POL Politica di sicurezza delle informazioni

Storia della versione

Versione	Data	Autore	Approvato da
1	14/01/2026	Stefano Castegnero	Sandro Castegnero

Indice

Scopo

La presente politica formalizza l'impegno del Top Management di 7networks Sagl verso la protezione degli asset informativi dell'organizzazione. In qualità di documento quadro del Sistema di Gestione della Sicurezza delle Informazioni (SGSI), essa stabilisce il riferimento strategico per istituire, attuare, mantenere e migliorare continuamente il sistema stesso, al fine di salvaguardare la riservatezza, l'integrità e la disponibilità delle informazioni trattate nell'ambito della progettazione, integrazione, gestione e supporto di infrastrutture IT, soluzioni cloud e servizi di cybersecurity.

Attraverso questo documento, la Direzione dichiara la propria determinazione a perseguire un livello di sicurezza adeguato al contesto operativo e al panorama delle minacce, sostenendo al contempo gli obiettivi strategici aziendali e le aspettative delle parti interessate. La politica costituisce il fondamento su cui si innestano tutte le ulteriori policy e procedure di sicurezza dell'organizzazione, orientando le decisioni operative verso la riduzione sistematica del rischio e la conformità ai requisiti normativi applicabili.

Campo di applicazione

La presente politica si applica a tutte le attività, i processi, gli asset informativi, i sistemi informativi e di rete e le sedi operative dell'organizzazione, compresa la sede principale di Via Cantonale 36, 6928 Manno e il datacenter in colocation presso Bancadati SA, Centro Galleria 2, 6928 Manno. Coinvolge tutto il personale, inclusi dipendenti, collaboratori a contratto, consulenti esterni e terze parti che accedono alle informazioni o ai sistemi aziendali, indipendentemente dalla loro ubicazione geografica o dalla modalità di lavoro (in sede o da remoto). Sono escluse dal perimetro del SGSI le attività di sviluppo software, non svolte dall'organizzazione.

Riferimenti normativi

- ISO/IEC 27001:2022
- ISO/IEC 27002:2022
- Direttiva (UE) 2022/2555
- D.Lgs. 138/2024
- LPD (Legge federale sulla protezione dei dati, Svizzera)

Termini e definizioni

- **Sicurezza delle informazioni:** preservazione della riservatezza, dell'integrità e della disponibilità delle informazioni.
- **Riservatezza:** proprietà per cui le informazioni non sono rese disponibili o divulgate a individui, entità o processi non autorizzati.

- **Integrità:** proprietà di accuratezza e completezza delle informazioni.
- **Disponibilità:** proprietà di essere accessibile e utilizzabile su richiesta da parte di un'entità autorizzata.
- **Sistema di gestione della sicurezza delle informazioni (SGSI):** parte del sistema di gestione complessivo, basata su un approccio al rischio d'impresa, volta a stabilire, implementare, gestire, monitorare, riesaminare, mantenere e migliorare la sicurezza delle informazioni.
- **Rischio:** effetto dell'incertezza sugli obiettivi, espresso in termini di combinazione delle conseguenze di un evento e della relativa probabilità di accadimento.
- **Trattamento del rischio:** processo volto a modificare il rischio, che può includere evitare, assumere, rimuovere la fonte, modificare la probabilità o le conseguenze, condividere il rischio o mantenerlo per decisione informata.
- **Evento di sicurezza delle informazioni:** occorrenza identificata in un sistema, servizio o rete che indica una possibile violazione della politica di sicurezza delle informazioni, un fallimento dei controlli o una situazione precedentemente sconosciuta che potrebbe avere rilevanza per la sicurezza.
- **Incidente di sicurezza delle informazioni:** uno o più eventi di sicurezza delle informazioni che hanno una probabilità significativa di compromettere le operazioni aziendali e di minacciare la sicurezza delle informazioni.
- **Miglioramento continuo:** attività ricorrente volta ad accrescere le prestazioni del sistema di gestione.

Ruoli e responsabilità

- **Top Management (Direzione):** approva la presente politica e le politiche specifiche del SGSI, assicura la disponibilità delle risorse necessarie e riesamina periodicamente l'adeguatezza del sistema di gestione della sicurezza delle informazioni.
- **RSGSI Primary:** supervisiona l'implementazione e il mantenimento del SGSI, conduce le valutazioni dei rischi e gli audit interni e riferisce alla Direzione sullo stato della sicurezza delle informazioni e della conformità.
- **RSGSI Secondary:** supporta il RSGSI Primary nella gestione quotidiana del SGSI, monitora l'efficacia dei controlli e contribuisce alla formazione sulla consapevolezza della sicurezza delle informazioni.
- **Cybersecurity e protezione dati:** sviluppa e mantiene la strategia di cybersecurity e le politiche di protezione dei dati, supervisiona il monitoraggio continuo delle reti e conduce valutazioni dei rischi specifiche.
- **Sistemi:** garantisce la progettazione, l'implementazione e la manutenzione sicura dei sistemi e delle infrastrutture IT secondo le politiche di sicurezza dell'organizzazione.
- **Network and Security:** progetta e mantiene architetture di rete sicure, gestisce i dispositivi di sicurezza perimetrale e monitora il traffico di rete per anomalie e minacce.

- **Tutto il personale:** si conforma alle politiche e alle procedure del SGSI, segnala tempestivamente eventi e incidenti di sicurezza attraverso i canali previsti e partecipa alle attività di formazione e sensibilizzazione.

Obiettivi di sicurezza delle informazioni

7networks Sagl persegue la protezione sistematica del proprio patrimonio informativo attraverso obiettivi di sicurezza che traducono la visione strategica della Direzione in impegni misurabili e verificabili. Tali obiettivi sono coerenti con il contesto operativo dell'organizzazione — fornitore di servizi IT gestiti, soluzioni Microsoft Cloud e cybersecurity per il mercato B2B svizzero — e tengono conto dei rischi identificati, delle aspettative delle parti interessate e dei requisiti normativi applicabili.

L'organizzazione si impegna a:

- Preservare la riservatezza, l'integrità e la disponibilità delle informazioni proprie e dei clienti durante l'intero ciclo di vita dei dati, dalla raccolta alla dismissione sicura.
- Minimizzare la probabilità e l'impatto degli incidenti di sicurezza delle informazioni, assicurando la capacità di rilevarli tempestivamente, contenerli efficacemente e ripristinare le normali operazioni entro i tempi definiti nei piani di continuità operativa.
- Gestire i rischi per la sicurezza delle informazioni attraverso un processo strutturato e periodico di valutazione e trattamento, fondato sulla metodologia Probabilità × Impatto e coerente con gli standard ISO 27005 e NIST adottati dall'organizzazione.
- Garantire la conformità alla normativa applicabile in materia di sicurezza delle informazioni e protezione dei dati, incluse le disposizioni della Direttiva NIS 2 e della legge federale svizzera sulla protezione dei dati.
- Promuovere la consapevolezza e la competenza di tutto il personale in materia di sicurezza delle informazioni, mediante programmi di formazione annuali differenziati per ruolo e livello di accesso ai sistemi.
- Assicurare la sicurezza della catena di approvvigionamento, monitorando i fornitori critici — in particolare i data center provider e i distributori di prodotti IT — attraverso criteri di qualifica, clausole contrattuali di sicurezza e verifiche periodiche.
- Integrare la sicurezza delle informazioni nella gestione dei progetti sin dalla fase di avvio, garantendo che i rischi siano identificati e trattati nel rispetto del principio di security by design.

Gli obiettivi sono declinati in indicatori specifici documentati nel programma di miglioramento e riesaminati periodicamente dalla Direzione nell'ambito del riesame del sistema di gestione, al fine di verificarne il raggiungimento e definire le azioni correttive o di adeguamento necessarie.

Principi fondamentali di sicurezza delle informazioni

La presente politica si fonda su un insieme di principi che orientano ogni decisione, controllo e comportamento in materia di sicurezza delle informazioni all'interno dell'organizzazione. Questi principi permeano l'intero SGSI e costituiscono il riferimento

permanente per l'elaborazione delle politiche specifiche, delle procedure operative e dei piani di trattamento del rischio.

Approccio basato sul rischio. L'organizzazione adotta un metodo sistematico di identificazione, valutazione e trattamento dei rischi per la sicurezza delle informazioni, proporzionato alla criticità degli asset e al contesto delle minacce. Le decisioni in materia di controlli, investimenti e priorità discendono dai risultati delle valutazioni del rischio, garantendo che le risorse siano concentrate dove l'esposizione è maggiore.

Responsabilità condivisa. La sicurezza delle informazioni non è prerogativa esclusiva delle funzioni tecniche: ogni persona che accede alle informazioni o ai sistemi dell'organizzazione contribuisce attivamente alla loro protezione. La Direzione promuove una cultura in cui ciascun ruolo comprende i propri obblighi di sicurezza e li esercita nella pratica quotidiana.

Difesa in profondità. L'organizzazione implementa controlli di sicurezza su più livelli — organizzativi, fisici, logici e procedurali — in modo che il cedimento di un singolo controllo non comprometta la protezione complessiva. Questo approccio si estende alla segmentazione delle reti, alla protezione perimetrale, alla cifratura dei dati e al monitoraggio continuo delle attività.

Minimo privilegio e necessità di conoscere. L'accesso alle informazioni e ai sistemi è concesso nella misura strettamente necessaria allo svolgimento delle mansioni assegnate. Le abilitazioni sono riesaminate periodicamente e revocate tempestivamente al modificarsi delle responsabilità o alla cessazione del rapporto.

Conformità e legalità. L'organizzazione si impegna a rispettare i requisiti legislativi, regolamentari e contrattuali applicabili, adattando il proprio SGSI all'evoluzione del panorama normativo. La conformità è verificata attraverso audit interni periodici, riesami di direzione e, ove previsto, audit di seconda e terza parte.

Miglioramento continuo. Il SGSI è sottoposto a un ciclo permanente di pianificazione, attuazione, verifica e azione correttiva. I risultati delle valutazioni dei rischi, degli audit, degli incidenti e dei riesami di direzione alimentano piani di adeguamento approvati dalla Direzione, assicurando che il livello di sicurezza progredisca in linea con l'evoluzione del contesto e delle minacce.

Segnalazione degli eventi di sicurezza. L'organizzazione promuove un ambiente in cui ogni persona è incoraggiata a segnalare tempestivamente eventi o sospetti di sicurezza, senza timore di conseguenze. A tal fine è stabilito un meccanismo di segnalazione attraverso canali dedicati, a supporto della rilevazione precoce e della risposta efficace agli incidenti.

Protezione degli asset in ogni contesto operativo. Gli asset informativi dell'organizzazione — dispositivi, supporti, dati — sono protetti indipendentemente dalla loro ubicazione. L'organizzazione riconosce che il lavoro da remoto, gli spostamenti e l'uso di dispositivi personali ampliano la superficie di esposizione e adotta controlli specifici quali la cifratura integrale dei dischi, l'autenticazione a più fattori e la cancellazione remota per mitigare tali rischi.

Scrivania pulita e schermo pulito. L'organizzazione adotta regole che impediscono l'esposizione di informazioni classificate negli ambienti di lavoro, richiedendo la custodia

sicura dei documenti cartacei e dei supporti rimovibili e il blocco automatico e manuale delle postazioni.

Archiviazione e aggiornamento

La presente politica è un documento controllato del SGSI e viene archiviata all'interno del sistema documentale dell'organizzazione secondo le modalità definite nella *PRO Procedura di gestione delle informazioni documentate* . Il **RSGSI Primary** ne assicura la revisione con cadenza almeno annuale, ovvero a seguito di cambiamenti significativi nell'organizzazione, nella tecnologia, nel contesto delle minacce o nel quadro normativo applicabile. Ogni aggiornamento è sottoposto all'approvazione del **Top Management** prima della diffusione. Una volta approvata, la politica è comunicata a tutte le articolazioni competenti dell'organizzazione e resa disponibile alle parti interessate esterne nei limiti della classificazione attribuita, tenuto conto della necessità di conoscere.

Documenti di riferimento

- POL Politica di sicurezza operativa
- POL Politica dei ruoli e delle responsabilità in materia di sicurezza delle informazioni
- POL Politica di classificazione ed etichettatura delle informazioni
- POL Politica di gestione del rischio
- PRO Procedura di gestione dei rischi
- PRO Procedura di gestione delle informazioni documentate
- PRO Procedura di gestione degli incidenti di sicurezza delle informazioni
- PRO Procedura di gestione delle risorse umane
- PRO Procedura di continuità operativa e di ripristino di emergenza
- PRO Procedura di gestione e controllo degli accessi logici
- PRO Procedura di sicurezza fisica e ambientale
- PRO Procedura di gestione della sicurezza della rete
- PRO Procedura di gestione degli acquisti e delle terze parti
- PRO Procedura di crittografia e gestione delle chiavi crittografiche
- PRO Procedura di configurazione, gestione e smaltimento degli asset