# POL Politica di sicurezza delle informazioni

| | |
|---|---|
| **Nome della società** | Uno Communications |
| **Data di entrata in vigore** | 18/08/2024 |

## Storia della versione

| Versione | Data | Descrizione | Autore | Approvato da |
|---|---|---|---|---|
| 1 | 18/08/2024 | -- N / D -- | Carlo Capacci | Carlo Capacci |
| 2 | 09/09/2025 | -- N / D -- | Stefano Licandro | Carlo Capacci |

## 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

# 1. Campo di Applicazione

La presente politica definisce gli obiettivi strategici e i principi fondamentali per la sicurezza delle informazioni di Uno Communications. Il suo scopo è proteggere gli asset informativi aziendali, assicurare la conformità normativa e mantenere la fiducia di clienti e partner. Questa politica si applica a tutto il personale, ai collaboratori, ai processi di business e a tutte le risorse tecnologiche e informative gestite dall'azienda, sia all'interno delle sedi che in modalità di lavoro remoto.

# 2. Riferimenti Normativi

- **ISO/IEC 27001:2022**: Sistemi di gestione per la sicurezza delle informazioni — Requisiti.
- **Regolamento (UE) 2016/679 (GDPR)**: Regolamento Generale sulla Protezione dei Dati, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati.

# 3. Termini e Definizioni

- **Riservatezza**: Proprietà che assicura che le informazioni non siano rese disponibili o divulgate a individui, entità o processi non autorizzati.
- **Integrità**: Proprietà che salvaguarda l'accuratezza e la completezza delle informazioni e dei metodi di elaborazione, proteggendole da modifiche o cancellazioni non autorizzate.
- **Disponibilità**: Proprietà che assicura che le informazioni siano accessibili e utilizzabili su richiesta da un'entità autorizzata.

# 4. Ruoli e Responsabilità

- **Top Management**: Approva la politica di sicurezza delle informazioni, assegna le risorse e le responsabilità necessarie e garantisce l'allineamento tra gli obiettivi di sicurezza e la strategia aziendale.
- **Responsabile del Sistema di Gestione (SG)**: Mantiene e supervisiona il Sistema di Gestione della Sicurezza delle Informazioni (SGSI), assicura la conformità allo standard ISO/IEC 27001 e coordina le attività di audit e di miglioramento continuo.
- **IT Manager**: Progetta, implementa e gestisce le misure tecniche e organizzative per proteggere gli asset informativi, incluse le procedure di sicurezza, la gestione degli incidenti e la continuità operativa legata all'IT.
- **Utente Responsabile**: Rispetta le politiche di sicurezza delle informazioni aziendali, inclusa la corretta gestione delle password, la protezione dei dati e l'uso appropriato degli strumenti IT forniti.

# 5. Obiettivi di sicurezza delle informazioni

Uno Communications definisce i seguenti obiettivi strategici per la sicurezza delle informazioni, in linea con la propria missione di fornire soluzioni personalizzabili e garantire un alto livello di servizio. Il Top Management si impegna a perseguire tali obiettivi per proteggere gli asset informativi aziendali e mantenere la fiducia di clienti e partner.

Gli obiettivi fondamentali del Sistema di Gestione della Sicurezza delle Informazioni (SGSI) sono:

- **Riservatezza**: Garantire che l'accesso alle informazioni sia consentito esclusivamente al personale autorizzato. La protezione dei dati sensibili, dei segreti commerciali e delle informazioni dei clienti da accessi non autorizzati è una priorità assoluta.
- **Integrità**: Assicurare che le informazioni siano protette da modifiche non autorizzate, mantenendone l'accuratezza, la completezza e la coerenza. Solo le persone autorizzate possono modificare le informazioni.
- **Disponibilità**: Garantire che le informazioni e i servizi associati siano accessibili e utilizzabili su richiesta da parte degli utenti autorizzati, in accordo con le esigenze di business e gli accordi contrattuali.
- **Conformità**: Assicurare il pieno rispetto dei requisiti legali, statutari, regolamentari e contrattuali applicabili in materia di sicurezza delle informazioni e protezione dei dati personali.
- **Miglioramento Continuo**: Monitorare, riesaminare e migliorare costantemente l'efficacia del SGSI per adattarsi all'evoluzione delle minacce, delle vulnerabilità e del contesto aziendale.

Il Top Management ha la responsabilità di definire e riesaminare periodicamente questi obiettivi. Il Responsabile del Sistema di Gestione (SG) deve assicurare che tali obiettivi siano comunicati, compresi e perseguiti a tutti i livelli dell'organizzazione. Le modalità per la definizione, pianificazione e monitoraggio degli obiettivi sono dettagliate nel documento "PRO Obiettivi e pianificazione per il loro raggiungimento".

# 6. Principi fondamentali di sicurezza delle informazioni

## 6.1. Governance e Responsabilità

La presente politica e le politiche specifiche per argomento sono approvate dal Top Management. Il Responsabile del Sistema di Gestione (SG) deve assicurarne la pubblicazione, la comunicazione a tutto il personale e alle parti interessate rilevanti, e il riesame a intervalli pianificati, almeno annualmente, e ogni qualvolta si verifichino cambiamenti significativi. La gestione delle modifiche è disciplinata dalla "PRO Procedura di gestione del cambiamento".

Tutto il personale è tenuto a prendere visione e accettare formalmente la presente politica e i documenti ad essa correlati. La comunicazione avviene attraverso i canali aziendali ufficiali, come il portale interno, e una versione pubblica è disponibile sul sito web di Uno Communications.

## 6.2. Approccio Basato sul Rischio

Tutte le decisioni e le misure di sicurezza delle informazioni sono fondate su un processo strutturato di valutazione del rischio, volto a identificare, analizzare e trattare le minacce agli asset informativi. Tale processo è sotto la supervisione del Responsabile del Sistema di Gestione (SG) e dell'IT Manager, in accordo con la "PRO Procedura di gestione dei rischi".

## 6.3. Uso Accettabile delle Risorse

Tutte le risorse informative e tecnologiche di Uno Communications, inclusi hardware, software, dati e reti, devono essere utilizzate esclusivamente per scopi aziendali autorizzati e in modo responsabile. L'IT Manager definisce e implementa le regole per l'uso accettabile, che sono ulteriormente dettagliate nel "Codice di condotta" e nella "POL Politica di sicurezza operativa". Ogni Utente Responsabile è tenuto a rispettare tali regole e a proteggere le risorse assegnate da usi impropri.

### 6.4. Protezione degli Asset nelle Sedi Aziendali e in Remoto

La protezione degli asset informativi è un obbligo che si estende oltre i confini fisici dell'azienda.

- **Scrivania e Schermo Puliti (Clear Desk and Clear Screen)**: Ogni Utente Responsabile deve assicurare che le informazioni sensibili, sia in formato cartaceo che su supporti di memorizzazione rimovibili, non siano lasciate incustodite e siano conservate in modo sicuro. Le postazioni di lavoro devono essere bloccate quando lasciate incustodite. L'IT Manager deve implementare un blocco automatico dello schermo dopo un periodo di inattività massimo di 5 minuti. La gestione dei supporti è normata dalla "POL Politica di classificazione ed etichettatura delle informazioni".
- **Sicurezza degli Asset Fuori Sede**: Le stesse regole di sicurezza si applicano agli asset utilizzati al di fuori delle sedi aziendali (es. lavoro da remoto). Il personale che opera in remoto deve adottare le seguenti misure:
  - Utilizzare esclusivamente software antivirus approvato e mantenerlo costantemente aggiornato.
  - Assicurare che le reti domestiche siano protette da password robuste e che le credenziali predefinite dei dispositivi di rete siano state modificate.
  - È fatto divieto di disattivare o modificare i controlli di sicurezza forniti dall'azienda, come firewall o software di protezione.
  - L'uso della VPN aziendale è obbligatorio per la trasmissione di informazioni riservate su reti Wi-Fi pubbliche o non fidate.
  - L'Utente Responsabile è responsabile della protezione fisica dei dispositivi mobili contro furto, perdita o danneggiamento.

### 6.5. Segnalazione degli Eventi di Sicurezza

Tutto il personale ha la responsabilità di segnalare tempestivamente qualsiasi evento, debolezza o sospetto incidente di sicurezza delle informazioni. Le segnalazioni devono essere effettuate attraverso i canali designati dall'IT Manager. Ogni evento segnalato deve essere registrato e gestito secondo la "PRO Procedura di gestione degli incidenti di sicurezza delle informazioni" e tracciato nel "MOD Registro degli incidenti di sicurezza delle informazioni".

## 7. Archiviazione e Aggiornamenti

Il presente documento è gestito e archiviato all'interno del sistema di gestione documentale aziendale. Viene riesaminato con cadenza almeno annuale, o a seguito di cambiamenti significativi nel contesto organizzativo, tecnologico o normativo, per garantirne la continua idoneità, adeguatezza ed efficacia. Ogni aggiornamento è approvato dal Top Management.

# 8. Documenti di Riferimento

- Codice di condotta
- MOD Registro degli incidenti di sicurezza delle informazioni
- POL Politica di sicurezza operativa
- POL Politica di classificazione ed etichettatura delle informazioni
- PRO Obiettivi e pianificazione per il loro raggiungimento
- PRO Procedura di gestione del cambiamento
- PRO Procedura di gestione dei rischi
- PRO Procedura di gestione degli incidenti di sicurezza delle informazioni