					Inserire qui la denominazione dell'entità giuridica registrata							
Numero del documento: P21S					Titolo del documento: **Politica di sicurezza della rete**							
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

Norma/Regolamento	Clausola/Articolo	Commento
ISO/IEC 27001:2022	Clausola 8	-
ISO/IEC 27002:2022	Controllo 8	-
NIST SP 800-53 Rev.5	AC-4, SC-7	-
GDPR UE	Articolo 32	-
NIS2 UE	Articoli 21(2)(d), (e)	-
DORA UE	Articoli 9, 10	-
COBIT 2019	DSS05.02, APO13	-

1. Finalità

1.1. La presente politica ha lo scopo di garantire che tutte le comunicazioni di rete interne ed esterne siano protette da accessi non autorizzati, manomissioni, intercettazioni o usi impropri mediante controlli di sicurezza chiaramente definiti.

1.2. La presente politica definisce le regole per la progettazione sicura, l'utilizzo e la gestione dell'infrastruttura di rete, inclusi router, punti di accesso wireless, connessioni di accesso remoto e reti segmentate.

1.3. La presente politica mira a ridurre al minimo l'esposizione alle minacce provenienti da Internet, a garantire la riservatezza dei dati trasmessi sulle reti interne ed esterne e a mantenere la disponibilità dei servizi critici.

1.4. La presente politica supporta la certificazione ISO/IEC 27001:2022 e contribuisce direttamente alla conformità agli obblighi legali e regolamentari ai sensi di GDPR, NIS2 e DORA, fornendo al contempo adeguate garanzie tecniche a clienti e auditor.

2. Ambito di applicazione

2.1. La presente politica si applica a tutti i componenti della rete IT dell'organizzazione, inclusi:

2.1.1. l'infrastruttura cablata e wireless presso le sedi aziendali

2.1.2. router, switch, punti di accesso, firewall e gateway

2.1.3. connessioni di accesso remoto, incluse VPN, RDP e tunnel cloud

2.1.4. applicazioni cloud accessibili da reti interne o esterne

2.1.5. dispositivi connessi alla rete da dipendenti, collaboratori esterni o ospiti

2.2. La presente politica disciplina sia i segmenti di rete fisici sia quelli logici, comprese le reti guest, i dispositivi IoT e i sistemi di back-office.

2.3. La politica si applica a tutto il personale con accesso alla rete dell'organizzazione, inclusi:

2.3.1. dipendenti

2.3.2. lavoratori da remoto e personale in modalità ibrida

2.3.3. fornitori esterni, consulenti e provider di servizi

2.3.4. ospiti che utilizzano accesso Wi-Fi temporaneo

3. Obiettivi

3.1. Garantire che la rete dell'organizzazione sia protetta da accessi non autorizzati e minacce informatiche esterne.

3.2. Assicurare un'adeguata segmentazione tra reti fidate e non fidate, ad esempio Wi-Fi guest e accesso dei fornitori.

3.3. Consentire una connettività remota sicura senza compromettere i sistemi interni.

3.4. Prevenire la propagazione di malware e l'esfiltrazione di dati attraverso i canali di rete.

3.5. Garantire il monitoraggio, la generazione di avvisi e l'audit delle attività di rete a supporto del rilevamento degli incidenti e della conformità.

3.6. Garantire che solo i dispositivi approvati e protetti siano autorizzati a connettersi alle reti interne.

3.7. Soddisfare gli obblighi previsti da ISO 27001, GDPR e dai relativi quadri di riferimento per la cybersicurezza.

4. Ruoli e responsabilità

4.1. Direttore generale (GM)

4.1.1. È il titolare della politica e assicura l'assegnazione di risorse adeguate per la progettazione e la gestione sicura della rete.

4.1.2. Riesamina le eccezioni ai controlli di sicurezza della rete e approva gli accordi di accesso alla rete per i fornitori.

4.1.3. Riesamina gli incidenti o le risultanze degli audit relativi a debolezze nella sicurezza della rete.

4.2. Fornitore di supporto IT / funzione IT interna

4.2.1. Implementa, configura e mantiene firewall, router, switch e controller wireless.

4.2.2. Gestisce la segmentazione tra reti interne, guest ed esterne.

4.2.3. Monitora log e avvisi relativi a tentativi di accesso non autorizzato o anomalie di rete.

4.2.4. Garantisce che gli aggiornamenti di firmware e configurazione siano applicati in modo sicuro e tempestivo.

[... 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

9.1.1. La presente politica deve essere riesaminata almeno una volta l'anno dal Direttore generale con il Fornitore di supporto IT e il Referente privacy.

9.2. Eventi attivatori del riesame intermedio

9.2.1. Il riesame della politica deve essere attivato anche dai seguenti eventi:

9.2.1.1. modifiche rilevanti all'architettura di rete, ad esempio nuovi sistemi VPN o firewall

9.2.1.2. un incidente correlato alla rete, ad esempio intrusione, diffusione di ransomware o esfiltrazione di dati

9.2.1.3. aggiornamenti legislativi, regolamentari o dei quadri di riferimento che incidono sulla protezione della rete

9.2.1.4. nuove piattaforme di fornitori che richiedono metodi o protocolli di accesso alternativi

9.3. Gestione delle versioni e documentazione

9.3.1. Le revisioni della politica devono essere registrate con numero di versione, data e sintesi delle modifiche.

9.3.2. Le versioni precedenti devono essere archiviate per almeno 3 anni.

9.3.3. Gli aggiornamenti devono essere comunicati ai dipendenti interessati, con presa visione della politica ove vengano introdotti cambiamenti comportamentali significativi.

10. Politiche correlate e collegamenti

10.1. La presente politica deve essere applicata congiuntamente alle seguenti politiche di sicurezza per le PMI:

10.1.1. P9S – Politica di lavoro da remoto: definisce metodi sicuri di accesso remoto, requisiti VPN e protezione degli endpoint per gli utenti fuori sede.

10.1.2. P12S – Politica di gestione degli asset: garantisce che tutti i sistemi connessi alla rete siano identificati, categorizzati e tracciati con stato di sicurezza aggiornato.

10.1.3. P17S – Politica di protezione dei dati e privacy: garantisce che segmentazione della rete, controllo degli accessi e registrazione nei log supportino i principi di privacy e protezione dei dati ai sensi del GDPR.

10.1.4. P22S – Politica di registrazione e monitoraggio: specifica i requisiti per l'acquisizione e il riesame dei log provenienti da dispositivi di rete, connessioni remote e controller wireless.

10.1.5. P30S – Politica di risposta agli incidenti: definisce le azioni richieste in risposta a violazioni della rete, tentativi di accesso non autorizzato o propagazione di malware tramite reti interne.

11. Standard e quadri di riferimento

11.1. ISO/IEC 27001

11.1.1. Clausola 8.1 – Richiede l'implementazione di controlli per garantire operazioni sicure e resilienti, incluse le reti.

11.2. ISO/IEC 27002

11.2.1. Controllo 8.20 – Fornisce indicazioni tecniche e procedurali per la protezione dell'accesso alla rete, della segmentazione e del monitoraggio.

11.3. NIST SP 800-53 Rev.5

11.3.1. AC-4 – Richiede il controllo dei flussi informativi all'interno delle reti e tra i sistemi.

11.3.2. SC-7 – Richiede la protezione dei confini, l'instradamento sicuro e la segmentazione della rete per ridurre il rischio di accessi non autorizzati.

11.4. GDPR UE

11.4.1. Articolo 32 – Richiede misure tecniche e organizzative adeguate per garantire la riservatezza, l'integrità e la disponibilità dei sistemi e dei servizi di rete che trattano dati personali.

11.5. Direttiva UE NIS2

11.5.1. Articolo 21(2)(d) – Richiede misure tecniche basate sul rischio, inclusa la sicurezza della rete e il controllo degli accessi.

11.5.2. Articolo 21(2)(e) – Richiede la segmentazione e l'isolamento dei sistemi per impedire la propagazione degli incidenti informatici.

11.6. DORA UE

11.6.1. Articolo 9 – Richiede alle organizzazioni di implementare controlli di gestione del rischio ICT, inclusi quelli relativi a reti e comunicazioni sicure.

11.6.2. Articolo 10 – Richiede che le strategie di resilienza digitale comprendano la protezione dell'infrastruttura di rete e della connettività remota.

11.7. COBIT 2019

11.7.1. DSS05.02 – Richiede una protezione efficace dell'infrastruttura informatica e degli ambienti di rete contro minacce interne ed esterne.

11.7.2. APO13.01 – Richiede strategie di gestione del rischio che includano segmentazione della rete e monitoraggio come parte della mitigazione delle minacce.