

# POL Politica di sicurezza delle informazioni

## Storia della versione

Versione	Data	Autore	Approvatore
1	13-01-2026	Tommaso Dembech	Cristina Piluso

## Scopo

Lo scopo della presente politica è dichiarare e comunicare l'impegno del Top Management verso la protezione degli asset informativi dell'organizzazione. Questo documento definisce il quadro di riferimento per istituire, attuare, mantenere e migliorare continuamente il Sistema di Gestione della Sicurezza delle Informazioni (SGSI), al fine di proteggere la riservatezza, l'integrità e la disponibilità delle informazioni e di supportare gli obiettivi strategici aziendali.

## Indice

- Campo di Applicazione
- Riferimenti Normativi
- Termini e Definizioni
- Ruoli e Responsabilità
- Obiettivi di sicurezza delle informazioni
- Principi fondamentali di sicurezza delle informazioni
- Archiviazione e Aggiornamenti
- Documenti di Riferimento

## Campo di Applicazione

La presente politica definisce i principi e gli obiettivi strategici per la sicurezza delle informazioni di Kronos Informatica S.r.l. e si applica a tutto il personale, ai collaboratori e alle terze parti che hanno accesso agli asset informativi aziendali. Il documento stabilisce il quadro di riferimento per il Sistema di Gestione della Sicurezza delle Informazioni (SGSI) in conformità con i requisiti della norma ISO/IEC 27001.

## Riferimenti Normativi

ISO/IEC 27001 - Sicurezza delle informazioni, cybersecurity e protezione della privacy – Sistemi di gestione della sicurezza delle informazioni – Requisiti.

Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (GDPR).

D.Lgs. 196/2003 (Codice in materia di protezione dei dati personali).

## Termini e Definizioni

- **Riservatezza** : La proprietà che le informazioni non siano rese disponibili o divulgate a individui, entità o processi non autorizzati.
- **Integrità** : La proprietà di salvaguardare l'accuratezza e la completezza degli asset e delle informazioni.
- **Disponibilità** : La proprietà di essere accessibile e utilizzabile su richiesta da un'entità autorizzata.

## Ruoli e Responsabilità

- **Top Management (CEO, Consigliere e Direttore Vendite)** : Assume la guida e la responsabilità del Sistema di Gestione della Sicurezza delle Informazioni, assicurandone l'allineamento con gli indirizzi strategici aziendali.
- **CEO** : Approva formalmente le politiche di sicurezza delle informazioni e ne autorizza l'emissione.
- **Responsabile del sistema di gestione** : Sviluppa, mantiene aggiornate, comunica e riesamina le politiche di sicurezza. Gestisce la documentazione del SGSI e coordina la gestione delle segnalazioni e degli incidenti di sicurezza.
- **IT Manager** : Assicura l'implementazione e l'applicazione tecnica delle regole di sicurezza, come le policy di uso accettabile e di schermo pulito, e collabora alla predisposizione dei canali per la segnalazione degli eventi di sicurezza.

## Obiettivi di sicurezza delle informazioni

Kronos Informatica S.r.l. si impegna a proteggere i propri asset informativi e quelli dei suoi clienti, garantendo la riservatezza, l'integrità e la disponibilità delle informazioni. Il Top Management (CEO, Consigliere e Direttore Vendite) assume la guida e la responsabilità del Sistema di Gestione della Sicurezza delle Informazioni (SGSI), assicurando che sia allineato con gli indirizzi strategici aziendali e conforme ai requisiti della norma ISO/IEC 27001:2022.

Gli obiettivi strategici per la sicurezza delle informazioni sono:

- **Protezione degli Asset Informativi** : Garantire che tutte le informazioni, sia interne che affidate ai clienti, siano protette da accessi non autorizzati, modifiche improprie e indisponibilità, attraverso un approccio basato sulla valutazione e sul trattamento del rischio.
- **Conformità Normativa e Contrattuale** : Assicurare il pieno rispetto delle leggi vigenti, delle normative applicabili (incluso il GDPR) e degli obblighi contrattuali sottoscritti con clienti e fornitori.

- **Resilienza Operativa** : Mantenere la continuità dei servizi erogati ai clienti e delle operazioni interne, anche a fronte di incidenti di sicurezza o eventi avversi, attraverso piani di continuità e ripristino.
- **Cultura della Sicurezza** : Promuovere una cultura della sicurezza a tutti i livelli dell'organizzazione, in cui ogni membro del personale sia consapevole delle proprie responsabilità e contribuisca attivamente alla protezione delle informazioni.
- **Miglioramento Continuo** : Monitorare, misurare e riesaminare periodicamente le prestazioni del SGSI per identificare opportunità di miglioramento e garantire la sua continua adeguatezza ed efficacia.

La presente politica fornisce il quadro di riferimento per la definizione e il riesame periodico di obiettivi misurabili, che vengono formalizzati e monitorati come descritto nella procedura "PRO Gestione riesame della direzione".

## Principi fondamentali di sicurezza delle informazioni

### Gestione e Revisione delle Politiche

La presente politica e le politiche specifiche per argomento costituiscono il vertice normativo del SGSI. Il **Responsabile del sistema di gestione** ha il compito di sviluppare e mantenere aggiornato il corpo delle politiche di sicurezza, assicurandone la coerenza e l'adeguatezza.

Tutte le politiche di sicurezza devono essere:

- **Approvate** : L'approvazione formale è di competenza del **CEO** , che ne autorizza l'emissione.
- **Pubblicate e Comunicate** : Devono essere rese disponibili e comunicate a tutto il personale e, ove pertinente, alle parti interessate esterne. La responsabilità della comunicazione è del **Responsabile del sistema di gestione**.
- **Riconosciute** : Il personale è tenuto a prendere visione e comprendere le politiche applicabili alla propria mansione. L'avvenuta presa visione è documentata come parte degli adempimenti legati al rapporto di lavoro.
- **Riesaminate** : Le politiche sono soggette a riesame con cadenza almeno annuale, o a seguito di cambiamenti significativi nel contesto aziendale, tecnologico o normativo. Tale attività è coordinata dal **Responsabile del sistema di gestione** e formalizzata nell'ambito della "PRO Gestione riesame della direzione".

### Uso Accettabile delle Risorse

Tutte le informazioni e le risorse associate, inclusi hardware, software, sistemi di rete e servizi cloud, sono di proprietà di Kronos Informatica S.r.l. e devono essere utilizzate esclusivamente per scopi aziendali autorizzati. L'uso di tali risorse è disciplinato dalle regole definite nella "POL Politica di sicurezza operativa" e dai principi etici stabiliti nel "Codice di condotta".

L' **IT Manager** deve assicurare che le regole per l'uso accettabile siano implementate e tecnicamente applicate ove possibile. Ogni dipendente è responsabile per la custodia e l'utilizzo corretto degli asset che gli sono stati assegnati. L'assegnazione è formalizzata tramite la firma del documento di trasporto, che avviene alla consegna del bene.

L'accesso alle informazioni e ai sistemi è basato sul principio del minimo privilegio e regolato in base al ruolo ricoperto, come definito nella "PRO Procedura dei ruoli e responsabilità" e gestito tramite la "PRO Procedura di gestione e controllo degli accessi logici".

### Protezione delle Postazioni di Lavoro e dei Beni

La protezione delle informazioni in formato fisico e digitale e dei beni aziendali è una responsabilità di tutto il personale.

- **Scrivania Libera (Clear Desk)** : Il personale deve assicurare che i documenti cartacei, specialmente se contenenti informazioni classificate come riservate, non siano lasciati incustoditi sulle scrivanie. Al di fuori dell'orario di lavoro o in caso di assenza prolungata, tali documenti devono essere riposti in armadi o cassettiere chiusi a chiave, in accordo con la "PRO Procedura di sicurezza fisica e ambientale".
- **Schermo Pulito (Clear Screen)** : Tutte le postazioni di lavoro fisse e mobili devono essere configurate con un blocco schermo automatico che si attiva dopo 5 minuti di inattività. È responsabilità di ogni utente bloccare manualmente la propria sessione (es. tramite **Win+L** o **Ctrl+Cmd+Q** ) ogni qualvolta si allontanano dalla postazione. L' **IT Manager** è responsabile dell'implementazione tecnica di tale controllo a livello di dominio.
- **Sicurezza dei Beni Fuori Sede** : Gli asset aziendali utilizzati al di fuori delle sedi di Kronos Informatica S.r.l., come laptop e smartphone, devono essere costantemente protetti da furto, smarrimento, danneggiamento e accessi non autorizzati. La responsabilità primaria della protezione fisica del bene ricade sull'assegnatario, formalizzato tramite il "MOD Modulo di assegnazione dei beni". Le direttive operative per la gestione di tali asset sono contenute nella "PRO Procedura di configurazione, gestione e smaltimento degli asset".

#### **Segnalazione degli Eventi di Sicurezza delle Informazioni**

Tutto il personale ha il dovere di segnalare tempestivamente qualsiasi evento di sicurezza delle informazioni osservato o sospetto, incluse anomalie di funzionamento dei sistemi, comportamenti imprevisti o potenziali debolezze di sicurezza.

L'organizzazione, tramite il **Responsabile del sistema di gestione** e l' **IT Manager** , deve mettere a disposizione canali chiari, noti e accessibili per effettuare le segnalazioni.

Le modalità di segnalazione e gestione sono dettagliate nella "PRO Procedura di gestione degli incidenti di sicurezza delle informazioni".

Ogni segnalazione ricevuta deve essere registrata e tracciata dal **Responsabile del sistema di gestione** all'interno del "MOD Registro degli incidenti di sicurezza delle informazioni" per la successiva analisi e risoluzione. Nessuna azione disciplinare sarà intrapresa nei confronti di chi segnala un evento in buona fede, anche se dovesse rivelarsi un falso allarme. La segnalazione è un atto di responsabilità fondamentale per la protezione dell'azienda.

## Archiviazione e Aggiornamenti

La presente politica è gestita in formato elettronico e archiviata secondo le procedure aziendali. È soggetta a riesame con cadenza almeno annuale, o a seguito di cambiamenti significativi, sotto il coordinamento del Responsabile del sistema di gestione. Ogni aggiornamento viene approvato dal CEO prima della sua pubblicazione e comunicazione a tutto il personale.

## Documenti di Riferimento

- PRO Gestione riesame della direzione
- POL Politica di sicurezza operativa
- Codice di condotta
- Documento di trasporto beni aziendali
- PRO Procedura dei ruoli e responsabilità
- PRO Procedura di gestione e controllo degli accessi logici
- PRO Procedura di sicurezza fisica e ambientale
- PRO Procedura di configurazione, gestione e smaltimento degli asset
- PRO Procedura di gestione degli incidenti di sicurezza delle informazioni
- MOD Registro degli incidenti di sicurezza delle informazioni

KRONOS INFORMATICA SRL  
Via E. Toti, 2 - 20123 Milano  
+39 02 8540 3176  
www.kronos.it

