinvolte, comprese procedure aggiornate o formazione sui sistemi, ove applicabile

10. Politiche correlate e collegamenti

10.1 La presente politica opera congiuntamente alle seguenti politiche correlate e ne supporta l'applicazione:

10.1.1 P4 - Politica di controllo degli accessi: garantisce che la visibilità degli asset sia allineata ai diritti di accesso e ai meccanismi di controllo nei sistemi e negli ambienti dati.

10.1.2 P7 - Politica di onboarding e cessazione del personale: disciplina il provisioning tempestivo e la restituzione dei beni fisici e degli asset logici durante le transizioni del personale.

10.1.3 P13 - Politica di classificazione ed etichettatura dei dati: stabilisce le regole di classificazione obbligatorie per gli asset, che determinano etichettatura, gestione e procedure di smaltimento.

10.1.4 P14 - Politica di conservazione e smaltimento dei dati: definisce tempistiche e metodi di smaltimento sicuro per gli asset digitali e fisici contenenti informazioni.

10.1.5 P22 - Politica di registrazione e monitoraggio: consente la tracciabilità dell'accesso e dell'utilizzo degli asset tramite registrazione di sistema, visibilità degli endpoint e analisi comportamentale.

10.1.6 P30 - Politica di risposta agli incidenti: supporta il rapido contenimento e l'indagine delle violazioni correlate agli asset, come laptop smarriti o supporti di memorizzazione non tracciati.

10.2 Tali politiche costituiscono un quadro di governance coerente che garantisce che gli asset siano gestiti in modo sicuro, inventariati accuratamente e trattati in modo appropriato lungo il loro ciclo di vita.

11. Standard e quadri di riferimento

11.1 La presente politica è allineata a standard internazionalmente riconosciuti in materia di sicurezza delle informazioni e a quadri normativi che richiedono una solida gestione degli asset lungo il relativo ciclo di vita.

11.2 ISO/IEC 27001:

11.2.1 Clausola 8.1 - Richiede alle organizzazioni di pianificare, attuare e controllare i processi necessari per soddisfare i requisiti di sicurezza delle informazioni, inclusi quelli relativi alla gestione del ciclo di vita degli asset.

11.3 ISO/IEC 27002:2022 - Controlli 5.9 to 5.

11.3.1 Clausola 5.9 - Inventario degli asset informativi e degli altri asset associati: richiede un inventario aggiornato e completo di tutti gli asset rilevanti per il trattamento delle informazioni.

11.3.2 Clausola 5.10 - Uso accettabile delle informazioni e degli asset: supportato da regole di utilizzo, proprietà e processi di restituzione.

11.3.3 Clausola 5.11 - Restituzione degli asset: attuata tramite procedure formali di consegna e dismissione.

11.3.4 Tali controlli stabiliscono requisiti strutturati per identificare, etichettare, mantenere e tracciare gli asset dell'organizzazione, con corrispondenti responsabilità per proprietari e custodi lungo l'intero ciclo di vita.

11.4 NIST SP 800-53 Rev.5:

11.4.1 CM-8 - Inventario dei componenti del sistema: rispecchiato tramite gestione centralizzata degli asset, visibilità in tempo reale e collegamento alle configurazioni operative.

11.4.2 RA-3 - Valutazione del rischio: gli inventari degli asset costituiscono elementi fondamentali per la modellazione delle minacce e la valutazione del rischio.

11.4.3 MP-6 - Sanitizzazione dei supporti: applicata tramite metodi di smaltimento sicuro definiti nei controlli sul ciclo di vita degli asset e nella politica di smaltimento dei dati.

11.5 GDPR UE (2016/679):

11.5.1 Articolo 30 - Registri delle attività di trattamento: richiede alle organizzazioni di documentare sistemi, dispositivi e repository che archiviano o trattano dati personali.

11.5.2 Articolo 32 - Sicurezza del trattamento: è allineato alla valutazione del rischio basata sugli asset e a misure di sicurezza commisurate agli asset classificati e alle infrastrutture critiche.

11.6 Direttiva UE NIS2 (2022/2555):

11.6.1 Articolo 21(2)(a, b): impone visibilità e inventario degli asset quali elementi fondamentali per l'analisi del rischio, la protezione e la risposta agli incidenti di cibersicurezza.

11.6.2 Articolo 21(3): rafforza la necessità di una governance strutturata degli asset come parte della cultura della sicurezza dell'organizzazione.

11.7 DORA UE (2022/2554):

11.7.1 Articolo 5 - Governance ICT e controllo interno: richiede agli enti finanziari di controllare gli asset ICT con requisiti chiari in materia di inventario, proprietà e protezione.

11.7.2 Articolo 9 - Quadro di gestione del rischio ICT: stabilisce che i processi di gestione degli asset devono supportare la mitigazione delle minacce, la pianificazione della continuità operativa e la resilienza dei servizi.

11.8 COBIT 2019:

11.8.1 BAI09 - Gestire gli asset: direttamente allineato all'identificazione strutturata, alla classificazione, all'utilizzo e allo smaltimento dei beni aziendali.

11.8.2 DSS01 - Managed Operations: supporta l'applicazione di controlli che garantiscono la protezione degli asset e una governance operativa continua.

11.8.3 MEA03 - Monitor, Evaluate, and Assess Compliance: garantisce audit regolari dei controlli di gestione degli asset e della loro efficacia ai fini dell'allineamento normativo.