					Inserire qui la denominazione dell'entità giuridica registrata							
Numero del documento: P09S					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**

Allineata, ove applicabile, a standard e regolamenti

Standard/Regulation	Clause/Article	Comment
ISO/IEC 27001:2022	Clause 6.1, 6.2, 8	
ISO/IEC 27002:2022	Controllo 6	
NIST SP 800-53 Rev.5	AC-17, AC-2	
EU NIS2	Articles 21(2)(b), 21(2)(h)	EU NIS
EU DORA	Article 9	EU DORA
COBIT 2019	DSS05, APO13	COBIT 2019
EU GDPR	Article 32	EU GDPR

1. Finalità

1.1 La presente politica definisce i requisiti di sicurezza applicabili a dipendenti e collaboratori esterni che operano da remoto, incluso il lavoro da casa, da spazi di coworking o in mobilità.

1.2 Ha lo scopo di proteggere la riservatezza, l'integrità e la disponibilità (CIA) delle informazioni aziendali accessibili al di fuori di ambienti controllati dall'azienda.

1.3 La presente politica assicura la conformità agli standard internazionali e riduce i rischi quali accessi non autorizzati, perdita di dati e interruzione dei servizi.

2. Ambito di applicazione

2.1 La presente politica si applica a tutto il personale, inclusi dipendenti, collaboratori esterni, consulenti e lavoratori temporanei, che accede a sistemi, reti o dati aziendali durante il lavoro fuori sede.

2.2 La politica copre:

2.2.1 l'uso di dispositivi aziendali e dispositivi personali

2.2.2 l'accesso tramite VPN, desktop remoto o servizi cloud

2.2.3 la gestione sicura delle informazioni al di fuori delle sedi aziendali

2.2.4 il monitoraggio, la gestione delle eccezioni e l'applicazione della politica

2.3 Si applica sia alle modalità di lavoro da remoto a tempo pieno sia a tempo parziale, incluso l'accesso remoto occasionale.

3. Obiettivi

3.1 Prevenire accessi non autorizzati ai sistemi aziendali o a dati sensibili durante il lavoro da remoto.

3.2 Garantire che i dispositivi e i collegamenti di comunicazione utilizzati al di fuori dell'ufficio soddisfino i requisiti minimi di sicurezza.

3.3 Mantenere il controllo sui privilegi di accesso remoto e sulle attività di monitoraggio.

3.4 Fornire indicazioni chiare a dipendenti e responsabili sulle pratiche sicure di lavoro da remoto.

3.5 Soddisfare i requisiti di ISO, NIS2, GDPR, DORA e COBIT applicabili al lavoro remoto e in mobilità.

4. Ruoli e responsabilità

4.1 Direttore generale (GM)

4.1.1 Approva le modalità di lavoro da remoto e ne monitora la conformità.

4.1.2 Riceve l'escalation degli incidenti di sicurezza e dei casi ripetuti di non conformità.

4.1.3 Riesamina le eccezioni e assicura il follow-up degli incidenti.

4.2 Fornitore di supporto IT o fornitore esterno di servizi IT

4.2.1 Predispone l'accesso remoto in modo sicuro, ad esempio tramite VPN e autenticazione a più fattori (MFA), inclusa la gestione dei dispositivi mobili.

4.2.2 Applica la protezione degli endpoint, la cifratura e la configurazione sicura dei dispositivi.

4.2.3 Supporta gli utenti e analizza eventuali problematiche tecniche di sicurezza.

[... 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 Riesame annuale della politica

9.1.1 Il Direttore generale (GM) e il Fornitore di supporto IT devono riesaminare annualmente la presente politica per allinearla ai cambiamenti tecnologici, organizzativi e normativi.

9.2 Trigger per aggiornamento anticipato

9.2.1 È richiesto un riesame immediato a seguito di:

9.2.1.1 un grave incidente di sicurezza relativo al lavoro da remoto

9.2.1.2 modifiche ai requisiti NIS2, GDPR o DORA

9.2.1.3 transizione verso una nuova tecnologia di accesso remoto, ad esempio una diversa piattaforma VPN

9.3 Controllo delle versioni e archiviazione

9.3.1 Tutte le versioni della presente politica devono essere:

9.3.1.1 datate e approvate dal Direttore generale (GM)

9.3.1.2 identificate con un numero di versione

9.3.1.3 archiviate per almeno tre anni

9.4 Comunicazione al personale

9.4.1 Gli aggiornamenti della politica devono essere comunicati a tutti gli utenti remoti. Per qualsiasi modifica significativa è richiesta la presa d'atto.

10. Politiche correlate e collegamenti

10.1 La presente politica è collegata alle seguenti politiche e le supporta:

10.1.1 P2S – Politica sui ruoli e sulle responsabilità di governance: definisce chi autorizza e supervisiona l'accesso remoto

10.1.2 P4S – Politica di controllo degli accessi: stabilisce la configurazione sicura dell'accesso remoto e le procedure di revoca degli accessi

10.1.3 P6S – Politica di gestione del rischio: traccia e valuta i rischi relativi all'accesso fuori sede

10.1.4 P8S – Politica di consapevolezza e formazione sulla sicurezza delle informazioni: forma gli utenti sui rischi del lavoro da remoto e sulle buone pratiche

10.1.5 P30S – Politica di risposta agli incidenti: disciplina la risposta agli incidenti di accesso remoto, quali la perdita delle credenziali di accesso o lo smarrimento del dispositivo

11. Standard e quadri di riferimento

11.1 ISO/IEC 27001

11.1.1 Clausola 6.1 – Pianificazione basata sul rischio per gli scenari di accesso remoto

11.1.2 Clausola 6.2 – Definisce le responsabilità delle Risorse Umane (HR) nei contesti mobili e remoti

11.1.3 Clausola 8.1 – Pianificazione operativa e controllo dei processi remoti

11.2 ISO/IEC 27002

11.2.1 Controllo 6.7 – Fornisce indicazioni pratiche sulla sicurezza per il lavoro remoto e in mobilità

11.3 NIST SP 800-53 Rev.5

11.3.1 AC-17 – Controllo degli accessi remoti, protezione delle sessioni e monitoraggio della sicurezza

11.3.2 AC-2 – Controllo degli account per utenti fuori sede

11.4 EU GDPR

11.4.1 Articolo 32 – Richiede la protezione dei dati fin dalla progettazione e per impostazione predefinita, anche in contesti remoti

11.5 Direttiva UE NIS2

11.5.1 Articolo 21(2)(b) – Richiede l'uso sicuro dei sistemi informativi e di rete

11.5.2 Articolo 21(2)(h) – Richiede misure di sicurezza relative alle Risorse Umane (HR), inclusi i controlli fuori sede

11.6 EU DORA

11.6.1 Articolo 9 – Richiede ai soggetti finanziari di mantenere la resilienza dei sistemi ICT in tutte le modalità operative, incluso l'accesso remoto

11.7 COBIT 2019

11.7.1 DSS05 – Gestire i servizi di sicurezza: include la protezione degli endpoint e pratiche sicure per il lavoro da remoto

11.7.2 APO13 – Gestione della sicurezza: garantisce l'abilitazione sicura e la supervisione del rischio per l'accesso mobile e remoto