					Inserire qui la denominazione dell'entità giuridica registrata							
Numero del documento: P10					Titolo del documento: **Politica per scrivania e schermo puliti**							
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	Clausola 6.1.3, Clausola 8	Piano di trattamento del rischio, pianificazione e controllo operativi per spazi di lavoro sicuri
ISO/IEC 27002:2022	Controllo 7	Controlli comportamentali e ambientali per proteggere le informazioni fisiche non presidiate
NIST SP 800-53 Rev.5	PE-2, PS-7, MP-6, AC-11, CM-6, IA-5	Accesso fisico, sicurezza del personale esterno, smaltimento dei supporti, blocco della sessione, configurazione e controlli sugli autenticatori
GDPR UE	Articoli 5(1)(f), 32; Considerando 39	Integrità dei dati, riservatezza e misure di sicurezza fisica per i dati
NIS2 UE	Articoli 21(2)(d), 21(3)	Politiche per la sicurezza fisica, il comportamento degli utenti e la prevenzione della perdita di dati
DORA UE	Articoli 5, 8, 9	Governance interna, sistemi ICT, gestione degli incidenti che coinvolgono la sicurezza fisica
COBIT 2019	DSS01, DSS05, MEA	Operazioni gestite, servizi di sicurezza gestiti e monitoraggio della conformità

1. Finalità

1.1 La presente politica stabilisce controlli obbligatori per proteggere le informazioni sensibili, imponendo la gestione sicura di documenti cartacei, postazioni di lavoro, schermi e supporti rimovibili, sia negli uffici sia negli spazi di lavoro condivisi.

1.2 La politica supporta il Controllo 7.7 dell'Allegato A della ISO/IEC 27001, imponendo pratiche comportamentali e tecniche che mitigano il rischio di divulgazione non autorizzata, furto o perdita di dati dovuti a informazioni lasciate incustodite o visibili.

1.3 La presente politica rafforza la sicurezza fisica e la sicurezza delle informazioni nelle operazioni quotidiane e supporta la conformità agli obblighi legali, contrattuali e normativi applicabili.

2. Ambito di applicazione

2.1 La presente politica si applica a tutto il personale che opera in spazi di lavoro fisici o vi accede, inclusi:

2.1.1 dipendenti a tempo indeterminato e personale temporaneo

2.1.2 appaltatori, fornitori di servizi terzi, consulenti e tirocinanti

2.1.3 visitatori in sede con accesso a informazioni sensibili

2.2 I requisiti si applicano a:

2.2.1 uffici individuali, postazioni delimitate e spazi di lavoro open space

2.2.2 sale riunioni e aree collaborative condivise

2.2.3 aree stampanti, banchi reception e locali fotocopie

2.2.4 aree in cui vengono utilizzate postazioni di lavoro remote o chioschi condivisi

2.3 La presente politica si applica anche agli ambienti di lavoro temporanei o ibridi (ad esempio hot-desking) e ai contesti aperti al pubblico in cui sussiste il rischio di osservazione indebita o di dati lasciati incustoditi.

3. Obiettivi

3.1 Prevenire l'accesso non autorizzato a informazioni riservate, sensibili o soggette a regolamentazione lasciate esposte in forma fisica o digitale.

3.2 Promuovere un livello di sicurezza standardizzato in tutti gli ambienti di lavoro mediante misure di sicurezza fisica, configurazione delle postazioni di lavoro e comportamenti degli utenti finali.

3.3 Ridurre il rischio di violazioni della privacy, perdita di proprietà intellettuale ed esfiltrazione dei dati causate da negligenza o disattenzione.

3.4 Integrare i comportamenti di scrivania pulita e schermo bloccato nella cultura organizzativa, a supporto della disciplina operativa, della verificabilità e della difendibilità legale.

3.5 Supportare la conformità alla ISO/IEC 27001, all'Articolo 32 del GDPR, all'Articolo 15 della NIS2 e ad altri requisiti di sicurezza fisica rilevanti per dati critici o personali.

4. Ruoli e responsabilità

4.1 Alta Direzione

4.1.1 Approva la presente politica e promuove una cultura orientata alla sicurezza in tutte le unità aziendali.

4.1.2 Assegna risorse adeguate per l'attuazione della politica, le campagne di sensibilizzazione e i meccanismi di controllo fisico.

4.2 Responsabile della sicurezza delle informazioni (CISO) / Responsabile del SGSI

4.2.1 È il titolare della politica e ne assicura l'allineamento alla ISO/IEC 27001:2022, ai requisiti di audit e alle strategie di trattamento del rischio.

4.2.2 Definisce programmi di sensibilizzazione e controlli per garantire un'applicazione coerente nelle sedi e negli assetti di lavoro ibridi.

4.2.3 Si coordina con il team di gestione delle strutture e degli asset e con l'IT per assicurare l'adozione di adeguate misure di sicurezza fisica.

[... 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 Pianificazione del riesame della politica

9.1.1 La presente politica deve essere riesaminata:

9.1.1.1 almeno annualmente

9.1.1.2 a seguito di qualsiasi non conformità di audit relativa all'esposizione di spazi di lavoro o schermi

9.1.1.3 a seguito di un incidente fisico o ambientale (ad esempio furto di dispositivi, tailgating, sorveglianza)

9.1.1.4 all'attuazione di nuovi layout d'ufficio, politiche delle strutture o modelli di spazio di lavoro (ad esempio hot desking, hub remoti)

9.2 Responsabili

9.2.1 Il titolare della politica è il Responsabile della sicurezza delle informazioni (CISO) o il Responsabile del SGSI designato.

9.2.2 Il processo di riesame deve coinvolgere:

9.2.2.1 i team delle strutture e della sicurezza aziendale

9.2.2.2 IT e infrastruttura informatica per l'attuazione relativa ai dispositivi

9.2.2.3 Risorse Umane (HR) e Funzione legale e compliance per l'applicazione dei comportamenti e l'allineamento disciplinare

9.2.3 Tutti gli aggiornamenti della politica devono essere soggetti a controllo delle versioni, approvati dal Comitato direttivo del SGSI e ridistribuiti con nuova presa d'atto ove richiesto.

9.3 Comunicazione delle modifiche

9.3.1 Gli utenti devono essere informati degli aggiornamenti sostanziali tramite:

9.3.1.1 portale delle policy o intranet aziendale

9.3.1.2 comunicazioni e-mail mirate

9.3.1.3 aggiornamenti di onboarding e briefing trimestrali

9.3.1.4 richieste obbligatorie di presa d'atto per eventuali nuove clausole critiche di applicazione della politica

10. Politiche correlate e collegamenti

10.1 La presente politica è allineata e supporta quanto previsto dalle seguenti politiche:

10.1.1 P1 – Politica per la sicurezza delle informazioni: definisce le aspettative di comportamento degli utenti e di sicurezza fisica su cui si fonda la presente politica.

10.1.2 P3 – Politica di uso accettabile: disciplina la responsabilità degli utenti nella protezione di dati e sistemi, inclusi gli ambienti fisici.

10.1.3 P6 – Politica di gestione del rischio: include i rischi degli spazi di lavoro fisici nell'analisi dei rischi informativi a livello aziendale.

10.1.4 P12 – Politica di gestione degli asset: supporta il tracciamento e la gestione sicura di dispositivi e supporti lasciati sulle scrivanie.

10.1.5 P13 – Politica di classificazione ed etichettatura dei dati: collega l'applicazione della scrivania pulita ai documenti fisici etichettati come Riservato o Interno.

10.1.6 P14 – Politica di conservazione e smaltimento dei dati: disciplina la conservazione dei documenti fisici, la distruzione e la gestione dei contenitori di smaltimento.

10.1.7 P22 – Politica di registrazione di audit e monitoraggio: può essere utilizzata per monitorare lo stato di blocco delle postazioni di lavoro, i tempi di inattività o i flussi video delle telecamere negli spazi di lavoro, ove consentito.

10.2 Tali politiche correlate definiscono una cultura della sicurezza integrata, che combina consapevolezza degli utenti, misure di sicurezza fisica e responsabilizzazione per garantire spazi di lavoro resilienti.

11. Standard e quadri di riferimento

11.1 La presente politica è allineata a standard riconosciuti a livello globale e a requisiti legali che impongono la protezione delle informazioni sensibili negli ambienti fisici e tramite il comportamento degli utenti.

11.2 ISO/IEC 27001

11.2.1 Clausola 6.1.3 – Piano di trattamento del rischio: supporta l'applicazione dei controlli per mitigare i rischi fisici e ambientali, inclusi quelli associati al comportamento degli utenti negli spazi di lavoro aperti.

11.2.2 Clausola 8.1 – Pianificazione e controllo operativi: stabilisce misure di sicurezza operative per gestire spazi di lavoro sicuri e l'uso delle apparecchiature.

11.3 ISO/IEC 27002:2022 – Controllo 7

11.3.1 Questo controllo impone protezioni comportamentali e ambientali per prevenire l'accesso non autorizzato alle informazioni tramite supporti, schermi o materiali stampati non presidiati. La politica impone ordine negli spazi di lavoro fisici, uso del blocco schermo e smaltimento dei documenti sensibili.

11.4 NIST SP 800-53 Rev.5

11.4.1 PE-2 (Autorizzazioni di accesso fisico): collegato tramite restrizioni degli spazi di lavoro e imposizione dell'archiviazione chiusa a chiave negli ambienti ad alto rischio.

11.4.2 PS-7 (Sicurezza del personale esterno): applicato tramite i requisiti di scrivania pulita e schermo bloccato estesi ad appaltatori e utenti di terze parti.

11.4.3 MP-6 (Sanitizzazione dei supporti) e AC-11 (Blocco della sessione): attuati tramite procedure di smaltimento sicuro e timer obbligatori di blocco dello schermo.

11.4.4 CM-6 (Impostazioni di configurazione) e IA-5 (Gestione degli autenticatori): supportano l'attuazione tecnica del blocco dello schermo e del controllo della sessione sugli endpoint.

11.5 GDPR UE (2016/679)

11.5.1 Articolo 5(1)(f): impone integrità e riservatezza dei dati personali, incluse misure di protezione contro l'esposizione fisica o la visione da parte di soggetti non autorizzati.

11.5.2 Articolo 32 – Sicurezza del trattamento: richiede misure fisiche e organizzative adeguate per proteggere i dati personali da distruzione accidentale o illecita, perdita o divulgazione non autorizzata, obiettivo perseguito tramite i controlli su scrivanie e schermi.

11.5.3 Considerando 39: richiede di limitare l'accesso ai dati personali ai soli soggetti autorizzati; ciò include la loro protezione in forma fisica quando non sono presidiati.

11.6 Direttiva UE NIS2 (2022/2555)

11.6.1 Articolo 21(2)(d): richiede politiche e procedure relative alla sicurezza fisica e ambientale, incluse misure di protezione delle informazioni a livello di luogo di lavoro.

11.6.2 Articolo 21(3): promuove una cultura della sicurezza che incorpori comportamenti corretti degli utenti, sensibilizzazione e prevenzione delle perdite accidentali di dati, supportata dai controlli comportamentali di questa politica.

11.7 DORA UE (2022/2554)

11.7.1 Articolo 5 – Governance interna e controllo: richiede che tutti i rischi connessi ai sistemi ICT, comprese le minacce umane e ambientali, siano governati tramite politiche applicabili.

11.7.2 Articolo 8 – Gestione del rischio ICT: impone misure di sicurezza sia nei contesti digitali sia in quelli fisici, garantendo che gli utenti remoti, in sede e in locale non generino esposizioni non gestite.

11.7.3 Articolo 9 – Gestione degli incidenti: richiede che le carenze ambientali o comportamentali che determinano esposizione dei dati siano registrate, classificate e trattate con adeguate azioni correttive.

11.8 COBIT 2019

11.8.1 DSS01 – Managed Operations: assicura disciplina operativa nella protezione degli spazi di lavoro fisici e dei sistemi tramite controlli ripetibili.

11.8.2 DSS05 – Managed Security Services: supporta la protezione di dati, dispositivi ed endpoint di accesso tramite l'applicazione di comportamenti quali le pratiche di scrivania pulita.

11.8.3 MEA03 – Monitor, Evaluate, and Assess Compliance: promuove l'audit delle misure di sicurezza fisica e dell'adozione della politica nelle pratiche aziendali quotidiane.