					Inserire qui la denominazione dell'entità giuridica registrata							
Numero del documento: P09					Titolo del documento: **Politica sul lavoro da remoto**							
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 obbligatori per lo svolgimento sicuro del lavoro da remoto, inclusi l'utilizzo dei sistemi dell'organizzazione, l'accesso ai dati e l'esecuzione delle attività lavorative al di fuori dei locali aziendali.

1.2 Essa garantisce la riservatezza, l'integrità e la disponibilità (CIA) degli asset informativi a cui si accede da remoto e stabilisce i controlli necessari a mitigare i rischi associati agli ambienti di lavoro distribuiti.

1.3 La politica soddisfa il requisito dell'Appendice A, Controllo 6.7, della ISO/IEC 27001:2022 mediante l'applicazione di misure di sicurezza tecniche e procedurali adeguate alle condizioni di lavoro da remoto.

2. Ambito di applicazione

2.1 La presente politica si applica a tutto il personale autorizzato a lavorare da remoto, inclusi:

2.1.1 Dipendenti (a tempo pieno, part-time, a contratto)

2.1.2 Fornitori di servizi esterni, consulenti e fornitori

2.1.3 Personale temporaneo e personale assegnato a progetti con accesso remoto approvato

2.2 La politica copre:

2.2.1 L'accesso ai sistemi dell'organizzazione tramite VPN o strumenti di accesso remoto approvati

2.2.2 La gestione di informazioni sensibili e soggette a regolamentazione al di fuori delle aree sicure

2.2.3 L'uso di apparecchiature di proprietà dell'organizzazione o di dispositivi personali (BYOD)

2.2.4 Le misure di protezione fisica e logica negli ambienti remoti

2.3 La politica si applica in tutte le aree geografiche e i fusi orari in cui l'organizzazione consente il lavoro da remoto, sia esso regolare, ad hoc o attivato nell'ambito di eventi di continuità operativa.

3. Obiettivi

3.1 Garantire che solo i soggetti autorizzati possano accedere da remoto ai sistemi interni e alle informazioni.

3.2 Applicare la cifratura, l'autenticazione a più fattori (MFA) e la protezione degli endpoint su tutti i canali di accesso remoto.

3.3 Mantenere un livello di sicurezza adeguato rispetto a minacce quali phishing, malware, esfiltrazione dei dati ed esposizione non autorizzata dei sistemi.

3.4 Disciplinare le modalità con cui i dati sensibili sono trasmessi, archiviati o stampati in ambienti esterni alle sedi aziendali.

3.5 Integrare misure di sicurezza fisica che riducano la visibilità e l'osservazione non autorizzata durante le sessioni da remoto.

3.6 Rispettare i requisiti normativi internazionali relativi all'accesso remoto ai dati, inclusi GDPR, NIS2 e DORA.

4. Ruoli e responsabilità

4.1 Direzione aziendale

4.1.1 Approva la presente politica e assicura l'assegnazione di risorse adeguate, nonché la sua integrazione nei processi HR, IT e di sicurezza.

4.1.2 Autorizza i criteri di idoneità organizzativa al lavoro da remoto e la relativa applicabilità alle unità aziendali.

4.2 Chief Information Security Officer (CISO) / Responsabile del SGSI

4.2.1 È il titolare della politica, ne cura il mantenimento e ne garantisce l'allineamento con la propensione al rischio e con i requisiti normativi.

4.2.2 Definisce i controlli di sicurezza per l'accesso remoto (ad esempio cifratura, protezione degli endpoint, timeout di sessione).

4.2.3 Approva la gestione delle eccezioni e monitora l'efficacia dei controlli.

[... 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 Frequenza di riesame

9.1.1 La presente politica deve essere riesaminata annualmente, o con maggiore frequenza a seguito di:

9.1.1.1 Introduzione di nuove tecnologie di accesso remoto

9.1.1.2 Espansione significativa del lavoro da remoto (ad esempio iniziative di forza lavoro ibrida)

9.1.1.3 Emergere di nuove minacce, vulnerabilità o incidenti collegati ad ambienti remoti

9.1.1.4 Modifiche ai quadri giuridici o normativi pertinenti

9.2 Titolarità e processo di riesame

9.2.1 Il titolare della politica è il CISO. Il riesame deve essere coordinato con:

9.2.1.1 IT Operations e Architettura

9.2.1.2 HR e Gestione delle Strutture e degli Asset (per implicazioni operative e relative agli spazi di lavoro)

9.2.1.3 Responsabile della Protezione dei Dati (DPO) (per privacy e controlli sui dati transfrontalieri)

9.2.2 Gli aggiornamenti della politica devono essere:

9.2.2.1 Approvati dal Comitato direttivo del SGSI

9.2.2.2 Comunicati a tutto il personale e ai collaboratori esterni interessati

9.2.2.3 Integrati nei materiali di onboarding e formazione di aggiornamento

9.3 Controllo documentale e distribuzione

9.3.1 La politica deve includere il controllo delle versioni, la data di entrata in vigore e lo storico delle versioni.

9.3.2 Le versioni sostituite devono essere conservate secondo la Politica di gestione documentale (P14).

9.3.3 Le versioni riviste devono richiedere una nuova presa d'atto obbligatoria da parte degli utenti idonei al lavoro da remoto.

10. Politiche correlate e collegamenti

10.1 La presente politica opera congiuntamente a:

10.1.1 P1 – Politica per la sicurezza delle informazioni: stabilisce la baseline per la gestione sicura degli asset, applicabile a tutti gli ambienti di lavoro, incluso quello remoto.

10.1.2 P3 – Politica di uso accettabile: disciplina l'uso appropriato dei dispositivi e dei sistemi dell’organizzazione durante le sessioni di lavoro da remoto.

10.1.3 P4 – Politica di controllo degli accessi: garantisce che i privilegi di accesso remoto seguano il principio del privilegio minimo e adeguati meccanismi di autenticazione.

10.1.4 P6 – Politica di gestione del rischio: definisce come i rischi del lavoro da remoto sono identificati, trattati e monitorati nell'ambito del SGSI.

10.1.5 P12 – Politica di gestione degli asset: richiede inventario e gestione della configurazione per tutti i dispositivi utilizzati da remoto.

10.1.6 P22 – Politica di registrazione e monitoraggio: garantisce che le sessioni remote siano monitorate, sottoposte ad audit e conservate in conformità ai requisiti di compliance.

10.1.7 P14 – Politica di conservazione e smaltimento dei dati: definisce le regole di gestione dei dati rilevanti per il lavoro da remoto, inclusi i supporti rimovibili e lo smaltimento dei dispositivi.

10.2 Tali politiche, nel loro insieme, garantiscono che il lavoro da remoto sia sicuro, conforme e applicabile in tutte le funzioni e aree geografiche.

11. Standard e quadri di riferimento

11.1 La presente politica è allineata a quadri di riferimento internazionalmente riconosciuti in materia di sicurezza, protezione dei dati e gestione del rischio ICT, al fine di garantire pratiche di lavoro da remoto sicure, tracciabili e conformi.

11.2 ISO/IEC 27001

11.2.1 Clausola 6.1.3 – Pianificazione del trattamento del rischio: la presente politica contribuisce al trattamento dei rischi associati all'accesso remoto e agli ambienti di lavoro distribuiti.

11.2.2 Clausola 8.1 – Pianificazione e controllo operativi: richiede l'attuazione di controlli per i sistemi a cui si accede al di fuori dei locali dell'organizzazione.

11.2.3 Appendice A, Controllo 6.7 – Lavoro da remoto: la presente politica disciplina integralmente i controlli richiesti per la sicurezza delle informazioni quando il personale opera al di fuori dei locali dell'organizzazione, comprese le misure di protezione fisica e logica, la governance degli accessi e il monitoraggio del comportamento degli utenti.

11.3 ISO/IEC 27002:2022 – Controllo 6

11.3.1 Questo controllo richiede misure di sicurezza procedurali e tecniche per il lavoro da remoto. Include requisiti relativi alla sicurezza dei dispositivi, ai metodi di accesso, alla gestione dei dati, alle misure di protezione ambientale e alla gestione delle terze parti, tutti attuati attraverso la presente politica.

11.4 NIST SP 800-53 Rev.5

11.4.1 AC-17 (Accesso remoto): supportato direttamente mediante controlli VPN, MFA, registrazione delle sessioni e autorizzazione all'accesso remoto basata sui ruoli per gli utenti remoti.

11.4.2 AC-2 (Gestione degli account): disciplina l'idoneità all'accesso, l'assegnazione dei privilegi remoti e la disattivazione degli account.

11.4.3 SC-12 e SC-13 (Protezione crittografica, definizione e gestione delle chiavi crittografiche): attuati mediante uso obbligatorio di VPN e cifratura completa del disco per gli endpoint remoti.

11.4.4 MP-5 (Protezione del trasporto dei supporti) e PE-18 (Ubicazione dei componenti del sistema informativo): le disposizioni sul lavoro da remoto impongono protezione durante il trasporto e misure di sicurezza fisica negli ambienti esterni alle sedi aziendali.

11.4.5 AU-2, AU-6: la registrazione e il monitoraggio delle sessioni remote supportano i requisiti di audit e di risposta agli incidenti.

11.5 GDPR UE (2016/679)

11.5.1 Articolo 32 – Sicurezza del trattamento: la presente politica applica i controlli di sicurezza dell'accesso remoto, la cifratura e la registrazione necessari a proteggere i dati personali a cui si accede o che sono trattati da remoto.

11.5.2 Articolo 5(1)(f): garantisce che i dati personali consultati fuori sede siano protetti da trattamenti non autorizzati o illeciti e da perdita accidentale.

11.5.3 Considerando 39: sottolinea la limitazione dell'accesso, l'integrità e la riservatezza, aspetti particolarmente rilevanti quando i dispositivi escono dai locali sicuri.

11.6 Direttiva NIS2 UE (2022/2555)

11.6.1 Articolo 21(2)(a, b, d): richiede che l'accesso remoto sia protetto come parte del quadro di gestione del rischio ICT dell'organizzazione. La presente politica soddisfa il requisito relativo alle misure di sicurezza che coprono il controllo degli accessi, la sicurezza dei dati e le politiche organizzative per gli ambienti remoti.

11.6.2 Articolo 21(3): promuove la sensibilizzazione alla sicurezza e l'applicazione della politica tra il personale che lavora al di fuori delle sedi centrali.

11.7 DORA UE (2022/2554)

11.7.1 Articolo 5 – Quadro di governance e controllo interno: la presente politica supporta le aspettative di controllo del rischio ICT per tutti gli scenari operativi, inclusi i modelli ibridi e remoti.

11.7.2 Articolo 8 – Quadro di gestione del rischio ICT: i rischi dell'accesso remoto sono identificati, mitigati e governati mediante i controlli tecnici e organizzativi qui previsti.

11.7.3 Articolo 9 – Accordi di condivisione delle informazioni: protegge dalla diffusione non autorizzata da remoto delle informazioni condivise all'interno delle reti di resilienza operativa digitale.

11.8 COBIT 2019

11.8.1 DSS01 – Managed Operations: la presente politica supporta la continuità sicura delle operazioni aziendali indipendentemente dalla collocazione fisica.

11.8.2 BAI06 – Managed IT Changes e BAI09 – Managed Assets: garantiscono che i dispositivi utilizzati per il lavoro da remoto siano tracciati, configurati in modo sicuro e gestiti come asset critici.

11.8.3 APO13 – Managed Security: promuove un quadro definito di governance della sicurezza per gli ambienti remoti.

11.8.4 MEA03 – Monitor, Evaluate, and Assess Compliance: stabilisce che l'attività di lavoro da remoto deve essere registrata, riesaminata e sottoposta ad audit.