					Inserire qui la denominazione dell'entità giuridica registrata							
Numero del documento: P10S					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**

Allineata a standard e regolamenti

Standard/Regulation	Clause/Article	Comment
ISO/IEC 27001:2022	Clauses 7.2, 8	
ISO/IEC 27002:2022	Control 7	
NIST SP 800-53 Rev.5	PE-2, AC-11	
EU NIS2	Article 21(2)(d)	
EU DORA	Article 9(2)(f)	
COBIT 2019	DSS01.06, DSS05	
EU GDPR	Article 32	

1. Finalità

1.1 La presente politica stabilisce regole vincolanti per mantenere un ambiente di lavoro sicuro, assicurando che scrivanie, postazioni di lavoro e schermi siano privi di informazioni riservate visibili quando non presidiati.

1.2 L'obiettivo principale è prevenire l'accesso non autorizzato a informazioni sensibili tramite stampe lasciate incustodite, schermi non bloccati o supporti rimovibili conservati in modo improprio, sia negli ambienti fisici d'ufficio sia nelle sedi di lavoro da remoto.

1.3 Le pratiche di scrivania e schermo puliti definite nella presente politica rafforzano la capacità dell'organizzazione di soddisfare i requisiti di certificazione ISO/IEC 27001, riducendo i rischi di esposizione prevenibili. Tali pratiche forniscono inoltre a clienti, partner e auditor evidenza del fatto che la sicurezza delle informazioni è gestita con la dovuta attenzione, anche in contesti con risorse limitate.

1.4 La presente politica promuove una cultura della responsabilità e della consapevolezza, assicurando che tutto il personale, indipendentemente dal ruolo o dal livello di competenza tecnica, comprenda le proprie responsabilità nella protezione delle informazioni aziendali e dei clienti dall'esposizione visiva, dal furto o dalla perdita.

2. Ambito di applicazione

2.1 La presente politica si applica a:

2.1.1 tutti i dipendenti, i collaboratori esterni, i tirocinanti e il personale temporaneo che utilizzano postazioni di lavoro, scrivanie o dispositivi mobili di proprietà aziendale o loro assegnati a uso personale

2.1.2 tutti i luoghi fisici utilizzati per attività aziendali, inclusi uffici dedicati, ambienti di coworking e spazi di lavoro remoti o domestici

2.1.3 tutti i dispositivi digitali dotati di funzionalità di visualizzazione, inclusi computer desktop, laptop, tablet e monitor esterni utilizzati per finalità aziendali

2.2 La politica si estende a qualsiasi asset fisico o digitale che possa visualizzare, contenere o trasmettere informazioni sensibili, inclusi:

2.2.1 documenti stampati o note manoscritte

2.2.2 unità USB, CD e dischi rigidi esterni

2.2.3 telefoni cellulari utilizzati per messaggistica aziendale o posta elettronica

2.2.4 monitor e proiettori collegati ai sistemi di lavoro

2.3 La presente politica resta applicabile anche al di fuori del normale orario di lavoro e durante attività non ordinarie (ad esempio, interventi di manutenzione fuori orario o attività di risposta alle emergenze).

3. Obiettivi

3.1 Applicare controlli pratici e coerenti che assicurino che nessuna informazione sensibile sia lasciata esposta su scrivanie, schermi o spazi comuni.

3.2 Ridurre al minimo il rischio di accesso non autorizzato, sia da fonti interne (ad esempio accesso non intenzionale da parte di altri dipendenti) sia da minacce esterne (ad esempio visitatori, addetti alle pulizie o collaboratori esterni).

3.3 Supportare le restrizioni di accesso fisico e logico richiedendo al personale di mettere attivamente in sicurezza i materiali di lavoro e di bloccare i computer quando non presidiati.

3.4 Rafforzare la consapevolezza del personale in merito alle pratiche di lavoro sicure e fornire regole semplici e vincolanti applicabili nelle attività quotidiane, indipendentemente dal luogo di lavoro.

3.5 Assicurare l'allineamento con l'Appendice A, controllo 7.7, della ISO/IEC 27001 e con le relative linee guida di attuazione previste dalla ISO/IEC 27002 per i requisiti di scrivania e schermo puliti.

3.6 Assicurare che l'organizzazione possa dimostrare la dovuta diligenza e la conformità in sede di audit senza richiedere infrastrutture di livello enterprise.

4. Ruoli e responsabilità

4.1 Direttore Generale (GM)

4.1.1 È il titolare della politica e assicura che la stessa sia adeguatamente comunicata, compresa e rispettata da tutti i dipendenti e collaboratori esterni.

4.1.2 È responsabile dell'approvazione di eventuali eccezioni, della gestione delle violazioni e della supervisione della formazione relativa alle pratiche di lavoro sicure.

4.1.3 Deve effettuare o delegare controlli regolari, almeno trimestrali, per verificare che gli spazi di lavoro fisici e digitali soddisfino i requisiti della politica.

4.2 Membro del personale designato (se nominato)

4.2.1 Può ricevere la responsabilità di applicare configurazioni tecniche, ad esempio impostazioni di timeout dello schermo, o distribuire strumenti di archiviazione fisica, ad esempio cassetti con serratura.

4.2.2 Supporta il GM segnalando casi di non conformità, gestendo promemoria sulla sicurezza degli spazi di lavoro e monitorando le azioni correttive quando vengono individuate criticità.

4.2.3 Contribuisce ad assicurare che tutti i dipendenti dispongano, ove fattibile, di idonei meccanismi di chiusura o di spazi di archiviazione sicuri.

[... 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 Il GM deve riesaminare la presente politica almeno una volta all'anno e a seguito di uno qualsiasi dei seguenti eventi:

9.1.1 introduzione di nuovi spazi d'ufficio, dispositivi o sistemi condivisi

9.1.2 modifiche ai requisiti legali o di certificazione applicabili

9.1.3 risultanze di audit, valutazioni del rischio o incidenti di sicurezza

9.2 Gli aggiornamenti intermedi devono essere comunicati a tutti i dipendenti tramite e-mail, con obbligo di presa visione.

9.3 Le versioni precedenti della presente politica devono essere conservate in modo sicuro e verificabile ai fini di audit, per dimostrare il continuo allineamento con la ISO/IEC 27001 e i relativi quadri di riferimento.

10. Politiche correlate e collegamenti

10.1 P2S – Politica sui ruoli e sulle responsabilità di governance: chiarisce l'autorità del GM nell'applicazione della politica e nell'esecuzione di audit sui comportamenti relativi agli spazi di lavoro fisici e digitali.

10.2 P4S – Politica di controllo degli accessi: supporta l'attuazione tecnica delle pratiche di blocco dello schermo e di accesso sicuro alla postazione di lavoro.

10.3 P8S – Politica di consapevolezza e formazione sulla sicurezza delle informazioni: rafforza la formazione comportamentale necessaria per la conformità alla politica.

10.4 P17S – Politica di protezione dei dati e privacy: definisce gli obblighi relativi al trattamento e alla protezione dei dati personali e sensibili in conformità al GDPR.

10.5 P30S – Politica di risposta agli incidenti: fornisce il quadro di escalation e risposta qualora una violazione determini esposizione dei dati o una violazione dei dati personali.

11. Standard e quadri di riferimento

11.1 ISO/IEC 27001

11.1.1 Clausola 7.2: richiede che tutto il personale sia consapevole delle proprie responsabilità in materia di sicurezza, incluse le misure di protezione fisica.

11.1.2 Clausola 8.1: i controlli operativi devono assicurare adeguate misure di protezione fisica e logica.

11.2 ISO/IEC 27002

11.2.1 Controllo 7.7: fornisce indicazioni dettagliate sull'istituzione, comunicazione e applicazione dei requisiti di scrivania e schermo puliti.

11.3 NIST SP 800-53 Rev.5

11.3.1 PE-2: stabilisce i requisiti del controllo degli accessi fisici, compresi i comportamenti del personale negli ambienti sicuri.

11.3.2 AC-11: richiede la funzionalità di blocco della sessione per le postazioni di lavoro, al fine di prevenire visualizzazione o interazione non autorizzate.

11.4 EU GDPR

11.4.1 Articolo 32: richiede alle organizzazioni di proteggere i dati personali mediante misure di sicurezza fisiche e tecniche, incluse postazioni di lavoro e documenti.

11.5 Direttiva UE NIS2

11.5.1 Articolo 21(2)(d): richiede alle organizzazioni di implementare politiche di accesso fisico e logico basate sul rischio.

11.6 EU DORA

11.6.1 Articolo 9(2)(f): richiede politiche di sicurezza dei sistemi ICT, incluse pratiche sicure di gestione dello spazio di lavoro, per gli operatori del settore finanziario e le relative catene di fornitura.

11.7 COBIT 2019

11.7.1 DSS01.06: richiede pratiche di protezione degli asset, inclusi controlli fisici sugli spazi di lavoro e sui supporti.

11.7.2 DSS05.02: supporta l'applicazione delle pratiche di sicurezza degli utenti finali nei diversi ambienti operativi.