# POL Politica del sistema di gestione

## Storia della versione

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

## Indice

# Scopo

7networks Sagl riconosce che la protezione delle informazioni e dei dati rappresenta un elemento strategico inscindibile dalla propria missione di progettazione, integrazione, gestione e supporto di infrastrutture IT, soluzioni cloud e servizi di cybersecurity. La presente politica formalizza l'impegno della Direzione a perseguire un equilibrio sostenibile tra le esigenze di crescita economica e creazione di valore — proprie di un'azienda che opera nel mercato B2B dei servizi gestiti e della continuità operativa — e la salvaguardia della riservatezza, dell'integrità e della disponibilità degli asset informativi dell'organizzazione e dei propri clienti.

L'organizzazione si impegna altresì a promuovere una cultura del rispetto della normativa vigente in materia di sicurezza delle informazioni e protezione dei dati, incoraggiando la diffusione di comportamenti conformi ai principi legali e ai requisiti contrattuali applicabili presso tutto il personale, i collaboratori e le terze parti coinvolte.

# Campo di applicazione

La presente politica si applica a tutte le attività, i processi, i sistemi informativi e gli asset informatici di 7networks Sagl presso entrambe le sedi operative: l'ufficio principale di Via Cantonale 36, 6928 Manno, e il datacenter in colocation presso Bancadati SA, Centro Galleria 2, 6928 Manno. Coinvolge tutto il personale — dipendenti, collaboratori, consulenti e terze parti — indipendentemente dalla modalità e dal luogo di lavoro. Sono escluse le attività di sviluppo software, non rientranti nel perimetro dell'organizzazione.

# Riferimenti normativi

- ISO/IEC 27001:2022
- ISO/IEC 27002:2022
- ISO/IEC 27005
- LPD (Legge federale sulla protezione dei dati, Svizzera)
- Direttiva (UE) 2022/2555 (NIS2)

# 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.

- **Rischio** : effetto dell'incertezza sugli obiettivi, espresso come combinazione della probabilità di un evento e delle sue conseguenze.
- **Sistema di gestione** : insieme di elementi correlati o interagenti di un'organizzazione per stabilire politiche, obiettivi e processi per conseguire tali obiettivi.
- **Miglioramento continuo** : attività ricorrente finalizzata ad accrescere le prestazioni del sistema di gestione.

# Ruoli e responsabilità

- **RSGSI Primary** : sovrintende all'attuazione, al mantenimento e all'aggiornamento della presente politica, coordinandone la comunicazione interna e verificandone la coerenza con il contesto organizzativo.
- **RSGSI Secondary** : supporta il RSGSI Primary nel monitoraggio della conformità alla politica e contribuisce alla preparazione degli input per il riesame di direzione.
- **Cybersecurity e Protezione Dati** : sviluppa la strategia di cybersecurity e le misure di protezione dei dati in coerenza con i principi e gli obiettivi espressi nella presente politica.
- **Sistemi** : garantisce che le infrastrutture IT siano gestite in conformità agli indirizzi di sicurezza stabiliti dalla politica.
- **Network and Security** : assicura che le architetture di rete e i dispositivi di sicurezza operino in accordo con i principi di protezione qui definiti.
- **Backoffice** : cura l'archiviazione, la distribuzione controllata e la gestione documentale della presente politica.

# Impegno e obiettivi del sistema di gestione

## Impegno della Direzione

7networks Sagl è impegnata a stabilire e mantenere un Sistema di Gestione della Sicurezza delle Informazioni (SGSI) appropriato al proprio contesto competitivo — quello di un fornitore svizzero di servizi IT gestiti, soluzioni Microsoft Cloud e cybersecurity rivolto a piccole e medie imprese del Canton Ticino — e coerente con i propri indirizzi strategici. Tale impegno si traduce nelle seguenti dichiarazioni di intento:

L'organizzazione assicura la disponibilità di risorse adeguate — finanziarie, umane e tecnologiche — affinché il SGSI possa operare efficacemente e migliorare nel tempo. A tal fine promuove l'assegnazione del ruolo di **RSGSI Primary** con autorità diretta verso la Direzione, così che la governance della sicurezza delle informazioni mantenga un collegamento costante con le decisioni strategiche.

L'organizzazione è impegnata a soddisfare i requisiti applicabili in materia di sicurezza delle informazioni e protezione dei dati, siano essi di natura legislativa — in particolare la Legge federale sulla protezione dei dati e la Direttiva NIS2 — regolamentare o contrattuale, garantendo la conformità alle aspettative delle parti interessate rilevanti: clienti, partner tecnologici, enti di certificazione, autorità di vigilanza e personale interno.

L'organizzazione persegue il miglioramento continuo del SGSI attraverso un ciclo permanente di pianificazione, attuazione, verifica e azione correttiva, alimentato dai risultati delle valutazioni del rischio, degli audit interni, dell'analisi degli incidenti e dei riesami di direzione. I risultati di tali processi confluiscono in piani di miglioramento approvati dalla Direzione, affinché il livello di protezione evolva in linea con il panorama delle minacce e le trasformazioni dell'organizzazione.

## Obiettivi di sicurezza delle informazioni

La presente politica fornisce il quadro per la definizione e il riesame periodico degli obiettivi di sicurezza delle informazioni. In tale contesto, l'organizzazione si impegna a perseguire i seguenti indirizzi:

- Preservare la riservatezza, l'integrità e la disponibilità delle informazioni proprie e dei clienti lungo l'intero ciclo di vita del dato — dalla raccolta alla cancellazione sicura.
- Minimizzare la probabilità e l'impatto degli incidenti di sicurezza, assicurando rilevamento tempestivo, contenimento efficace e ripristino delle operazioni entro i tempi definiti nei piani di continuità operativa.
- Gestire i rischi per la sicurezza delle informazioni mediante un processo strutturato di valutazione e trattamento basato sulla metodologia Probabilità × Impatto, in coerenza con gli standard ISO 27005 e NIST.
- Garantire la conformità alle disposizioni legislative e regolamentari in materia di sicurezza delle informazioni e protezione dei dati personali vigenti nel contesto svizzero ed europeo.
- Promuovere la consapevolezza e la competenza di tutto il personale tramite programmi formativi annuali differenziati per ruolo.
- Assicurare la sicurezza della catena di fornitura monitorando i fornitori critici — in particolare i provider di datacenter e i distributori di prodotti IT — attraverso criteri di qualificazione, clausole contrattuali di sicurezza e verifiche periodiche.
- Integrare la sicurezza delle informazioni nella gestione dei progetti fin dalla fase iniziale, affinché i rischi siano identificati e trattati secondo il principio di security by design.

## Principi fondamentali

L'azione dell'organizzazione in materia di sicurezza delle informazioni è guidata dai seguenti principi:

- **Approccio basato sul rischio** — identificazione, valutazione e trattamento sistematico dei rischi in proporzione alla criticità degli asset e al contesto delle minacce.
- **Responsabilità condivisa** — ogni persona che accede a informazioni o sistemi contribuisce attivamente alla loro protezione.
- **Difesa in profondità** — controlli di sicurezza implementati su più livelli (organizzativo, fisico, logico, procedurale), così che il cedimento di un singolo controllo non comprometta la protezione complessiva.

- **Minimo privilegio e need to know** — accesso concesso esclusivamente nella misura strettamente necessaria alle mansioni assegnate, con revisione periodica e revoca tempestiva.
- **Conformità e legalità** — rispetto dei requisiti legislativi, regolamentari e contrattuali, verificato mediante audit interni e riesami di direzione.
- **Segnalazione degli eventi di sicurezza** — un ambiente nel quale tutto il personale è incoraggiato a segnalare tempestivamente eventi o sospetti attraverso canali dedicati, senza timore di conseguenze.
- **Protezione degli asset in ogni contesto operativo** — le informazioni e i dispositivi sono protetti indipendentemente dalla sede di lavoro, attraverso controlli specifici quali la crittografia, l'autenticazione a più fattori e la cancellazione remota.

### Comunicazione della politica

La presente politica, classificata come documento pubblico, è resa disponibile a tutto il personale dell'organizzazione tramite i canali interni di distribuzione controllata e agli stakeholder esterni — clienti, fornitori e organismi di certificazione — quale dimostrazione dell'impegno di 7networks Sagl verso la protezione delle informazioni. Il **RSGSI Primary** coordina la diffusione e ne verifica la presa visione da parte dei destinatari.

## Archiviazione e aggiornamento

La presente politica è archiviata in formato elettronico nell'ambiente SharePoint dell'organizzazione, con backup periodici a garanzia della disponibilità e leggibilità nel tempo. Il **RSGSI Primary** la sottopone a riesame almeno una volta all'anno, oppure a seguito di modifiche significative del contesto organizzativo, tecnologico, normativo o del panorama delle minacce. Ogni revisione comporta l'aggiornamento del numero di versione e della data, la sintesi delle modifiche nella tabella storica e la riapprovazione da parte della Direzione prima della ridistribuzione.

## Documenti di riferimento

- POL Politica di sicurezza delle informazioni
- PRO Processi direzionali
- PRO Procedura di gestione dei rischi
- PRO Gestione riesame della direzione
- PRO Procedura di gestione delle informazioni documentate