DOC 5 – POLITICA AZIENDALE DI GESTIONE DEI SERVIZI IT

N° REVISIONE	DATA	PAGG. REV	REDAZIONE	VERIFICA	APPROVAZIONE
REV. 0	31/01/2025				
REV. 1	13/02/2026				

Sommario

POLITICA

Il presente documento definisce la Politica Aziendale riguardante gli aspetti del Sistema di Gestione Integrato di SINCON.

Il documento è redatto dalla Direzione Aziendale ed ha lo scopo di definire gli obiettivi e le misure adottate al fine di conseguire, in linea con le norme:

- ISO/IEC 20000-1:2018 (Sistema di Gestione dei Servizi IT)
- ISO/IEC 27001:2022 (Sistema di Gestione della Sicurezza delle Informazioni)
- ISO 9001:2015 (Sistema di Gestione per la Qualità)
- Direttiva (UE) 2022/2555 – NIS 2 e normativa nazionale di recepimento

uno standard coerente con le certificazioni conseguite per l'erogazione di specifici servizi, in modo tale da essere di supporto al business e al raggiungimento degli obiettivi strategici aziendali.

Impegno della Direzione

L'Azienda si prefigge di:

- Pianificare, progettare, erogare, monitorare, mantenere e migliorare continuamente il Sistema di Gestione Integrato;
- Implementare e mantenere un SGS-IT conforme alle direttive ISO/IEC 20000-1:2018;
- Garantire la sicurezza delle informazioni in conformità alla ISO/IEC 27001:2022;
- Assicurare la qualità dei processi secondo ISO 9001:2015;
- Garantire la resilienza operativa e la gestione del rischio cyber in conformità ai requisiti della Direttiva NIS 2.

Tali obiettivi vengono perseguiti mediante le seguenti azioni:

- Miglioramento dell'efficacia nell'erogazione dei servizi attraverso una qualificazione costante delle risorse impiegate e la valutazione di percorsi formativi idonei allo standard pianificato dei servizi erogati;
- Miglioramento dell'efficienza, qualità, affidabilità, puntualità e dinamicità dei processi mediante costante monitoraggio, con particolare focus su Business Continuity e Capacity Plan;

- Adozione di politiche di sviluppo sicuro del software (Secure SDLC);
- Utilizzo di contromisure tecnologiche e organizzative per prevenire incidenti di sicurezza delle informazioni;
- Miglioramento continuo dei servizi tramite sistemi strutturati di raccolta feedback clienti per incrementare la Customer Satisfaction;
- Coinvolgimento attivo del personale affinché riconosca l'importanza del proprio ruolo;
- Rispetto della legislazione cogente e delle normative applicabili in materia di qualità, sicurezza delle informazioni, protezione dei dati e sicurezza delle reti e dei sistemi informativi;
- Comunicazione della politica a tutte le parti interessate e sensibilizzazione di fornitori, collaboratori e partner al rispetto del SGI-IT.

Impegni specifici in materia di Sicurezza delle Informazioni

La Direzione si impegna ad assicurare che:

- Le informazioni siano protette da accessi non autorizzati nel rispetto della riservatezza;
- Le informazioni siano disponibili agli utenti autorizzati quando necessario;
- Le informazioni siano salvaguardate da modifiche non autorizzate (integrità);
- Siano predisposti, mantenuti e testati piani di Business Continuity e Disaster Recovery;
- Il personale riceva adeguato addestramento sulla sicurezza delle informazioni;
- Tutte le violazioni e vulnerabilità siano tempestivamente segnalate e gestite.

Integrazione dei requisiti NIS 2

In coerenza con la Direttiva NIS 2, SINCON si impegna inoltre a:

- Adottare un approccio strutturato alla gestione del rischio cyber basato su analisi, valutazione e trattamento dei rischi;
- Implementare misure tecniche, operative e organizzative adeguate e proporzionate alla gestione dei rischi di sicurezza delle reti e dei sistemi informativi;
- Garantire capacità di prevenzione, rilevazione, risposta e ripristino da incidenti informatici;
- Stabilire procedure di gestione e notifica degli incidenti significativi alle Autorità competenti nei tempi previsti dalla normativa;

- Rafforzare la sicurezza della supply chain e dei fornitori critici;
- Garantire la responsabilizzazione del management sui temi di sicurezza informatica e resilienza;
- Promuovere la cultura della cybersicurezza a tutti i livelli aziendali;
- Assicurare monitoraggio continuo delle minacce e miglioramento costante delle misure di protezione.

CAMPO DI APPLICAZIONE

La presente politica si applica a tutti i settori e a tutti i processi aziendali coinvolti nell'erogazione dei seguenti servizi:

1. Servizi di Assistenza Hardware e Software di Base;
2. Supporto Specialistico applicativo ed operativo su applicativi software relativi a processi amministrativi e sanitari;
3. Gestione e conduzione Data Center;
4. System Management in ambienti Cloud.

Campo di applicazione ISO/IEC 27001:2022

Il Sistema di Gestione della Sicurezza delle Informazioni si applica a:

- Tutti gli asset informativi aziendali (informazioni, dati, sistemi, infrastrutture, applicazioni, reti);
- Tutto il personale interno, collaboratori, consulenti e fornitori che trattano informazioni aziendali;
- Tutte le sedi operative e ambienti IT, inclusi ambienti cloud e data center;
- Tutti i processi aziendali che comportano trattamento di informazioni o gestione di sistemi informativi.

Campo di applicazione NIS 2

Il perimetro di applicazione include le reti e i sistemi informativi utilizzati per l'erogazione dei servizi digitali e infrastrutturali critici, nonché le relazioni con fornitori e partner rilevanti ai fini della sicurezza e continuità operativa.

RESPONSABILITA’

Le figure responsabili dell’attuazione della presente politica sono:

Direzione Aziendale

- Definisce gli obiettivi strategici;
- Mette a disposizione mezzi e risorse;
- Approva le politiche di gestione del rischio e sicurezza;
- Supervisiona la conformità ai requisiti ISO e NIS 2;
- Garantisce la responsabilità e il coinvolgimento del management in materia di cybersecurity.

Responsabile del Sistema di Gestione Aziendale

- Coordina e monitora l’attuazione del SGI-IT;
- Verifica l’applicazione delle procedure;
- Supervisiona analisi dei rischi, controlli e audit;
- Coordina la gestione degli incidenti di sicurezza.

Responsabile Sicurezza delle Informazioni / Cybersecurity

- Monitora minacce e vulnerabilità;
- Gestisce il processo di incident management;
- Supporta la Direzione nella conformità NIS 2;
- Cura la reportistica verso le Autorità competenti ove richiesto.

Personale Aziendale

- Opera nel rispetto delle procedure;
- Partecipa ai programmi di formazione;
- Segnala tempestivamente anomalie o incidenti.

Fornitori e Clienti

- Sono tenuti a rispettare i requisiti di sicurezza e continuità previsti contrattualmente;
- Devono collaborare nella gestione di eventuali incidenti che impattano sui servizi.

RIESAME

Con cadenza almeno annuale la Direzione effettua il riesame della politica.

Durante il riesame vengono analizzati:

- Raggiungimento degli obiettivi;
- Prestazioni dei servizi;
- Indicatori di sicurezza e incidenti;
- Risultati di audit interni ed esterni;
- Evoluzione del contesto normativo;
- Adeguatezza delle misure di gestione del rischio cyber.

Il riesame valuta l'efficacia del Sistema di Gestione Integrato e individua eventuali azioni di miglioramento.

OBIETTIVI AZIENDALI

Annualmente la Direzione individua obiettivi misurabili coerenti con:

- Qualità del servizio;
- Continuità operativa;
- Sicurezza delle informazioni;
- Resilienza cyber e conformità NIS 2;
- Soddisfazione del cliente;
- Miglioramento continuo.

Gli obiettivi sono formalizzati nel documento:

DOC 5 - POLITICA AZIENDALE – APPENDICE – ANNO.docx

reso disponibile a tutto il personale nell'area documentale aziendale.