ALLEGATO 2 - POLITICA AZIENDALE

La **Politica Aziendale** impone che, in coerenza con la missione aziendale, la gestione di tutti i processi aziendali sia impostata con le regole proprie dell'applicazione del Sistema di gestione secondo la norma **ISO/IEC 27001:2022**, integrata dai controlli specifici per la sicurezza dei servizi cloud delle norme **ISO/IEC 27017** e **ISO/IEC 27018** e dai principi di gestione della qualità della norma **ISO 9001**, in un'ottica di sistema di gestione integrato.

SCOPO E OBIETTIVI

La direzione di **SINTE SRL** ha definito, ha divulgato e si impegna a mantenere attiva a tutti i livelli della propria organizzazione la presente politica per la Gestione della Sicurezza delle Informazioni.

Lo scopo della presente policy è di garantire la tutela e la protezione da tutte le minacce, interne o esterne, intenzionali o accidentali, delle informazioni nell'ambito delle proprie attività in accordo con le indicazioni fornite dallo standard ISO/IEC 27001 e dalle linee guida contenute nello standard ISO/IEC 27002, nonché con i controlli aggiuntivi per la sicurezza dei servizi cloud (ISO/IEC 27017) e per la protezione dei dati personali (PII) trattati in ambiente cloud (ISO/IEC 27018), nelle loro ultime versioni. La gestione è inoltre integrata con i principi di gestione della qualità della norma ISO 9001, al fine di assicurare l'orientamento al cliente, l'approccio per processi e il miglioramento continuo del Sistema di Gestione.

CAMPO DI APPLICAZIONE

La presente politica si applica indistintamente a tutti gli organi e i livelli dell'Azienda.

L'attuazione della presente politica è obbligatoria per tutto il personale e deve essere inserita nella regolamentazione degli accordi con qualsiasi soggetto esterno che, a qualsiasi titolo, possa essere coinvolto con il trattamento di informazioni che rientrano nel campo di applicazione del Sistema di Gestione (SGSD), inclusi i fornitori di servizi cloud (cloud service provider) e i relativi sub-fornitori.

L'azienda consente la comunicazione e la diffusione delle informazioni verso l'esterno solo per il corretto svolgimento delle attività aziendali che devono avvenire nel rispetto delle regole e delle norme cogenti.

POLICY SICUREZZA DELLE INFORMAZIONI

Il patrimonio informativo da tutelare è costituito dall'insieme delle informazioni gestite attraverso i servizi forniti e localizzate in tutte le sedi dell'azienda e presso i servizi cloud utilizzati.

È necessario assicurare:

- la **confidenzialità** delle informazioni: ovvero le informazioni devono essere accessibili solo da chi è autorizzato;
- l'**integrità** delle informazioni: ovvero proteggere la precisione e la completezza delle informazioni e dei metodi per la loro elaborazione;
- la **disponibilità** delle informazioni: ovvero che gli utenti autorizzati possano effettivamente accedere alle informazioni e ai beni collegati nel momento in cui lo richiedono.

La mancanza di adeguati livelli di sicurezza può comportare il danneggiamento dell'immagine aziendale, la mancata soddisfazione del cliente, il rischio di incorrere in sanzioni legate alla violazione delle normative vigenti nonché danni di natura economica e finanziaria.

Un adeguato livello di sicurezza è altresì basilare per la condivisione delle informazioni.

L'azienda identifica tutte le esigenze di sicurezza tramite l'analisi dei rischi che consente di acquisire consapevolezza sul livello di esposizione a minacce del proprio sistema informativo, inclusi i rischi specifici derivanti dall'utilizzo di servizi cloud. La valutazione del rischio permette di valutare le potenziali conseguenze e i danni che possono derivare dalla mancata applicazione di misure di sicurezza al sistema informativo e quale sia la realistica probabilità di attuazione delle minacce identificate.

I risultati di questa valutazione determinano le azioni necessarie per gestire i rischi individuati e le misure di sicurezza più idonee.

I principi generali della gestione della sicurezza delle informazioni abbracciano vari aspetti:

- Deve esistere un catalogo costantemente aggiornato degli asset aziendali rilevanti ai fini della gestione delle informazioni e per ciascuno deve essere individuato un responsabile. Le informazioni devono essere classificate in base al loro livello di criticità, in modo da essere gestite con livelli di riservatezza ed integrità coerenti ed appropriati.
- Per garantire la sicurezza delle informazioni, ogni accesso ai sistemi deve essere sottoposto a una procedura d'identificazione e autenticazione. Le autorizzazioni di accesso alle informazioni devono essere differenziate in base al ruolo ed agli incarichi ricoperti dai singoli individui, in modo che ogni utente possa accedere alle sole informazioni di cui necessita, e devono essere periodicamente sottoposte a revisione.
- Devono essere definite delle procedure per l'utilizzo sicuro dei beni aziendali e delle informazioni e dei loro sistemi di gestione.
- Deve essere incoraggiata la piena consapevolezza delle problematiche relative alla sicurezza delle informazioni in tutto il personale (dipendenti e collaboratori) a partire dal momento della selezione e per tutta la durata del rapporto di lavoro.
- Per poter gestire in modo tempestivo gli incidenti, tutti devono notificare qualsiasi problema relativo alla sicurezza. Ogni incidente deve essere gestito come indicato nelle procedure.
- È necessario prevenire l'accesso non autorizzato alle sedi e ai singoli locali aziendali dove sono gestite le informazioni e deve essere garantita la sicurezza delle apparecchiature.
- Deve essere assicurata la conformità con i requisiti legali e con i principi legati alla sicurezza delle informazioni nei contratti con le terze parti.
- Deve essere predisposto un piano di continuità che permetta all'azienda di affrontare efficacemente un evento imprevisto, garantendo il ripristino dei servizi critici in tempi e con modalità che limitino le conseguenze negative sulla missione aziendale.
- Gli aspetti di sicurezza devono essere inclusi in tutte le fasi di progettazione, sviluppo, esercizio, manutenzione, assistenza e dismissione dei sistemi e dei servizi informatici.
- Devono essere garantiti il rispetto delle disposizioni di legge, di statuti, regolamenti o obblighi contrattuali e di ogni requisito inerente la sicurezza delle informazioni, riducendo al minimo il rischio di sanzioni legali o amministrative, di perdite rilevanti o danni alla reputazione.

SICUREZZA DEI SERVIZI CLOUD (ISO/IEC 27017 E ISO/IEC 27018)

In relazione all'utilizzo e all'erogazione di servizi cloud, l'azienda adotta controlli specifici, in coerenza con le norme ISO/IEC 27017 e ISO/IEC 27018:

- devono essere chiaramente definite e formalizzate le responsabilità in materia di sicurezza tra l'azienda (in qualità di cliente cloud) e il fornitore del servizio (cloud service provider), secondo il modello di responsabilità condivisa;

- devono essere garantite la segregazione e l'isolamento degli ambienti virtuali e dei dati dei diversi clienti nelle infrastrutture cloud condivise;
- gli accessi amministrativi e privilegiati ai servizi cloud devono essere gestiti, monitorati e tracciati, con particolare attenzione alle operazioni degli amministratori;
- deve essere garantita la corretta rimozione o restituzione dei dati al termine del contratto di servizio cloud, evitando ripristini non autorizzati delle informazioni;
- devono essere note e documentate l'ubicazione geografica e la giurisdizione in cui i dati, inclusi i dati personali (PII), sono trattati e conservati;
- il trattamento dei dati personali in cloud deve avvenire limitatamente alle finalità concordate con il cliente, garantendo trasparenza, la gestione delle richieste degli interessati e la tempestiva notifica in caso di violazione dei dati (data breach);
- devono essere attivati adeguati strumenti di monitoraggio, logging e gestione degli eventi relativi ai servizi cloud.

QUALITÀ E MIGLIORAMENTO CONTINUO (ISO 9001)

In coerenza con i principi di gestione della qualità della norma ISO 9001, l'azienda adotta un sistema di gestione integrato orientato a:

- l'orientamento al cliente, garantendo che i requisiti dei clienti e i requisiti cogenti applicabili siano compresi e soddisfatti in modo costante;
- un approccio per processi, in cui le attività sono gestite come processi correlati che contribuiscono al raggiungimento degli obiettivi aziendali;
- il miglioramento continuo delle prestazioni, attraverso il ciclo Plan-Do-Check-Act (PDCA) e l'analisi dei dati e degli indicatori;
- un processo decisionale basato su evidenze oggettive e sulla valutazione dei rischi e delle opportunità;
- il coinvolgimento e la responsabilizzazione del personale a tutti i livelli dell'organizzazione.

RESPONSABILITÀ DI OSSERVANZA E ATTUAZIONE

L'osservanza e l'attuazione delle policies sono responsabilità di:

1- Tutto il personale che, a qualsiasi titolo, collabora con l'azienda ed è in qualche modo coinvolto con il trattamento di dati ed informazioni che rientrano nel campo di applicazione del Sistema di Gestione.

Tutto il personale è altresì responsabile della segnalazione di tutte le anomalie e violazioni di cui dovesse venire a conoscenza.

2- Tutti i soggetti esterni che intrattengono rapporti e collaborano con l'azienda, che devono garantire il rispetto dei requisiti contenuti nella presente policy.

Il Responsabile del Sistema di Gestione nell'ambito del Sistema di Gestione e attraverso norme e procedure appropriate, deve:

- condurre l'analisi dei rischi con le opportune metodologie e adottare tutte le misure per la gestione del rischio;
- stabilire tutte le norme necessarie alla conduzione sicura di tutte le attività aziendali;
- verificare le violazioni alla sicurezza e adottare le contromisure necessarie e controllare l'esposizione dell'azienda alle principali minacce e rischi;

- organizzare la formazione e promuovere la consapevolezza del personale per tutto ciò che concerne la sicurezza delle informazioni;
- verificare periodicamente l'efficacia e l'efficienza del Sistema di Gestione.

Chiunque, dipendenti, consulenti e/o collaboratori esterni dell'Azienda, in modo intenzionale o riconducibile a negligenza, disattenda le regole di sicurezza stabilite e in tal modo provochi un danno all'azienda, potrà essere perseguito nelle opportune sedi e nel pieno rispetto dei vincoli di legge e contrattuali.

RIESAME

La Direzione verificherà periodicamente e regolarmente o in concomitanza di cambiamenti significativi l'efficacia e l'efficienza del Sistema di Gestione, in modo da assicurare un supporto adeguato all'introduzione di tutte le migliorie necessarie e in modo da favorire l'attivazione di un processo continuo, con cui viene mantenuto il controllo e l'adeguamento della policy in risposta ai cambiamenti dell'ambiente aziendale, del business, delle condizioni legali.

Il Responsabile del Sistema di Gestione ha la responsabilità del riesame della politica.

Il riesame dovrà verificare lo stato delle azioni preventive e correttive e l'aderenza alla politica.

Dovrà tenere conto di tutti i cambiamenti che possono influenzare l'approccio della azienda alla gestione della sicurezza delle informazioni, includendo i cambiamenti organizzativi, l'ambiente tecnico, l'evoluzione dei servizi cloud, la disponibilità di risorse, le condizioni legali, regolamentari o contrattuali e dei risultati dei precedenti riesami.

Il risultato del riesame dovrà includere tutte le decisioni e le azioni relative al miglioramento dell'approccio aziendale alla gestione della sicurezza delle informazioni e della qualità.

IMPEGNO DELLA DIREZIONE

La Direzione sostiene attivamente la sicurezza delle informazioni in azienda tramite un chiaro indirizzo, un impegno evidente, degli incarichi espliciti e il riconoscimento delle responsabilità relative alla sicurezza delle informazioni.

L'impegno della direzione si attua tramite una struttura i cui compiti sono:

- garantire che siano identificati tutti gli obiettivi relativi alla sicurezza delle informazioni e alla qualità e che questi incontrino i requisiti aziendali e dei clienti;
- stabilire i ruoli aziendali e le responsabilità per lo sviluppo e il mantenimento del SGSD;
- fornire risorse sufficienti alla pianificazione, implementazione, organizzazione, controllo, revisione, gestione e miglioramento continuo del SGSD;
- controllare che il SGSD sia integrato in tutti i processi aziendali e che procedure e controlli siano sviluppati efficacemente;
- approvare e sostenere tutte le iniziative volte al miglioramento della sicurezza delle informazioni e della qualità dei servizi;
- attivare programmi per la diffusione della consapevolezza e della cultura della sicurezza delle informazioni.

Milano, li 16/07/2026

DGE