Politica per la sicurezza delle informazioni

Versione	2
Lingua	IT
Data	10 ott 2025

INDICE

1. POLITICA

O3 Enterprise è un'azienda specializzata nello sviluppo di software nel settore medico. L'azienda riconosce l'importanza della sicurezza delle informazioni per garantire la fiducia dei clienti, la conformità alle normative di settore e la protezione dei dati sensibili.

Questa politica delinea il nostro impegno a salvaguardare la riservatezza, l'integrità e la disponibilità delle informazioni e delle *informazioni di identificazione personale* (PII) in conformità con gli standard ISO/IEC 27001:2022, ISO/IEC 27017:2021 e ISO/IEC 27018:2025 e le normative applicabili.

Questa politica si applica a tutti i processi gestiti dall'azienda e a tutti i dipendenti e terze parti che accedono o gestiscono informazioni aziendali.

Obblighi della Direzione:

- Implementare e mantenere un Sistema di Gestione della Sicurezza delle Informazioni (SGSI) conforme alle norme ISO/IEC 27001:2022, ISO/IEC 27017:2021 e ISO/IEC 27018:2025 e nel rispetto dei requisiti del Regolamento UE 2016/679;
- Adottare un approccio PDCA (Plan-Do-Check-Act) per migliorare continuamente il SGSI;
- Identificare, valutare e mitigare i rischi associati alla sicurezza delle informazioni e alla protezione delle *informazioni di identificazione personale* (PII);
- Garantire che tutti i processi di sviluppo software siano conformi ai requisiti normativi;
- Stabilire, attuare e mantenere controlli di sicurezza per proteggere i dati sensibili (es. controllo degli accessi, monitoraggio delle attività, ecc);
- Promuovere e sostenere la formazione continua e la sensibilizzazione del personale in materia di sicurezza delle informazioni e protezione dei dati sensibili.

Obblighi dei Dipendenti:

Ogni dipendente dell'azienda è tenuto a contribuire attivamente alla protezione delle informazioni e dei dati sensibili trattati nell'ambito delle proprie attività. In particolare, ciascun dipendente deve:

- Rispettare tutte le politiche, procedure e istruzioni operative relativa alla sicurezza delle informazioni e alla protezione dei dati trattati;
- Partecipare regolarmente ai programmi di formazione e sensibilizzazione promossi dall'azienda, al fine di mantenere un livello adeguato di consapevolezza sui rischi legati alla sicurezza delle informazioni e alla protezione dei dati personali;
- Segnalare tempestivamente eventuali incidenti, anomalie o sospette violazioni della sicurezza delle informazioni;
- Rispettare tutte le normative vigenti, politiche interne e i requisiti contrattuali.

O3 Enterprise adotta un approccio proattivo nella gestione degli incidenti di sicurezza, con processi volti a:

- Rilevare e segnalare violazioni e vulnerabilità;
- Indagare su ogni incidente e implementare azioni correttive;
- Mantenere un registro degli incidenti per analisi e miglioramento continuo.

Questa politica sarà rivista periodicamente per garantire la conformità alle normative applicabili e ai requisiti aziendali.

2. IMPEGNO DELLA DIREZIONE

Poiché ci viene affidato il trattamento di informazioni sensibili (dei pazienti) e di risorse aziendali riservate, la Direzione di O3 Enterprise ritiene fermamente che la nostra reputazione e il nostro successo dipendono dalla salvaguardia delle nostre informazioni e di quelle dei nostri clienti.
La divulgazione non autorizzata di informazioni riservate potrebbe avere conseguenze negative per la nostra organizzazione, esponendoci a rischi legali. Analogamente, eventuali danni ai dati su cui facciamo affidamento per il processo decisionale aziendale e i processi produttivi, o ritardi nell'accesso a informazioni critiche, sarebbero inaccettabili.

Confermiamo la nostra intenzione di trattare la sicurezza delle informazioni come parte integrante della nostra cultura.

Dimostriamo il nostro impegno per una forte sicurezza nei seguenti modi:

- Istituendo un sistema che consenta ai dipendenti di suggerire nuove politiche o misure di sicurezza;
- Identificando nel CEO il ruolo di responsabile della sicurezza;
- Stabilendo e comunicando politiche, standard e processi di sicurezza chiari e allineati con la direzione strategica dell'organizzazione;
- Garantendo che i requisiti e i controlli del SGSI siano integrati nei processi dell'organizzazione;
- Agendo come modelli di conformità alle politiche di sicurezza;
- Rilevando e affrontando prontamente le violazioni delle politiche di sicurezza;
- Dirigendo e supportando le persone direttamente coinvolte nella sicurezza delle informazioni e nel SGSI;

- Revisionando regolarmente e migliorando continuamente il nostro programma di sicurezza delle informazioni;
- Predisponendo risorse adeguate — umane, tecniche e finanziarie — per l'attuazione, il mantenimento e miglioramento continuo del SGSI e dei sistemi di protezione dei dati personali e sensibili.