POLITICA PER LA SICUREZZA DELLE INFORMAZIONI

IN CONFORMITÀ' ALLA NORMA ISO 27001:2017

CAMPO DI APPLICAZIONE

Il Sistema di Gestione per la Sicurezza delle Informazioni viene applicato a tutte le attività svolte dall'azienda per:

EROGAZIONE DI SERVIZI DI CYBERSECURITY E DATA PROTECTION TRA CUI SERVIZI DI RED TEAMING / OFFENSIVE SECURITY, SECURITY ASSESSMENT E TRAINING, BASATI SU TECNOLOGIA ON-PREMISE E CLOUD
Di seguito viene riportata la politica per la sicurezza delle informazioni diffusa in azienda affinché tutto il personale interno e/o esterno ne sia consapevole, ne condivida i principi e si attivi in modo tale da perseguirla.

La politica per la sicurezza delle informazioni si applica a tutto il personale interno e quello delle terze parti che collaborano alla gestione delle informazioni ed a tutti i processi e risorse coinvolte nel campo di applicazione sopra delineato.

DESCRIZIONE

Essere competitivi significa puntare a differenziare le caratteristiche dei propri servizi attraverso una costante ricerca volta al miglioramento dei processi aziendali dai punti di vista della qualità, delle prestazioni aziendali e della sicurezza delle informazioni. SISTechnology SRL ritiene che la sicurezza delle informazioni rappresenti un fattore determinante.

Per SISTechnology SRL la gestione della sicurezza delle informazioni ha come obiettivo primario la protezione dei dati e delle informazioni al fine di tutelare il patrimonio rappresentato dalle conoscenze aziendali, quello dei propri clienti e di tutelare le persone fisiche di cui si trattano i dati personali.

Per perseguire questo obiettivo SISTechnology SRL, attraverso un approccio by design, pone grande attenzione alla progettazione, alla gestione e alla manutenzione della propria struttura tecnologica, fisica, logica ed organizzativa e conseguentemente, impegna la propria organizzazione e le proprie persone a sviluppare e manutenere un Sistema di Gestione della Sicurezza delle Informazioni nell'ambito delle attività svolte e dei servizi erogati al fine di garantire la disponibilità l'integrità e la riservatezza dei dati, oltre che delle informazioni e degli accessi.

Tutte le persone che lavorano e/o collaborano con l'Organizzazione sono impegnate a rispettare i seguenti principi:

1. Riservatezza: assicurare che l'informazione sia accessibile solamente ai soggetti e/o ai processi debitamente autorizzati e che le informazioni non siano rese disponibili o divulgate a persone o entità non autorizzate;
2. Integrità: salvaguardare la consistenza dell'informazione da modifiche non autorizzate e garantire che l'informazione non subisca modifiche o cancellazioni a seguito di errori o di azioni volontarie, ma anche a seguito di malfunzionamenti o danni dei sistemi tecnologici;
3. Disponibilità: assicurare che gli utenti autorizzati abbiano accesso alle informazioni e agli elementi architetturali associati quando ne fanno richiesta;
4. Controllo: assicurare che la gestione dei dati avvenga sempre attraverso processi e strumenti sicuri e testati;
5. Autenticità: garantire una provenienza affidabile dell'informazione.
6. Privacy: garantire la protezione ed il controllo dei dati personali.

La Direzione è fortemente impegnata a una grande responsabilizzazione di tutte le persone che lavorano per e con l'Organizzazione nel garantire la rigorosità del proprio operato per adempiere, con la massima attenzione, ai compiti assegnati. In particolare, questo obiettivo è perseguito attraverso l'impegno a garantire:

- il rispetto delle leggi e normative vigenti;
- l'efficienza operativa e affidabilità dei processi di sviluppo prodotti e servizi correlati;
- le condizioni di salute e sicurezza sui luoghi di lavoro per il personale e terzi;
- la continuità e l'efficienza dei processi organizzativi e operativi al fine di prevenire e ridurre al minimo l'impatto degli incidenti volontari o casuali sulla sicurezza dei dati/informazioni gestite;
- la protezione dei mezzi resi disponibili, ed il loro corretto utilizzo;
- la riservatezza, la correttezza e la disponibilità dei dati/informazioni gestiti dall'organizzazione e la salvaguardia della proprietà intellettuale;
- l'adozione di misure di prevenzione di anomalie di processo/prodotto/servizio.

Per dare attuazione alla propria politica della sicurezza delle informazioni, l'Organizzazione ha sviluppato e si impegna a mantenere un sistema di gestione per la sicurezza delle informazioni conforme ai requisiti specificati dalla norma UNI CEI EN ISO/IEC 27001:2017 e delle leggi cogenti.

La politica della sicurezza delle informazioni dell'Organizzazione garantisce:

- che l'organizzazione abbia piena conoscenza delle informazioni gestite e valuti di volta in volta la loro criticità, al fine di agevolare l'implementazione di adeguati livelli di protezione;
- che l'accesso alle informazioni avvenga in modo sicuro e adatto a prevenire i trattamenti non autorizzati o realizzati senza i diritti necessari;
- che l'organizzazione e le terze parti collaborino al trattamento delle informazioni adottando procedure volte al rispetto di adeguati livelli di sicurezza;
- che l'organizzazione e le terze parti che collaborano al trattamento delle informazioni siano adeguatamente formate e abbiano piena consapevolezza delle problematiche relative alla sicurezza;
- che le anomalie e gli incidenti aventi ripercussioni sul sistema informativo, sui servizi e sui livelli di sicurezza aziendale siano tempestivamente riconosciuti e correttamente gestiti attraverso efficienti sistemi di prevenzione, comunicazione e reazione al fine di minimizzare l'impatto sul business;
- che l'accesso alla sede ed ai singoli locali aziendali avvenga esclusivamente da personale autorizzato, a garanzia della sicurezza delle aree e degli asset presenti;
- la conformità con i requisiti di legge ed il rispetto degli impegni di sicurezza stabiliti nei contratti con le terze parti;
- la rilevazione di eventi anomali, incidenti e vulnerabilità dei sistemi informativi al fine di rispettare la sicurezza e la disponibilità dei servizi e delle informazioni;
- la business continuity aziendale e il disaster recovery, attraverso l'applicazione di procedure di sicurezza stabilite;
- che i trattamenti dei dati personali avvengano nel rispetto del Regolamento Europeo sulla Protezione dei Dati Personali GDPR 679/2016;
- l'osservanza dei livelli di sicurezza stabiliti attraverso l'implementazione SGSI (sistema di gestione della sicurezza delle informazioni);
- il rispetto delle normative vigenti e degli standard internazionali di sicurezza per la propria infrastruttura tecnologica e organizzativa;
- la selezione di partner affidabili dal punto di vista della gestione in sicurezza delle informazioni e della protezione dei dati personali.

LA POLITICA SOPRA DESCRITTA VIENE COMUNICATA ALL'INTERNO DELL'ORGANIZZAZIONE MEDIANTE AFFISSIONE NELLE BACHECHE AZIENDALI ED È RESA DISPONIBILE PER LE PARTI INTERESSATE MEDIANTE PUBBLICAZIONE SUL SITO INTERNET AZIENDALE.

AD OGNI RIESAME ANNUALE DA PARTE DELLA DIREZIONE O IN CASO DI CAMBIAMENTI SIGNIFICATIVI NE VIENE VERIFICATA LA SUA ADEGUATEZZA.

CUNEO (CN), 22/09/2022

La Direzione Aziendale

SISTechnology srl
Via Artigiani, 6 - CUNEO
P.I: 03952720047