					Inserire qui la denominazione dell'entità giuridica registrata							
Numero del documento: P12S					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**

Allineamento a standard e regolamenti

Standard/Regolamento	Clausola/Articolo	Commento
ISO/IEC 27001:2022	Clausola 8	Requisiti per la gestione degli asset
ISO/IEC 27002:2022	Controllo 5	Controlli per la gestione degli asset
NIST SP 800-53 Rev.5	CM-8	Inventario degli asset dei componenti di sistema
Direttiva UE NIS2	Articolo 21(2)(a)	Tracciamento degli asset per la protezione dei sistemi di rete e informativi
Regolamento UE DORA	Articolo 5(8)	Requisiti relativi all'inventario degli asset ICT
COBIT 2019	BAI	Gestione del ciclo di vita degli asset IT
Regolamento UE GDPR	Articolo 30	Inventario delle attività di trattamento dei dati

1. Finalità

1.1 La presente politica definisce le modalità con cui l'organizzazione identifica, traccia, protegge e dismette i propri asset informativi, inclusi i componenti fisici e digitali.

1.2 L'obiettivo è ridurre i rischi operativi e di sicurezza, mantenendo visibilità, responsabilità e gestione sicura di tutti gli asset aziendali lungo l'intero ciclo di vita.

1.3 Un inventario degli asset affidabile supporta la conformità normativa, la risposta agli incidenti, la pianificazione della continuità operativa e la gestione del rischio.

1.4 La presente politica supporta inoltre la certificazione ISO/IEC 27001 e dimostra l'allineamento agli obblighi legali, finanziari e di cybersicurezza previsti da quadri di riferimento quali GDPR, NIS2 e DORA.

1.5 Per le piccole e medie imprese (PMI), un approccio semplice ma sistematico alla gestione degli asset è essenziale per prevenire dispositivi non gestiti, perdita di dati o esiti negativi in sede di audit, soprattutto in presenza di risorse tecniche limitate.

2. Ambito di applicazione

2.1 La presente politica si applica a tutti gli asset di proprietà, in leasing o comunque gestiti dall'organizzazione, inclusi quelli utilizzati in:

2.1.1 attività d'ufficio

2.1.2 modalità di lavoro da remoto o ibride

2.1.3 operazioni sul campo o in mobilità

2.1.4 ambienti cloud e in outsourcing

2.2 Le tipologie di asset coperte includono, a titolo esemplificativo e non esaustivo:

2.2.1 Hardware: laptop, desktop, monitor, telefoni, tablet, unità USB, router, stampanti, supporti di backup

2.2.2 Software: applicazioni installate, servizi SaaS, sistemi operativi, strumenti antivirus, licenze

2.2.3 Asset informativi: repository di dati aziendali, fogli di calcolo, registrazioni clienti, codice sorgente

2.2.4 Credenziali e servizi digitali: nomi di dominio, certificati digitali, chiavi API, account e-mail, credenziali di accesso al cloud

2.2.5 Dispositivi di accesso: chiavi, smart card, badge di accesso, token biometrici

2.3 Rientrano nell'ambito di applicazione della presente politica tutti i dipendenti, i collaboratori esterni e i fornitori terzi che trattano asset dell'organizzazione.

2.4 La politica disciplina inoltre sia gli asset a breve termine (ad esempio laptop dedicati a specifici progetti) sia quelli a lungo termine, nonché gli asset condivisi utilizzati da più membri del personale.

3. Obiettivi

3.1 Istituire e mantenere un inventario degli asset completo e accurato di tutti gli asset rilevanti, aggiornato con continuità.

3.2 Assicurare che ciascun asset abbia un proprietario dell'asset designato, responsabile del suo utilizzo, della sua custodia e della sua restituzione.

3.3 Classificare gli asset in base a sensibilità, impatto aziendale o rilevanza normativa, così da consentire livelli di protezione differenziati.

3.4 Definire procedure chiare per l'assegnazione, la riassegnazione, la manutenzione, la segnalazione di smarrimento e la dismissione degli asset.

3.5 Assicurare che gli asset siano gestiti in modo sicuro lungo il loro ciclo di vita e che le informazioni in essi memorizzate siano protette oppure cancellate in modo sicuro al momento dello smaltimento.

3.6 Ridurre la probabilità di incidenti di sicurezza causati da asset dell'organizzazione non tracciati, non restituiti o utilizzati in modo improprio.

3.7 Supportare la conformità alle leggi applicabili (ad esempio il principio di accountability del GDPR) e agli standard di certificazione in materia di cybersicurezza.

4. Ruoli e responsabilità

4.1 Direttore generale (GM)

4.1.1 È il titolare della politica ed è responsabile di assicurare che le pratiche di gestione degli asset siano applicate e rispettate in tutta l'organizzazione.

4.1.2 Riesamina e approva gli aggiornamenti dell'inventario degli asset e autorizza, ove necessario, la dismissione o il trasferimento degli asset.

4.1.3 Deve essere informato di qualsiasi perdita, furto o uso improprio significativo degli asset.

4.2 Responsabile IT o referente designato per la gestione degli asset

4.2.1 Mantiene l'inventario degli asset (ad esempio in un foglio di calcolo, in un sistema di ticketing o in uno strumento leggero di tracciamento degli asset).

4.2.2 Assegna la titolarità degli asset e ne traccia le variazioni di stato (ad esempio nuovo, in uso, in riparazione, dismesso).

4.2.3 Verifica che tutti gli asset assegnati siano documentati e associati a una persona o a un'unità aziendale.

4.2.4 Assicura che le etichette di classificazione siano applicate e rispettate (ad esempio Interno, Riservato).

4.2.5 Coordina il recupero, la sanitizzazione e la disattivazione degli asset durante l'offboarding o la dismissione.

4.2.6 Segnala al GM eventuali discrepanze sugli asset non risolte.

[... 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 l'anno e ogniqualvolta:

9.1.1 vengano introdotte nuove tipologie di tecnologie o asset

9.1.2 cambino le procedure di tracciamento degli asset (ad esempio tramite l'adozione di nuovi strumenti o piattaforme)

9.1.3 nuovi obblighi normativi incidano sulla tracciabilità o sullo smaltimento degli asset

9.1.4 un incidente o un audit individui una lacuna nelle attuali pratiche di gestione degli asset

9.2 I riesami devono coinvolgere il GM e il responsabile IT e includere aggiornamenti alle procedure di gestione degli asset, ai modelli di inventario e alle linee guida di classificazione.

9.3 Tutti gli aggiornamenti devono essere documentati e comunicati al personale interessato. Deve essere conservato un registro delle modifiche soggetto a controllo di versione.

10. Politiche correlate e collegamenti

10.1 P2S – Politica sui ruoli e sulle responsabilità di governance: assegna la responsabilità della titolarità delle politiche e delle operazioni IT.

10.2 P4S – Politica di controllo degli accessi: collega l'uso degli asset (ad esempio laptop, dispositivi mobili) ai diritti di accesso degli utenti e alla gestione delle identità e degli accessi.

10.3 P7S – Politica di onboarding e cessazione del personale: assicura che assegnazione e recupero degli asset siano integrati nei processi del ciclo di vita del personale.

10.4 P13S – Politica di classificazione ed etichettatura dei dati: fornisce le regole per determinare se un asset debba essere classificato come Interno o Riservato.

10.5 P30S – Politica di risposta agli incidenti: disciplina le procedure di risposta nel caso in cui un evento relativo a un asset comporti una violazione della sicurezza o della privacy.

11. Standard e quadri di riferimento

11.1 ISO/IEC 27001

11.1.1 Clausola 8.1: richiede controlli operativi per gestire gli asset e proteggerli durante tutto il loro utilizzo.

11.2 ISO/IEC 27002

11.2.1 Controllo 5.9: descrive come identificare, assegnare la titolarità, classificare e gestire gli asset in modo sicuro.

11.3 NIST SP 800-53 Rev.5

11.3.1 CM-8: richiede alle organizzazioni di sviluppare e mantenere un inventario dei componenti di sistema, inclusi asset hardware, software e virtuali.

11.4 Regolamento UE GDPR

11.4.1 Articolo 30: richiede la documentazione delle attività di trattamento dei dati, che dipende dalla conoscenza di dove i dati sono conservati e su quali asset.

11.5 Direttiva UE NIS2

11.5.1 Articolo 21(2)(a): richiede misure tecniche e organizzative, incluso il tracciamento degli asset, per proteggere i sistemi di rete e informativi.

11.6 Regolamento UE DORA

11.6.1 Articolo 5(8): i soggetti finanziari devono mantenere inventari dettagliati degli asset ICT nell'ambito della gestione del rischio ICT.

11.7 COBIT 2019

11.7.1 BAI09: specifica che gli asset IT devono essere gestiti lungo l'intero ciclo di vita, dall'acquisizione alla dismissione, con chiara titolarità e controlli definiti.