

POL Politica di sicurezza delle informazioni

Storia della versione

Versione	Data	Autore	Approvato da
1	09/06/2026	Luca Trecarichi	Biagio Passaro

Indice

- Scopo
- Campo di applicazione
- Riferimenti normativi
- Termini e definizioni
- Ruoli e responsabilità
- Obiettivi di sicurezza delle informazioni
- Principi fondamentali di sicurezza delle informazioni
- Protezione degli asset fuori sede
- Archiviazione e aggiornamento
- Documenti di riferimento

Scopo

VOISMART S.R.L. riconosce la sicurezza delle informazioni come un pilastro essenziale della propria attività di sviluppo software, progettazione e fornitura di soluzioni per le telecomunicazioni e di erogazione di servizi cloud SaaS. La presente politica formalizza l'impegno degli organi di amministrazione e direttivi verso la protezione del patrimonio informativo e definisce il quadro di riferimento per istituire, attuare, mantenere e migliorare continuamente il Sistema di Gestione della Sicurezza delle Informazioni, componente del Sistema di Gestione Integrato (SGI).

Attraverso questo documento l'organizzazione persegue la salvaguardia della riservatezza, dell'integrità e della disponibilità delle informazioni proprie, dei clienti e di tutte le parti interessate. VOISMART promuove una cultura della sicurezza fondata sull'approccio basato sul rischio, sulla responsabilità condivisa e sul miglioramento continuo, con l'obiettivo di sostenere gli indirizzi strategici aziendali e di consolidare la fiducia delle organizzazioni B2B e della pubblica amministrazione che si affidano ai propri prodotti e servizi.

La politica indirizza altresì le specificità dell'ambiente cloud computing, nel quale VOISMART opera sia come fornitore di servizi cloud sia come cliente di servizi cloud di terze parti, e recepisce gli obblighi in materia di cybersicurezza derivanti dalla normativa nazionale e dell'Unione Europea. Essa costituisce il documento apicale dal quale discendono le politiche tematiche e le procedure operative che compongono il sistema documentale di sicurezza dell'organizzazione.

Campo di applicazione

La presente politica si applica a tutte le attività, i processi, gli asset informativi, i sistemi informatici e di rete e le tre sedi operative di VOISMART S.R.L.: la sede legale e operativa di Via Benigno Crespi 57, 20159 Milano (MI), la sede operativa di Piazza Madre Teresa di Calcutta 48, 71042 Cerignola (FG) e la sede operativa di Strada Regionale 630 Km 28,4, 04020 Spigno Saturnia (LT). Coinvolge tutto il personale, inclusi dipendenti, collaboratori a contratto, consulenti e terze parti che accedono alle informazioni o ai sistemi aziendali, indipendentemente dalla sede di lavoro o dalla modalità operativa, compreso il lavoro da remoto. La politica copre inoltre i servizi cloud erogati da VOISMART in qualità di fornitore SaaS e quelli di cui l'organizzazione fruisce in qualità di cliente di servizi cloud.

Riferimenti normativi

- ISO/IEC 27001:2022
- ISO/IEC 27002:2022
- ISO/IEC 27017:2015
- Direttiva (UE) 2022/2555
- D.Lgs. 138/2024

- Regolamento (UE) 2016/679

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 di un'entità autorizzata.
- **Rischio** : effetto dell'incertezza sugli obiettivi.
- **Valutazione del rischio** : processo complessivo di identificazione, analisi e ponderazione del rischio.
- **Trattamento del rischio** : processo volto a modificare il rischio, che può includere l'adozione di controlli, l'accettazione, l'evitamento o il trasferimento.
- **Asset informativo** : qualsiasi elemento, materiale o immateriale, che abbia valore per l'organizzazione in relazione alla gestione delle informazioni.
- **Evento di sicurezza delle informazioni** : occorrenza identificata di uno stato di un sistema, servizio o rete che indica una possibile violazione della politica di sicurezza delle informazioni o un malfunzionamento dei controlli.
- **Incidente di sicurezza delle informazioni** : uno o più eventi di sicurezza delle informazioni indesiderati o inattesi che hanno una significativa probabilità di compromettere le operazioni aziendali e di minacciare la sicurezza delle informazioni.
- **Servizio cloud** : capacità erogata mediante cloud computing e resa disponibile tramite rete.
- **Multi-tenancy** : allocazione di risorse fisiche o virtuali tale che più clienti e i rispettivi dati ed elaborazioni siano isolati gli uni dagli altri.

Ruoli e responsabilità

- **Responsabile del sistema di gestione** : coordina l'attuazione, il mantenimento e il miglioramento continuo della sicurezza delle informazioni nell'ambito del SGI e promuove il riesame periodico della presente politica.
- **Technical Support Manager** : assicura che i principi di segnalazione e gestione degli eventi di sicurezza siano applicati nell'erogazione dei servizi di supporto tecnico.
- **PBX & Voice Product Development Lead** : integra i principi di sicurezza delle informazioni nelle attività di sviluppo dei prodotti PBX e di comunicazione unificata.
- **InPiazza Product Development Lead** : integra i principi di sicurezza delle informazioni nello sviluppo e nella manutenzione della piattaforma InPiazza.

- **PBX North Business Unit Manager** : assicura il rispetto dei principi di sicurezza delle informazioni da parte del personale della propria unità operativa nell'Italia settentrionale.
- **PBX South Business Unit Manager** : assicura il rispetto dei principi di sicurezza delle informazioni da parte del personale della propria unità operativa nell'Italia meridionale.
- **InPiazza Business Unit Manager** : assicura il rispetto dei principi di sicurezza delle informazioni da parte del personale dell'unità InPiazza.

Obiettivi di sicurezza delle informazioni

VOISMART definisce i propri obiettivi strategici di sicurezza delle informazioni in coerenza con il contesto operativo, gli indirizzi strategici e le aspettative delle parti interessate. Tali obiettivi orientano l'intero sistema di politiche e procedure di sicurezza e vengono riesaminati nell'ambito del riesame della direzione, come documentato nel *MOD Verbale di riesame della direzione*.

L'organizzazione si impegna a proteggere la riservatezza, l'integrità e la disponibilità delle informazioni lungo il loro intero ciclo di vita, garantendo livelli di protezione proporzionati alla classificazione e alla criticità di ciascun asset informativo. VOISMART adotta e mantiene un approccio sistematico alla gestione del rischio di sicurezza delle informazioni, fondato su una valutazione periodica delle minacce e delle vulnerabilità e sul trattamento tempestivo dei rischi che raggiungono o superano la soglia di accettabilità definita dall'organizzazione, coerentemente con la formula Probabilità per Impatto e con i livelli di rischio basso, medio e alto documentati nel *MOD Valutazione dei rischi di sicurezza delle informazioni*.

VOISMART persegue la piena conformità alla normativa vigente in materia di sicurezza informatica e protezione dei dati personali, con particolare riguardo agli obblighi derivanti dalla Direttiva NIS 2 e dal D.Lgs. 138/2024, e mantiene un *MOD Elenco norme* aggiornato per tracciare i requisiti legali e regolamentari applicabili. L'organizzazione intende inoltre garantire la sicurezza dei propri servizi cloud SaaS, preservando l'isolamento dei dati dei clienti in ambienti multi-tenant, la trasparenza dei controlli implementati e la resilienza dell'infrastruttura sottostante.

La promozione della consapevolezza e della competenza del personale rappresenta un ulteriore obiettivo prioritario: VOISMART si adopera affinché ogni collaboratore comprenda le proprie responsabilità e contribuisca attivamente alla protezione del patrimonio informativo, come monitorato attraverso la *MOD Matrice delle competenze*.

L'organizzazione persegue infine il miglioramento continuo del SGI mediante la definizione di piani di adeguamento fondati sugli esiti degli audit interni, del riesame della direzione e delle valutazioni di efficacia delle misure di sicurezza, i cui interventi confluiscono nel *MOD Programma di miglioramento*.

Principi fondamentali di sicurezza delle informazioni

Approccio basato sul rischio

VOISMART fonda ogni decisione in materia di sicurezza delle informazioni sulla valutazione sistematica dei rischi. L'organizzazione identifica le minacce e le vulnerabilità

che possono compromettere i propri asset informativi, ne stima la probabilità e l'impatto e adotta misure di trattamento proporzionate al livello di rischio rilevato. Le opzioni di trattamento comprendono la mitigazione, l'accettazione, l'evitamento e il trasferimento del rischio, secondo quanto stabilito nella *PRO Procedura di gestione dei rischi* e nella *POL Politica di gestione del rischio*. I risultati della valutazione alimentano la pianificazione dei controlli e vengono riesaminati con regolarità, affinché il profilo di rischio resti allineato all'evoluzione del contesto organizzativo, tecnologico e normativo.

Governance della sicurezza delle informazioni

L'organizzazione riconosce la sicurezza delle informazioni come responsabilità condivisa a ogni livello aziendale. Gli organi di amministrazione e direttivi approvano le politiche di sicurezza informatica e ne ricevono rendicontazione periodica, in conformità con le disposizioni del D.Lgs. 138/2024. VOISMAST mantiene una struttura organizzativa per la sicurezza informatica, i cui ruoli e responsabilità sono definiti nella *POL Politica dei ruoli e delle responsabilità in materia di sicurezza delle informazioni* e formalizzati nel *MOD Organigramma* e nel *MOD Mansionario*. Tale struttura include il punto di contatto e il suo sostituto per le interlocuzioni con l'Agenzia per la Cybersicurezza Nazionale, il referente CSIRT e gli eventuali sostituti. Ruoli e responsabilità vengono riesaminati e, ove opportuno, aggiornati periodicamente e in occasione di incidenti significativi, variazioni organizzative o mutamenti dell'esposizione alle minacce.

L'organizzazione adotta e documenta politiche di sicurezza informatica per almeno i seguenti ambiti:

- gestione del rischio
- ruoli e responsabilità
- affidabilità delle risorse umane
- conformità e audit di sicurezza
- gestione dei rischi della catena di approvvigionamento
- gestione degli asset
- gestione delle vulnerabilità
- continuità operativa, ripristino in caso di disastro e gestione delle crisi informatiche
- gestione dell'autenticazione, delle identità digitali e del controllo accessi
- sicurezza fisica
- formazione del personale e consapevolezza
- sicurezza dei dati
- sviluppo, configurazione, manutenzione e dismissione dei sistemi informativi e di rete
- protezione delle reti e delle comunicazioni
- monitoraggio degli eventi di sicurezza
- risposta agli incidenti e ripristino

Tali politiche sono rese note alle articolazioni competenti secondo il principio della necessità di conoscere.

Classificazione e uso accettabile delle informazioni

VOISMART classifica le proprie informazioni secondo livelli di riservatezza, come dettagliato nella *POL Politica di classificazione ed etichettatura delle informazioni*, e associa a ciascun livello specifici requisiti di protezione per il trattamento, la trasmissione e la conservazione. L'organizzazione promuove un uso responsabile e consapevole delle informazioni e di tutte le risorse associate, stabilendo regole di comportamento che ogni collaboratore è tenuto a conoscere e rispettare, coerentemente con quanto definito nella *POL Politica di sicurezza operativa* e nel *Codice di condotta*.

Controllo degli accessi

L'organizzazione adotta il principio del minimo privilegio e il controllo basato sui ruoli per garantire che ciascun utente acceda esclusivamente alle informazioni e ai sistemi necessari allo svolgimento delle proprie funzioni. Le modalità di gestione dell'intero ciclo di vita degli accessi sono definite nella *PRO Procedura di gestione e controllo degli accessi logici*, mentre il *Registro degli utenti autorizzati all'uso delle informazioni* documenta i sistemi, i repository e le tipologie di informazioni cui ciascun utente è abilitato.

Sicurezza del cloud computing

In qualità di fornitore di servizi cloud SaaS, VOISMART si impegna a proteggere i dati dei clienti negli ambienti multi-tenant, adottando controlli di isolamento, crittografia e gestione sicura del ciclo di vita delle istanze virtualizzate. L'organizzazione garantisce trasparenza verso i clienti in merito ai controlli di sicurezza implementati, alle giurisdizioni applicabili e alle modalità di gestione dei dati, e fornisce su richiesta evidenza della conformità alla normativa e ai requisiti contrattuali vigenti.

In qualità di cliente di servizi cloud, VOISMART valuta i rischi associati all'affidamento di informazioni e processi a fornitori esterni, verifica la conformità di tali fornitori ai requisiti di sicurezza dell'organizzazione e richiede idonee certificazioni, come stabilito nella *POL Politica di sicurezza del cloud* e nella *PRO Procedura di gestione degli acquisti e delle terze parti*.

Segnalazione degli eventi e gestione degli incidenti

VOISMART promuove una cultura in cui ogni persona è chiamata a segnalare tempestivamente gli eventi di sicurezza delle informazioni osservati o sospetti, attraverso i canali appropriati e senza timore di conseguenze per le segnalazioni in buona fede. L'organizzazione registra e traccia ogni evento nel *MOD Registro degli incidenti di sicurezza delle informazioni*, con informazioni che coprono la rilevazione, la classificazione della gravità, le azioni di contenimento, la risoluzione e l'analisi delle cause. Le modalità operative di risposta e i protocolli di notifica alle autorità competenti sono definiti nella *PRO Procedura di gestione degli incidenti di sicurezza delle informazioni*.

Conformità ai requisiti legali e contrattuali

L'organizzazione identifica, documenta e tiene costantemente aggiornato il quadro dei requisiti legali, regolamentari e contrattuali applicabili alla sicurezza delle informazioni, avvalendosi del *MOD Elenco norme* e della *PRO Procedura Obblighi di conformità*. In qualità di fornitore di servizi cloud, VOISMART informa i clienti delle giurisdizioni legali che governano il servizio e fornisce prova della propria conformità alla legislazione e ai requisiti contrattuali applicabili. In qualità di cliente di servizi cloud, l'organizzazione richiede ai propri fornitori evidenze di conformità, incluse certificazioni rilasciate da revisori terzi, consapevole che le responsabilità di conformità restano in capo al cliente del servizio cloud.

Sicurezza delle risorse umane

VOISMART integra la cybersicurezza nelle proprie pratiche di gestione delle risorse umane. Il personale autorizzato ad accedere ai sistemi informativi e di rete rilevanti è individuato previa valutazione dell'esperienza, delle capacità e dell'affidabilità, e gli amministratori di sistema sono designati con le medesime cautele. L'organizzazione prevede clausole contrattuali in materia di riservatezza e sicurezza informatica che restano valide anche dopo la cessazione del rapporto di lavoro, secondo quanto definito nella *PRO Procedura di gestione delle risorse umane*.

Protezione fisica e scrivania e schermo puliti

VOISMART protegge le proprie sedi e le aree critiche attraverso controlli di accesso fisico, sorveglianza e misure di protezione ambientale, come dettagliato nella *PRO Procedura di sicurezza fisica e ambientale*. L'organizzazione adotta il principio della scrivania e dello schermo puliti: i dispositivi si bloccano automaticamente dopo un periodo di inattività, i documenti riservati non vengono lasciati esposti sulle postazioni di lavoro e i supporti di memorizzazione rimovibili sono custoditi in modo sicuro.

Miglioramento continuo

VOISMART persegue il miglioramento continuo dell'efficacia del SGI e delle misure di sicurezza delle informazioni. L'organizzazione definisce, attua e aggiorna un piano di valutazione dell'efficacia delle misure di gestione del rischio per la sicurezza informatica, e informa periodicamente gli organi di amministrazione e direttivi sugli esiti di tale piano e dei piani di adeguamento. Gli audit interni, il riesame della direzione e le valutazioni di efficacia costituiscono le fonti primarie per l'identificazione degli interventi di miglioramento, i cui risultati vengono documentati nel *MOD Programma di miglioramento* e nel *MOD Rapporto di audit*.

Protezione degli asset fuori sede

VOISMART si impegna a proteggere gli asset informativi anche quando sono utilizzati al di fuori delle proprie sedi, riconoscendo che il lavoro da remoto, le trasferte e la collaborazione con terze parti espongono dispositivi e dati a rischi aggiuntivi rispetto

all'ambiente controllato degli uffici. I principi che seguono si applicano a tutti gli asset affidati al personale, inclusi notebook, dispositivi mobili e documenti aziendali. Le misure tecniche e le configurazioni specifiche a tutela degli asset in mobilità sono dettagliate nella *POL Politica di sicurezza operativa*.

Custodia e utilizzo. Il personale assegnatario di un asset è il primo responsabile della sua protezione. I dispositivi aziendali non sono lasciati incustoditi in veicoli, mezzi pubblici, aree comuni di strutture ricettive o spazi di coworking. In contesti di lavoro da remoto il collaboratore impedisce che terze persone, compresi i familiari, possano accedere ai dati o visualizzare lo schermo, e blocca il dispositivo ogni volta che si allontana dalla postazione, anche temporaneamente. L'assegnazione formale degli asset è tracciata nel *MOD Modulo di assegnazione dei beni*, che documenta la tipologia, il numero di serie, le condizioni d'uso e gli obblighi di sicurezza e riservatezza.

Comunicazioni e accesso alla rete. L'accesso alle risorse aziendali da postazioni esterne alle sedi dell'organizzazione avviene esclusivamente attraverso canali di comunicazione sicuri. Il personale si astiene dall'utilizzare reti pubbliche non protette per trattare informazioni aziendali di natura riservata, conformandosi alle regole stabilite nella *POL Politica di sicurezza operativa*.

Documenti cartacei. I documenti contenenti informazioni riservate sono conservati in modo sicuro al di fuori dei locali aziendali, custoditi in contenitori dotati di chiusura adeguata e, al rientro nella sede di lavoro, distrutti secondo le modalità previste dall'organizzazione.

Segnalazione di smarrimento, furto o danneggiamento. Il personale segnala tempestivamente qualunque smarrimento, furto o danneggiamento di un asset aziendale attraverso i canali previsti dalla *PRO Procedura di gestione degli incidenti di sicurezza delle informazioni*. La segnalazione attiva le misure di contenimento e l'evento viene registrato come incidente di sicurezza delle informazioni.

Restituzione. Al termine del rapporto di lavoro, del progetto o della trasferta, il personale restituisce gli asset aziendali attraverso il *MOD Modulo di restituzione dei beni*, che documenta la tipologia, il numero di serie e lo stato di conservazione di ciascun bene. La mancata restituzione può comportare responsabilità per il collaboratore.

Archiviazione e aggiornamento

La presente politica è un documento controllato del SGI, archiviato e gestito secondo le modalità definite nella *PRO Procedura di gestione delle informazioni documentate* e tracciato nel *MOD Elenco della documentazione*. Il **Responsabile del sistema di gestione** ne promuove il riesame con cadenza almeno annuale, nonché in occasione di evoluzioni del contesto normativo in materia di sicurezza informatica, incidenti significativi, variazioni organizzative o mutamenti dell'esposizione alle minacce e ai relativi rischi. In sede di riesame viene verificata almeno la conformità della politica alla normativa vigente in materia di sicurezza informatica e gli esiti sono conservati in un apposito registro.

Gli organi di amministrazione e direttivi approvano la presente politica e ogni suo aggiornamento, e ne autorizzano la diffusione alle articolazioni competenti dell'organizzazione, nel rispetto del principio della necessità di conoscere. La politica è

altresì resa disponibile alle parti interessate esterne secondo le modalità stabilite dall'organizzazione.

Documenti di riferimento

- POL Politica di gestione del rischio
- POL Politica di classificazione ed etichettatura delle informazioni
- POL Politica di sicurezza operativa
- POL Politica di sicurezza del cloud
- POL Politica dei ruoli e delle responsabilità in materia di sicurezza delle informazioni
- PRO Procedura di gestione dei rischi
- PRO Procedura di gestione degli incidenti di sicurezza delle informazioni
- PRO Procedura di gestione e controllo degli accessi logici
- PRO Procedura di gestione degli acquisti e delle terze parti
- PRO Procedura di gestione delle risorse umane
- PRO Procedura di sicurezza fisica e ambientale
- PRO Procedura di gestione delle informazioni documentate
- PRO Procedura Obblighi di conformità
- Codice di condotta
- MOD Organigramma
- MOD Mansionario
- MOD Verbale di riesame della direzione
- MOD Valutazione dei rischi di sicurezza delle informazioni
- MOD Elenco norme
- MOD Matrice delle competenze
- MOD Programma di miglioramento
- MOD Registro degli incidenti di sicurezza delle informazioni
- MOD Rapporto di audit
- MOD Elenco della documentazione
- MOD Modulo di assegnazione dei beni
- MOD Modulo di restituzione dei beni
- Registro degli utenti autorizzati all'uso delle informazioni