Con il presente documento Novation Tech spa fornisce una linea guida che sottolinea l'importanza della sicurezza delle informazioni per la propria strategia aziendale. Questa guida tiene conto delle normative, delle leggi e delle minacce potenziali alla sicurezza delle informazioni. È importante che tutti coloro coinvolti riconoscano che la Direzione dell'organizzazione sostiene la sicurezza delle informazioni coinvolgendo tutti i propri dipendenti. Inoltre, è essenziale rispettare le linee guida e le regole stabilite per garantire un ambiente sicuro per le informazioni dell'azienda.

L'azienda

Novation Tech s.p.a. è impegnata nella realizzazione di parti strutturali, componenti in fibra di carbonio, materiali compositi avanzati e combinazione di componenti in carbonio, plastica e metallo con operazioni di assemblaggio. L'obiettivo è trasformare idee e progetti in componenti ad altissimo contenuto tecnologico, utilizzando diverse tecnologie.

La continua collaborazione con clienti di diversi settori, con i centri di ricerca e con i fornitori più qualificati permette di offrire alternative innovative e soluzioni personalizzate. L'obiettivo principale è garantire la realizzazione di prodotti che soddisfino pienamente le aspettative del cliente, sia in termini di design che di prestazioni e qualità.

Scopo

Questo documento illustra le linee guida sulla sicurezza informatica per Novation Tech, specificando gli obiettivi chiave, le strategie e le responsabilità. L'approccio dell'azienda all'implementazione è guidato da normative internazionali stabilite, standard e requisiti legali.

Responsabili

Team "Sicurezza delle Informazioni":
Matteo Tabassi, matteo.tabassi@novationtech.com
Giovanni Collatuzzo, giovanni.collatuzzo@novationtech.com
Reparto IT, IT@novationtech.com

Ambito di applicazione

La linea guida si applica all'intera azienda con sede a 31044 MONTEBELLUNA (TV) ed è vincolante per tutti i dipendenti dell'azienda.

Requisiti

La fiducia dei clienti dell'azienda si basa su questi fondamenti:

- Gestire in modo affidabile i progetti e i servizi offerti dall'organizzazione;
- consegnare o conservare i prodotti in modo sicuro;
- mantenere la riservatezza delle informazioni dei clienti;
- garantire l'integrità delle informazioni dei clienti;

- garantire la disponibilità delle informazioni da proteggere;
- rispettare i requisiti di legge;
- rispettare i requisiti contrattuali;
- rispettare le misure di sicurezza che l'organizzazione si è prefissata;
- proteggere in modo sostanziale i segreti commerciali e le innovazioni;
- in caso di danno, ridurre gli effetti a un livello accettabile attraverso adeguate misure preventive;
- preservare la propria reputazione e la fiducia dei propri stakeholders evitando di compromettere gli obiettivi di sicurezza.

I rischi

I rischi includono:

- la violazione delle specifiche dei clienti (ad esempio a causa di guasti al sistema, perdita di dati, divulgazione non autorizzata di informazioni),
- la divulgazione non autorizzata / inosservata di segreti commerciali,
- conformità incompleta/errata ai requisiti di legge (ad es. GDPR).

Obiettivi di sicurezza

Il successo commerciale dell'azienda dipende dalla capacità di riconoscere i rischi esistenti, di evitarli o ridurli adottando misure adeguate e di trattare in modo appropriato i rischi residui. Questo standard definisce le linee guida e i principi generali per l'implementazione di un sistema di gestione della sicurezza delle informazioni , nonché gli obiettivi e le misure per garantire un'adeguata disponibilità, riservatezza e integrità dei dati dei clienti.

Importanza e sicurezza

In considerazione delle molteplici esigenze, sia interne che esterne, e in particolare dei requisiti di sicurezza richiesti dalla clientela, è imprescindibile che la sicurezza delle informazioni venga considerata come un elemento cardine all'interno della filosofia aziendale. È importante sottolineare che la perdita o la manipolazione non autorizzata di dati e informazioni potrebbe compromettere gravemente il successo a lungo termine dell'azienda. Pertanto, è necessario che ogni membro del personale sia pienamente consapevole dell'importanza della sicurezza delle informazioni e delle conseguenze cruciali che i rischi inerenti possono comportare.

Gli obiettivi del sistema di gestione della sicurezza dell'informazione (ISMS) includono

- garantire la disponibilità, l'integrità e la riservatezza dei sistemi e dei dati;
- migliorare la consapevolezza delle opportunità e dei rischi legati alla tecnologia dell'informazione;
- promuovere la comprensione della protezione delle informazioni;
- integrare la sicurezza dell'informazione nei processi aziendali.

Responsabilità

In linea di principio, chiunque utilizzi le informazioni è responsabile della loro sicurezza nell'ambito delle linee guida. Le responsabilità tecniche e organizzative sono delineate nelle rispettive linee guida per le

singole aree funzionali. I dirigenti, nell'ambito della loro area di responsabilità, hanno il compito di garantire un'adeguata sicurezza delle informazioni in ogni momento della gestione delle informazioni e dei sistemi informativi. Ciò comprende anche l'attuazione delle misure di sicurezza delle informazioni, il loro coordinamento con altre aree e il controllo della conformità alle normative. La responsabilità generale e la responsabilità esclusiva per i danni ricadono sulla direzione dell'azienda.

Violazioni e sanzioni

Le violazioni delle norme di sicurezza delle informazioni vengono verificate singolarmente in base alle disposizioni di legge e contrattuali pertinenti e punite di conseguenza.

Nel caso in cui venga stabilito un utilizzo delle informazioni tale per cui si attesti una mancanza di conformità alle norme stabilite, tra le violazioni, gli atti dolosi o le negligenze gravi rientrano in particolare atti, situazioni o eventi

- che danneggiano la sicurezza e la reputazione dell'azienda;
- che mettono in pericolo la sicurezza dei dipendenti o dei partner contrattuali;
- che causano all'azienda un'effettiva perdita finanziaria;
- che consentono l'accesso non autorizzato alle informazioni.

Regolamento di base

La direzione ha istituito un team di "Sicurezza delle Informazioni" per far rispettare gli obiettivi di sicurezza e gli ha dato il compito di creare linee guida uniformi per il processo di sicurezza specifico del sito, garantendo che tutti i dipendenti siano sufficientemente informati e verificando il rispetto delle linee guida di sicurezza. Al suddetto team vengono fornite risorse sufficienti per svolgere i propri compiti.

La sensibilizzazione e la verifica del rispetto delle linee guida di sicurezza e dell'aggiornamento della documentazione avvengono:

- regolarmente (durante gli audit interni);
- in relazione agli eventi, in caso di incidenti di sicurezza;
- in caso di importanti modifiche tecniche e organizzative;
- in caso di importanti modifiche al layout aziendale (ad es. misure strutturali);
- in caso di informazioni/progetti molto riservati.

Devono essere utilizzate misure tecniche, organizzative e infrastrutturali adeguate per controllare l'accesso ai sistemi sensibili, alle zone di sicurezza e alle strutture infrastrutturali critiche, nonché l'accesso alle informazioni e alle applicazioni critiche, consentendolo solo alle persone autorizzate. Le autorizzazioni di ammissione e di accesso vengono concesse e revocate solo dopo un processo di richiesta formalizzato, se necessario. I proprietari delle informazioni devono essere generalmente inclusi.

Vengono erogati corsi di formazione sulla sicurezza informatica ai dipendenti almeno una volta ogni tre anni. Al momento dell'assunzione, i nuovi dipendenti vengono istruiti sulle linee guida di sicurezza applicabili e sulle nozioni generali dei requisiti di sicurezza informatica previsti dalla TISAX.

I documenti e le registrazioni sono soggetti ai controlli documentali, che ne regolano la creazione, la versione, l'approvazione e la distribuzione. I documenti rilasciati sono resi disponibili nel server aziendale.

Il team "Sicurezza delle Informazioni" riferisce alla direzione sulla situazione della sicurezza a seguito degli audit interni, degli audit esterni e, in caso, di incidenti di sicurezza.

Regolamentazione dei visitatori

Solo i dipendenti autorizzati possono accedere ai locali dell'azienda. I visitatori esterni vengono tracciati in un registro elettronico dove vengono riportati:

- Nome e azienda del visitatore
- Dipendenti dell'azienda da visitare
- Data della visita
- Durata della visita

I visitatori sono accompagnati dalla persona ospitante o da un rappresentante aziendale e non sono mai lasciati incustoditi durante la loro permanenza nell'azienda. L'accesso alle aree autorizzate è rigorosamente controllato e monitorato.

Vietato fotografare

In tutta l'azienda / in tutte le sedi vige un divieto generale di fotografare e/o produrre video. I visitatori ne sono espressamente informati attraverso i moduli di visita.

Fotografare e/o produrre video di un prodotto è consentito solo previa autorizzazione opportunamente documentata. Le registrazioni digitali devono essere gestite in modo sicuro e cancellate dal supporto dati originale dopo il trasferimento.

Supporti di dati mobili per viaggi all'estero (al di fuori dell'Unione Europea)

Quando si tratta di proteggere le informazioni sensibili su supporti di dati mobili, è necessario tenere conto dei seguenti aspetti. Quando si portano con sé supporti di dati mobili, ogni dipendente deve informarsi sulle norme di sicurezza delle informazioni pertinenti presso il reparto IT prima di iniziare il viaggio:

- Protezione adeguata dei sistemi informatici portatili (ad es. crittografia, protezione antivirus).
- Crittografia, backup e protezione dei dati e dei supporti di dati

I viaggiatori sono responsabili di non creare opportunità per l'uso improprio di informazioni e dati critici.

Revisione regolare della politica di sicurezza delle informazioni

La politica di sicurezza delle informazioni viene verificata almeno una volta ogni tre anni o in caso di eventi occasionali (ad esempio, in caso di incidenti di sicurezza) o in caso di importanti cambiamenti nell'ambiente per garantire che sia aggiornata ed efficace e, se necessario, viene adeguata. Sono incluse le modifiche alle condizioni generali, ai compiti o alla strategia di sicurezza.

Implicitamente al controllo delle linee guida, vengono verificate le linee guida degli account utente e i diritti assegnati agli utenti.

Le misure di verifica comprendono
- Verifica delle linee guida per gli account utente e delle autorizzazioni assegnate agli utenti;
- Formazione dei dipendenti sulla sicurezza delle informazioni;
- Esercitazioni di emergenza / test di vari sistemi;
- Verifica delle porte, dei protocolli di sistema e dell'accesso al sistema (account di sistema).

Cambiamenti

Per quanto riguarda le aree rilevanti per la sicurezza, modifiche strutturali, trasferimenti, cambiamenti di responsabilità nella gestione, condizioni generali, ecc. vengono immediatamente segnalate alla sicurezza dell'azienda cliente o alla società di audit TISAX.

Comportamento in caso di incidenti speciali

Gli incidenti particolari che hanno un impatto indiretto o diretto sul cliente, come ad esempio effrazioni, furti, incendi, danni o attacchi di hacking, ecc. vengono immediatamente segnalati alla sicurezza del gruppo di clienti o alla sicurezza dell'azienda del cliente.

Obblighi

L'organizzazione dell'azienda si basa sullo standard TISAX®AL2 e tiene conto degli elementi di gestione di questo standard.

L'azienda/la direzione garantisce che
- la politica di sicurezza delle informazioni e gli obiettivi di sicurezza delle informazioni siano definiti e compatibili con l'organizzazione strategica;
- i requisiti del sistema di gestione della sicurezza delle informazioni siano integrati nei processi aziendali dell'organizzazione;
- l'importanza di avere un sistema robusto di gestione della sicurezza delle informazioni, che soddisfi tutti i requisiti necessari e garantisca l'efficacia del sistema;
- il sistema di gestione della sicurezza delle informazioni raggiunge gli obiettivi di sicurezza delle informazioni;
- i dipendenti vengono istruiti, formati e supportati affinché possano contribuire all'efficacia della sicurezza delle informazioni;

- il sistema di gestione della sicurezza delle informazioni viene continuamente promosso e ottimizzato;
- i manager vengono supportati per rendere chiaro il loro ruolo di leadership nelle rispettive aree di responsabilità;
- le risorse interne ed esterne necessarie per il sistema di gestione della sicurezza delle informazioni sono rese disponibili.

Ogni dipendente è tenuto a osservare e rispettare le linee guida generali sulla sicurezza e quelle applicabili al rispettivo posto di lavoro.

Tutti i rapporti sono redatti dalla direzione.

Rilascio della linea guida sulla sicurezza delle informazioni:

MONTEBELLUNA, 29/02/2024

Luogo, *Data*

Novation Tech S.p.A.
Via Feltrina Sud, 172
31044 MONTEBELLUNA (Treviso)
C. F. e P. IVA e Cod. ISO IT 04339720262

Responsabile