					Inserire qui la denominazione dell'entità giuridica registrata							
Numero del documento: P21					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 norme e regolamenti

Standard/Regulation	Clause/Article	Comment
ISO/IEC 27001:2022	Clause 8	N/A
ISO/IEC 27002:2022	Controls 8.20-8	N/A
NIST SP 800-53 Rev.5	SC-7, AC-4, SC-32	N/A
GDPR UE	Articolo 32	N/A
NIS2 UE	Articolo 21(2)(d)	N/A
DORA UE	Articolo 9	N/A
COBIT 2019	DSS01.03, DSS05.01, MEA	N/A

1. Finalità

1.1 La presente politica definisce i requisiti dell'organizzazione per la protezione delle reti interne ed esterne da accessi non autorizzati, indisponibilità dei servizi, intercettazione dei dati e utilizzo improprio.

1.2 Essa garantisce che l'intera infrastruttura di rete, inclusi gli ambienti fisici, virtuali, cloud e ibridi, sia protetta mediante controlli multilivello quali segmentazione e isolamento della rete, applicazione delle regole firewall, instradamento sicuro e monitoraggio centralizzato.

1.3 La presente politica dà attuazione alla Clause 8.1 della ISO/IEC 27001 e ai controlli dell'Annex A da 8.20 a 8.22, assicurando la conformità ai pertinenti obblighi legali e normativi ai sensi dell'Articolo 32 del GDPR, dell'Articolo 21 della NIS2 e dell'Articolo 9 del DORA.

2. Ambito di applicazione

2.1 La presente politica si applica a tutte le reti e ai relativi componenti infrastrutturali, inclusi:

2.1.1 router, switch, punti di accesso wireless e firewall

2.1.2 reti virtuali cloud (ad es. AWS VPC, Azure VNET), concentratori VPN e sistemi SD-WAN

2.1.3 LAN interne, zone demilitarizzate (DMZ), canali di accesso remoto (VPN, gestione dei dispositivi mobili) e connessioni inter-sito o di terze parti

2.1.4 sistemi di supporto quali DNS, DHCP, server proxy e apparati di monitoraggio

2.2 La politica è vincolante per tutto il personale e per i fornitori terzi che gestiscono, configurano, monitorano o si interfacciano con le reti dell'organizzazione, sia in locale sia nel cloud.

2.3 Tutti i sistemi e le applicazioni connessi alle reti dell'organizzazione, indipendentemente dall'ubicazione o dalla proprietà, devono essere conformi ai presenti requisiti di sicurezza della rete.

3. Obiettivi

3.1 Garantire la riservatezza, l'integrità e la disponibilità (CIA) dei dati trasmessi sulle reti mediante robusti controlli di accesso, instradamento sicuro e monitoraggio.

3.2 Prevenire accessi non autorizzati, movimenti laterali e sfruttamento delle risorse di rete applicando segmentazione, zonizzazione e protezione del perimetro.

3.3 Mantenere configurazioni di rete coerenti, basate sugli standard di settore e sulle informazioni sulle minacce, per difendersi dalle minacce informatiche in evoluzione.

3.4 Proteggere le comunicazioni esterne, le interconnessioni cloud e l'accesso remoto mediante canali cifrati, autenticazione forte e validazione degli endpoint.

3.5 Garantire visibilità sulle attività di rete mediante registrazione centralizzata, ispezione del traffico in tempo reale e avvisi automatici.

3.6 Assicurare la conformità normativa allineando tutte le operazioni di rete ai requisiti di ISO/IEC 27001:2022, GDPR, NIS2, DORA e COBIT 2019.

4. Ruoli e responsabilità

4.1 Responsabile della sicurezza delle informazioni (CISO)

4.1.1 È il proprietario della politica e ne assicura il riesame e l'allineamento con la strategia complessiva di cybersicurezza dell'organizzazione.

4.1.2 Approva i modelli di segmentazione della rete, i set di regole firewall per i sistemi sensibili e le richieste di eccezione.

4.2 Responsabile della sicurezza di rete / Responsabile della sicurezza infrastrutturale

4.2.1 Gestisce l'architettura di difesa della rete, inclusi firewall, sistemi di rilevamento/prevenzione delle intrusioni (IDS/IPS), VPN e instradamento sicuro.

4.2.2 Supervisiona la segmentazione della rete, le assegnazioni VLAN, la zonizzazione del traffico e la connettività esterna.

4.2.3 Assicura il riesame continuo del filtraggio del traffico in ingresso e in uscita e l'applicazione del modello zero trust tra i diversi livelli di rete.

[... 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 La presente politica deve essere riesaminata annualmente dal Responsabile della sicurezza di rete, in collaborazione con il Responsabile della sicurezza delle informazioni (CISO), e aggiornata sulla base di:

9.1.1 rischi emergenti (ad es. nuove tecniche di attacco, vulnerabilità dei protocolli)

9.1.2 modifiche dell'infrastruttura (ad es. migrazioni di sistema al cloud, introduzione di SD-WAN)

9.1.3 aggiornamenti normativi o degli standard che incidono sulle misure di protezione della rete

9.1.4 risultanze dell'audit, tendenze degli incidenti o degrado delle prestazioni causato dai controlli

9.2 I riesami devono inoltre essere attivati da:

9.2.1 modifiche rilevanti all'architettura di rete

9.2.2 implementazione di nuove piattaforme firewall, VPN o di rete cloud

9.2.3 dismissione di asset chiave o di zone attendibili

9.3 Gli aggiornamenti devono essere registrati nel registro di controllo documentale del SGSI e comunicati a:

9.3.1 infrastruttura e operazioni di rete

9.3.2 SOC e team di ingegneria della sicurezza

9.3.3 team applicativi con dipendenze di sistema dai flussi di rete

9.3.4 tutti i fornitori terzi con interconnessioni attive

9.4 Tutte le versioni precedenti della politica devono essere archiviate in modo sicuro con annotazioni della cronologia delle modifiche, al fine di preservare verificabilità e tracciabilità delle modifiche.

10. Politiche correlate e collegamenti

10.1 P1 - Politica per la sicurezza delle informazioni. Stabilisce i principi fondamentali di sicurezza e prescrive protezioni multilivello, inclusi controlli di accesso e controlli sulle minacce basati sulla rete.

10.2 P4 - Politica di controllo degli accessi. Garantisce che la segmentazione della rete sia applicata in coerenza con i ruoli utente, il principio del privilegio minimo e le regole di provisioning degli accessi.

10.3 P5 - Politica di gestione dei cambiamenti. Disciplina le modifiche ai firewall, gli adeguamenti delle regole VPN e le modifiche di instradamento attraverso un processo documentato e verificabile.

10.4 P12 - Politica di gestione degli asset. Supporta l'identificazione e la classificazione dei sistemi connessi alla rete e garantisce che tutti gli asset collegati siano gestiti entro ambiti definiti dalla politica.

10.5 P22 - Politica di registrazione e monitoraggio. Disciplina la raccolta, la correlazione e la conservazione dei log di rete, inclusi eventi firewall, tentativi di accesso e rilevazioni di anomalie.

10.6 P30 - Politica di risposta agli incidenti (P30). Definisce le procedure di escalation, contenimento ed eradicazione in risposta a minacce o intrusioni veicolate dalla rete, quali DDoS, movimenti laterali o accessi non autorizzati.

11. Standard e quadri di riferimento

11.1 La presente politica è allineata a standard internazionali e prescrizioni normative che definiscono operazioni di rete sicure, segmentazione, protezione perimetrale e accesso remoto sicuro.

11.2 ISO/IEC 27001

11.2.1 Clause 8.1 - Pianificazione e controllo operativi: richiede che i controlli tecnici, incluse le misure di sicurezza di rete, siano integrati nei processi operativi.

11.3 ISO/IEC 27002:2022

11.3.1 Controls 8.20-8: forniscono indicazioni sulla protezione delle reti, sulla segmentazione dei servizi e sulla sicurezza dei servizi di rete mediante controlli di accesso e monitoraggio.

11.4 NIST SP 800-53 Rev.5

11.4.1 SC-7 - Protezione dei confini: richiede controlli perimetrali, segmentazione e interconnessioni sicure.

11.4.2 AC-4 - Applicazione del flusso informativo: supporta la zonizzazione e le restrizioni del traffico basate su regole.

11.4.3 SC-32 - Partizionamento dei sistemi informativi: promuove la separazione logica dei sistemi informativi.

11.5 GDPR UE (2016/679)

11.5.1 Articolo 32 - Sicurezza del trattamento: richiede misure tecniche, quali firewall e segmentazione, per proteggere i dati personali.

11.6 Direttiva UE NIS2 (2022/2555)

11.6.1 Articolo 21(2)(d): richiede misure efficaci di sicurezza delle reti e dei sistemi informativi, protezione perimetrale, configurazione sicura e controlli di segregazione.

11.7 DORA UE (2022/2554)

11.7.1 Articolo 9 - Gestione del rischio ICT: impone alle entità finanziarie di proteggere reti e interconnessioni da accessi non autorizzati, perdite di dati e interruzioni operative.

11.8 COBIT 2019

11.8.1 DSS01.03 - Monitorare l'infrastruttura: richiede un controllo proattivo sullo stato della rete e sulla connettività.

11.8.2 DSS05.01 - Proteggere dal malware: include segmentazione e controllo dei confini per ridurre al minimo la propagazione.

11.8.3 MEA03 - Monitorare, valutare e verificare la conformità: rafforza l'applicazione della politica di rete e le valutazioni di conformità.