Politica per la Sicurezza delle Informazioni

La presente politica definisce l'impegno di **INFOTECH SYSTEM SRL** per la protezione da tutte le minacce, interne o esterne, intenzionali o accidentali, del proprio patrimonio informativo e di quello dei propri clienti, secondo le indicazioni dello standard internazionale ISO/IEC 27001.

Il campo di applicazione del SGSI implementato comprende:

L'azienda opera nella commercializzazione di prodotti hardware, software e servizi informatici, offrendo ai clienti un supporto completo nella scelta, implementazione e gestione delle soluzioni tecnologiche più adatte. In questo ambito, eroga servizi di assistenza sistemistica sia reattiva sia proattiva, avvalendosi di strumenti di monitoraggio continuo e di un service desk dedicato, con l'obiettivo di garantire continuità operativa, tempestività di intervento e affidabilità delle infrastrutture IT.

L'attività comprende inoltre la progettazione, realizzazione e gestione di infrastrutture di rete, soluzioni di Office Automation e sistemi di unified communications, supportando le organizzazioni nel miglioramento dell'efficienza, della collaborazione e della connettività aziendale. A completamento dell'offerta, l'azienda fornisce consulenza specialistica e implementa soluzioni avanzate in ambito cybersicurezza, vulnerability assessment e business continuity, con un approccio orientato alla protezione dei dati, alla riduzione dei rischi e alla resilienza dei sistemi informativi.

Particolare rilievo è attribuito anche alla progettazione e implementazione di soluzioni On Premise e Cloud per accompagnare le imprese nei percorsi di evoluzione e modernizzazione tecnologica. L'azienda eroga infine servizi in modalità e Managed Service Provider, proponendosi come partner tecnologico qualificato per la gestione continuativa e strategica dell'infrastruttura informatica del cliente.

La Direzione si impegna quindi personalmente e con tutta la struttura aziendale a sviluppare e mantenere attivo un sistema di gestione per la sicurezza delle informazioni nell'ambito delle attività svolte e dei servizi erogati alla propria clientela, nel rispetto dei seguenti principi generali di sicurezza delle informazioni:

- **Riservatezza:** Garantire che le informazioni proprie e dei clienti siano accessibili solo ai soggetti e/o ai processi regolarmente autorizzati;
- **Integrità:** Salvaguardare le informazioni proprie e dei clienti da modifiche o cancellazioni a seguito di errori o di azioni volontarie o involontarie, così come da malfunzionamenti o danni dei sistemi tecnologici, e garantirne l'accuratezza e la completezza;
- **Disponibilità:** Assicurare che gli utenti autorizzati abbiano accesso alle informazioni e alle risorse quando necessario e richiesto;
- **Conformità:** Rispettare i requisiti legali, normativi (GDPR, ISO 27001) e contrattuali con i clienti.

La Direzione è attiva in prima persona nell'impegno di coinvolgimento, formazione e responsabilizzazione delle risorse umane che lavorano in azienda e che collaborano con essa a vario titolo, affinché tutti partecipino con attenzione all'applicazione scrupolosa e puntuale delle procedure di protezione delle informazioni.

La Direzione si impegna quindi, e garantisce le risorse economiche e di tempo per identificare, valutare e trattare i rischi di sicurezza delle informazioni periodicamente (almeno annualmente), e ad adottare coerenti controlli di sicurezza (tecnici, organizzativi, fisici) proporzionati al rischio, basati sull'Allegato A della ISO 27001.

In quest'ottica promuove per il proprio personale e collaboratori frequenti momenti di formazione e sensibilizzazione periodica per tutto il personale sulla sicurezza informatica (phishing, gestione password, ecc.), e sottoscrizione di accordi di riservatezza (NDA) per dipendenti e collaboratori.

A livello tecnico, nel dettaglio la nostra azienda adotta i seguenti principi di precauzione:

- "minimo privilegio": gli accessi sono concessi solo per le attività strettamente necessarie;
- autenticazione obbligatoria a due fattori (2FA/MFA) e password complesse;
- Integrazione della sicurezza sin dalla fase di progettazione del software, degli impianti sistemistici e delle architetture cloud (Secure by Design);
- Adozione delle misure di sicurezza coerenti con la valutazione dei rischi, al fine di mantenere i rischi a livelli definiti accettabili e compatibili con le risorse disponibili e con i livelli di competitività aziendali;
- Gestione rigorosa dei cambiamenti (Change Management) e aggiornamento regolare dei sistemi (Patch Management);
- Segnalazione immediata di qualsiasi evento anomalo, incidente, vulnerabilità o potenziale violazione di sicurezza al Security Officer/IT Manager;
- Garantire con adeguate procedure di sicurezza la business continuity aziendale e la capacità di disaster recovery e situazioni di emergenza in generale.

La INFOTECH SYSTEM SRL si impegna a condividere con le parti interessate interne ed esterne la propria Politica per la sicurezza delle informazioni, a riesaminarla periodicamente durante gli audit interni e il riesame della direzione e ad aggiornarla in base agli sviluppi aziendali, al miglioramento del ISMS e alle misure tecniche e organizzative adottate per la sicurezza delle informazioni.

Venaria, 30 Marzo 2026

LA DIREZIONE