Politica per la sicurezza delle informazioni

Revisioni documento

Rev.	Data	Autore	Note
0.1	07/01/2025	Alberto Buratti	Prima versione
0.2	04/02/2025	Alberto Buratti	Aggiunto riferimenti a Riservatezza, Integrità e Disponibilità

Distribuzione

Nome	Titolo
Tutti i collaboratori	

Approvazione

Nome	Posizione	Data
Alberto Buratti	Direzione	07/01/2025

INDICE DEI CONTENUTI

1. Introduzione

Questo documento definisce la politica di sicurezza delle informazioni di Tecnica - Formazione - Sicurezza s.r.l..

In quanto azienda moderna e lungimirante, Tecnica - Formazione - Sicurezza s.r.l. riconosce ai livelli più alti la necessità di garantire che la propria attività operi senza problemi e senza interruzioni a beneficio dei clienti, degli azionisti e delle altre parti interessate.

Al fine di fornire un tale livello di operatività continua, Tecnica - Formazione - Sicurezza s.r.l. ha implementato un Sistema di Gestione della Sicurezza delle Informazioni (ISMS) in linea con lo Standard Internazionale per la Sicurezza delle Informazioni, ISO/IEC 27001, 27017 E 27018. Questo standard definisce i requisiti per un ISMS basato sulle migliori pratiche riconosciute a livello internazionale.

L'ISMS di Tecnica - Formazione - Sicurezza s.r.l. si basa sui principi di **riservatezza, integrità e disponibilità**, garantendo che le informazioni siano accessibili solo a chi ne ha diritto, che siano accurate e complete e che siano disponibili quando necessario.

Il funzionamento dell'ISMS comporta molti vantaggi per l'azienda, tra cui:

- **Protezione della continuità operativa** e dei flussi di reddito aziendali, garantendo l'erogazione costante dei servizi formativi e delle soluzioni offerte.
- **Garantire l'erogazione di servizi di alta qualità** ai clienti, rafforzando la fiducia e la soddisfazione delle parti interessate.
- **Consolidamento e sviluppo della reputazione aziendale**, aumentando il valore percepito dell'azienda nel mercato della formazione e della sicurezza.
- **Conformità ai requisiti legali, normativi e contrattuali**, rispettando le normative sulla sicurezza delle informazioni e la protezione dei dati personali.

Tecnica - Formazione - Sicurezza s.r.l. ha deciso di mantenere la piena certificazione ISO/IEC 27001, 27017 e 27018 affinché l'effettiva adozione delle migliori pratiche di sicurezza delle informazioni possa essere convalidata da una terza parte indipendente, un Organismo di Certificazione Registrato (RCB).

Questa politica si applica a tutti i sistemi, le persone e i processi che costituiscono i sistemi informativi dell'organizzazione, compresa la Direzione, i dipendenti, i fornitori e altre terze parti che hanno accesso ai sistemi di Tecnica - Formazione - Sicurezza s.r.l..

I seguenti documenti di supporto sono rilevanti per questa politica di sicurezza delle informazioni e forniscono ulteriori informazioni sulla sua applicazione:

- Valutazione del rischio e processo di trattamento
- Dichiarazione di applicabilità
- Processo di valutazione della sicurezza delle informazioni dei fornitori
- Politica di accesso a Internet

- Politica dei servizi cloud
- Politica sui dispositivi mobili
- Politica BYOD
- Politica di lavoro a distanza
- Politica di controllo degli accessi
- Criteri di controllo dell'accesso dinamico
- Processo di gestione dell'accesso degli utenti
- Politica crittografica
- Politica di sicurezza fisica
- Politica anti-malware
- Politica di backup
- Politica di registrazione e monitoraggio
- Politica del software
- Politica di gestione delle vulnerabilità tecniche
- Politica di sicurezza della rete
- Politica di messaggistica elettronica
- Politica di collaborazione online
- Politica di sviluppo sicuro
- Politica di sicurezza delle informazioni per i rapporti con i fornitori
- Politica di gestione della disponibilità
- Politica di conformità alla proprietà intellettuale e al copyright
- Politica di conservazione e protezione dei documenti
- Informativa sulla privacy e sulla protezione dei dati personali
- Politica della scrivania e dello schermo libero
- Politica sui social media
- Politica di sicurezza delle risorse umane
- Politica di intelligence sulle minacce
- Politica di gestione delle risorse
- Politica di utilizzo accettabile
- Politica sulle telecamere a circuito chiuso
- Politica di gestione della configurazione
- Politica di cancellazione delle informazioni
- Politica di mascheramento dei dati
- Politica di prevenzione delle fughe di dati
- Politica di monitoraggio
- Politica di filtraggio del web
- Politica di codifica sicura
- Politica di Whistleblowing per la sicurezza delle informazioni

I dettagli sull'ultimo numero di versione di ciascuno di questi documenti sono disponibili nel Registro della documentazione ISMS.

2. Politica di sicurezza delle informazioni

2.1. Requisiti di sicurezza delle informazioni

Una chiara definizione dei requisiti per la sicurezza delle informazioni all'interno di Tecnica - Formazione - Sicurezza s.r.l. sarà concordata e mantenuta con il business interno, in modo che tutte le attività del SGI siano focalizzate sul soddisfacimento di tali requisiti. Anche i requisiti statutari, normativi e contrattuali saranno documentati e inseriti nel processo di pianificazione. I requisiti specifici relativi alla sicurezza di sistemi o servizi nuovi o modificati saranno rilevati nella fase di progettazione di ogni progetto.

Questi requisiti includono la garanzia della **riservatezza**, **dell'integrità** e della **disponibilità** delle informazioni, in linea con le normative applicabili e le esigenze aziendali.

Un principio fondamentale del Sistema di gestione della sicurezza delle informazioni di Tecnica - Formazione - Sicurezza s.r.l. è che i controlli implementati sono guidati dalle esigenze aziendali e questo sarà regolarmente comunicato a tutto il personale attraverso riunioni di team e documenti informativi.

2.2. Quadro di riferimento per la definizione degli obiettivi

Per la definizione degli obiettivi di sicurezza delle informazioni si utilizzerà un ciclo regolare. Questi obiettivi si baseranno su una chiara comprensione dei requisiti aziendali, informata dal processo di revisione della gestione durante il quale si potranno ottenere i pareri delle parti interessate.

Gli obiettivi di sicurezza delle informazioni saranno documentati per un periodo di tempo concordato, insieme ai dettagli su come saranno raggiunti. Gli obiettivi saranno valutati e monitorati nell'ambito dei riesami della direzione per garantire che rimangano validi. Se sono necessarie modifiche, queste saranno gestite attraverso il processo di gestione delle modifiche.

In conformità alla norma ISO/IEC 27001, 27017 E 27018, i controlli di riferimento dettagliati nell'allegato A della norma saranno adottati, ove opportuno, da Tecnica - Formazione - Sicurezza s.r.l. . Questi saranno rivisti regolarmente alla luce dei risultati delle valutazioni dei rischi e in linea con i piani di trattamento dei rischi per la sicurezza delle informazioni. Per i dettagli su quali controlli dell'Allegato A sono stati implementati e quali sono stati esclusi, si rimanda *alla Dichiarazione di Applicabilità*.

Inoltre, verranno adottati e attuati, ove opportuno, controlli rafforzati e aggiuntivi dai seguenti codici di condotta:

- ISO/IEC 27002 - Codice di prassi per i controlli di sicurezza delle informazioni

- ISO/IEC 27017 - Codice di prassi per i controlli di sicurezza delle informazioni basato su ISO/IEC 27002 per i servizi cloud
- ISO/IEC 27018 - Codice di prassi per la protezione delle informazioni di identificazione personale (PII) nei cloud pubblici che agiscono come processori di PII

L'adozione di questi codici di condotta fornirà ulteriori garanzie ai nostri clienti e contribuirà alla nostra conformità con la legislazione internazionale sulla protezione dei dati.

2.3. Miglioramento continuo dell'ISMS

La politica di Tecnica - Formazione - Sicurezza s.r.l. in materia di miglioramento continuo è quella di:

- Migliorare continuamente l'efficacia dell'ISMS
- Migliorare i processi attuali per renderli conformi alle buone pratiche definite dalla norma ISO/IEC 27001, 27017 E 27018 e dagli standard correlati.
- Ottenere la certificazione ISO/IEC 27001, 27017 E 27018 e mantenerla su base continuativa
- Aumentare il livello di proattività (e la percezione di proattività da parte degli stakeholder) per quanto riguarda la sicurezza delle informazioni.
- Rendere più misurabili i processi e i controlli di sicurezza delle informazioni per fornire una solida base per decisioni informate.
- Rivedere le metriche pertinenti su base annuale per valutare se è opportuno modificarle, sulla base dei dati storici raccolti.
- Ottenere idee per il miglioramento attraverso incontri regolari e altre forme di comunicazione con le parti interessate.
- Esaminare le idee di miglioramento durante le riunioni periodiche della direzione per stabilire le priorità e valutare i tempi e i benefici.

Le idee di miglioramento possono provenire da qualsiasi fonte, compresi dipendenti, clienti, fornitori, personale IT, valutazioni dei rischi e rapporti di servizio. Una volta identificate, saranno registrate e valutate nell'ambito dei riesami della direzione.

Il processo di miglioramento continuo include la valutazione periodica dell'efficacia dei controlli di sicurezza nel garantire la riservatezza, l'integrità e la disponibilità delle informazioni.

2.4. Aree della politica di sicurezza delle informazioni

Tecnica - Formazione - Sicurezza s.r.l. definisce le politiche in un'ampia gamma di aree correlate alla sicurezza delle informazioni, che sono descritte in dettaglio in una serie completa di documenti sulle politiche che accompagnano questa politica generale sulla sicurezza delle informazioni.

Ciascuna di queste politiche viene definita e concordata da una o più persone competenti nell'area di riferimento e, una volta approvata formalmente, viene comunicata a un pubblico appropriato, sia interno che esterno all'organizzazione.

La tabella seguente mostra le singole politiche all'interno del set di documentazione e riassume il contenuto di ciascuna politica e il pubblico di riferimento delle parti interessate.

TITOLO DELLA POLITICA	AREE AFFRONTATE	PUBBLICO DI RIFERIMENTO
Politica di accesso a Internet	Uso aziendale di Internet, uso personale di Internet, gestione dell'account Internet, sicurezza e monitoraggio e usi non consentiti del servizio Internet.	Utenti del servizio Internet
Politica sul cloud computing	Due diligence, sottoscrizione, impostazione, gestione e rimozione dei servizi di cloud computing.	Dipendenti coinvolti nell'approvvigionamento e nella gestione dei servizi cloud
Politica sui dispositivi mobili	Cura e sicurezza dei dispositivi mobili come laptop, tablet e smartphone, se forniti dall'organizzazione per uso aziendale.	Utenti di dispositivi mobili forniti dall'azienda
Politica BYOD	Considerazioni sul BYOD (Bring Your Own Device), quando il personale desidera utilizzare i propri dispositivi mobili per accedere alle informazioni aziendali.	Utenti di dispositivi personali per uso aziendale limitato
Politica di telelavoro	Considerazioni sulla sicurezza delle informazioni nella creazione e nella gestione di un sito e di un sistema di telelavoro, ad esempio sicurezza fisica, assicurazione e attrezzature.	La direzione e i dipendenti coinvolti nella creazione e nel mantenimento di un sito di telelavoro
Politica di controllo degli accessi	Registrazione e cancellazione degli utenti, fornitura di diritti di accesso, accesso esterno, revisione degli accessi, politica delle password, responsabilità degli utenti e controllo degli accessi al sistema e alle applicazioni.	Dipendenti coinvolti nell'impostazione e nella gestione del controllo degli accessi
Criteri di controllo dell'accesso dinamico	Applicabilità e utilizzo dei controlli di accesso dinamici disponibili in ambienti specifici.	Proprietari degli asset e team ICT
Politica crittografica	Valutazione dei rischi, selezione delle tecniche, implementazione, test e revisione della crittografia e gestione delle chiavi.	Dipendenti coinvolti nell'impostazione e nella gestione dell'uso della tecnologia e delle tecniche crittografiche
Politica di sicurezza fisica	Aree sicure, sicurezza della carta e delle apparecchiature e gestione del ciclo di vita delle apparecchiature	Tutti i dipendenti

Politica anti-malware	Firewall, antivirus, filtro antispam, installazione e scansione del software, gestione delle vulnerabilità, formazione degli utenti, monitoraggio delle minacce e avvisi, revisioni tecniche e gestione degli incidenti malware.	Dipendenti responsabili della protezione dell'infrastruttura dell'organizzazione dal malware
Politica di backup	Cicli di backup, backup su cloud, archiviazione off-site, documentazione, test di ripristino e protezione dei supporti di archiviazione.	Dipendenti responsabili della progettazione e dell'implementazione dei regimi di backup
Politica di registrazione e monitoraggio	Impostazioni per la raccolta, la protezione e la revisione degli eventi	Dipendenti responsabili della protezione dell'infrastruttura dell'organizzazione dagli attacchi
Politica del software	Acquisto di software, registrazione, installazione e rimozione di software, sviluppo di software interno e utilizzo di software nel cloud.	Tutti i dipendenti
Politica di gestione delle vulnerabilità tecniche	Definizione delle vulnerabilità, fonti di informazione, patch e aggiornamenti, valutazione delle vulnerabilità, hardening, formazione alla consapevolezza e divulgazione delle vulnerabilità.	Dipendenti responsabili della protezione dell'infrastruttura dell'organizzazione dal malware
Politica di sicurezza della rete	Progettazione della sicurezza di rete, compresa la segregazione di rete, la sicurezza perimetrale, le reti wireless e l'accesso remoto; gestione della sicurezza di rete, compresi ruoli e responsabilità, registrazione e monitoraggio e modifiche.	I dipendenti responsabili della progettazione, dell'implementazione e della gestione delle reti
Politica di messaggistica elettronica	Invio e ricezione di messaggi elettronici, monitoraggio delle strutture di messaggistica elettronica e uso della posta elettronica.	Utenti di servizi di messaggistica elettronica
Politica di collaborazione online	Utilizzo di strumenti di collaborazione per la comunicazione, la condivisione e le videoconferenze.	Utenti di strumenti di collaborazione online
Politica di sviluppo sicuro	Specifica dei requisiti aziendali, progettazione, sviluppo e collaudo del sistema e sviluppo di software in outsourcing.	Dipendenti responsabili della progettazione, della gestione e della scrittura di codice per sviluppi software su misura
Politica di sicurezza delle informazioni per i rapporti con i fornitori	Due diligence, accordi con i fornitori, monitoraggio e revisione dei servizi, modifiche, controversie e fine del contratto.	Dipendenti coinvolti nella creazione e nella gestione dei rapporti con i fornitori
Politica di gestione della disponibilità	Requisiti e progettazione della disponibilità, monitoraggio e reporting, non disponibilità, verifica dei piani di disponibilità e gestione delle modifiche.	Dipendenti responsabili della progettazione dei sistemi e della gestione dell'erogazione dei servizi
Politica di conformità alla	Protezione della proprietà intellettuale, legge, sanzioni e conformità delle licenze software.	Tutti i dipendenti

proprietà intellettuale e al copyright		
Politica di conservazione e protezione dei documenti	Periodo di conservazione per tipi specifici di record, uso della crittografia, selezione dei supporti, recupero dei record, distruzione e revisione.	Dipendenti responsabili della creazione e della gestione dei documenti
Informativa sulla privacy e sulla protezione dei dati personali	Legislazione applicabile in materia di protezione dei dati, definizioni e requisiti.	Dipendenti responsabili della progettazione e della gestione di sistemi che utilizzano dati personali
Politica della scrivania e dello schermo libero	Sicurezza delle informazioni visualizzate sugli schermi, stampate e conservate su supporti rimovibili.	Tutti i dipendenti
Politica sui social media	Linee guida per l'utilizzo dei social media quando si rappresenta l'organizzazione e si discutono questioni rilevanti per l'organizzazione.	Tutti i dipendenti
Politica di sicurezza delle risorse umane	Assunzione, contratti di lavoro, conformità alle politiche, processo disciplinare, licenziamento	Tutti i dipendenti
Politica di utilizzo accettabile	Impegno dei dipendenti nei confronti delle politiche di sicurezza informatica dell'organizzazione.	Tutti i dipendenti
Politica di gestione delle risorse	Questo documento stabilisce le regole per la gestione degli asset dal punto di vista della sicurezza delle informazioni.	Tutti i dipendenti
Politica sulle telecamere a circuito chiuso	L'uso della TVCC nella sicurezza fisica, comprese le questioni e le considerazioni relative all'ubicazione e alla protezione dei dati.	Dipendenti responsabili della TVCC
Politica di gestione della configurazione	La configurazione sicura di hardware, software, servizi e reti.	Dipendenti responsabili della progettazione dei sistemi e della gestione dell'erogazione dei servizi
Politica di cancellazione delle informazioni	L'eliminazione delle informazioni memorizzate nei sistemi informativi, nei dispositivi o in qualsiasi altro supporto di memorizzazione, quando non sono più necessarie.	Dipendenti responsabili della progettazione e della gestione di sistemi che utilizzano dati personali
Politica di mascheramento dei dati	L'uso di tecniche di mascheramento dei dati, come l'anonimizzazione e la pseudonimizzazione, per proteggere le informazioni di identificazione personale (PII).	Dipendenti responsabili della progettazione e della gestione di sistemi che utilizzano dati personali
Politica di prevenzione delle fughe di dati	La configurazione di strumenti software pertinenti per rilevare e prevenire la fuga di dati.	Dipendenti responsabili della progettazione dei sistemi e della gestione dell'erogazione dei servizi
Politica di monitoraggio	Il monitoraggio dell'ambiente ICT per rilevare attività anomale.	Dipendenti responsabili della progettazione di sistemi e

		della gestione dell'erogazione di servizi
Politica di filtraggio del web	Limitare l'accesso a siti Internet ritenuti inappropriati.	Dipendenti responsabili della progettazione di sistemi e della gestione dell'erogazione di servizi
Politica di codifica sicura	I principi che verranno utilizzati nello sviluppo di codice sicuro.	Dipendenti responsabili della progettazione, della gestione e della scrittura di codice per lo sviluppo di software su misura
Politica di intelligence sulle minacce	La raccolta e l'uso di informazioni sulle minacce a livello strategico, tattico e operativo.	Dipendenti responsabili della protezione dell'infrastruttura dell'organizzazione dagli attacchi
Politica di Whistleblowing per la sicurezza delle informazioni	La sollevazione di questioni relative alla sicurezza delle informazioni all'interno dell'organizzazione.	Tutti i dipendenti e le altre parti interessate

2.5. Applicazione della politica di sicurezza delle informazioni

Le dichiarazioni di politica contenute in questo documento e nella serie di politiche di supporto elencate nella Tabella 1 sono state esaminate e approvate dalla Direzione di Tecnica - Formazione - Sicurezza s.r.l. e devono essere rispettate. La mancata osservanza di queste politiche da parte di un dipendente può comportare l'adozione di provvedimenti disciplinari in conformità con il *Processo disciplinare per i dipendenti dell*'organizzazione.

Le domande relative a qualsiasi politica di Tecnica - Formazione - Sicurezza s.r.l. devono essere rivolte in prima istanza al diretto responsabile del dipendente.

La consapevolezza e la formazione del personale in merito alla **riservatezza, all'integrità e alla disponibilità** delle informazioni sono fondamentali per l'efficace applicazione di questa politica.

2.6. Sicurezza dei Servizi Cloud

Tecnica - Formazione - Sicurezza s.r.l. riconosce l'importanza di garantire la sicurezza delle informazioni nei servizi cloud. In conformità con la norma ISO/IEC 27017, l'organizzazione adotta misure specifiche per affrontare i rischi e le sfide uniche associate all'utilizzo del cloud computing. Queste misure includono:

- **Segregazione dei dati:** I dati dei clienti sono segregati in modo logico e fisico per garantire la riservatezza e prevenire l'accesso non autorizzato.

- **Protezione delle informazioni dei clienti:** Vengono implementati controlli di sicurezza per proteggere le informazioni dei clienti da accessi non autorizzati, divulgazione, modifica o distruzione.
- **Responsabilità condivisa:** L'organizzazione collabora con i fornitori di servizi cloud per definire e implementare controlli di sicurezza appropriati, in base al modello di responsabilità condivisa.
- **Conformità alle normative:** L'organizzazione si impegna a rispettare tutte le normative applicabili in materia di protezione dei dati e sicurezza delle informazioni nel cloud.

2.7. Protezione delle Informazioni di Identificazione Personale (PII) nel Cloud

Tecnica - Formazione - Sicurezza s.r.l. si impegna a proteggere la riservatezza e la sicurezza delle informazioni di identificazione personale (PII) trattate nei servizi cloud. In conformità con la norma ISO/IEC 27018, l'organizzazione adotta i seguenti principi:

- **Obbligo contrattuale/Legittimo interesse:** Il trattamento delle PII nel cloud è necessario per l'esecuzione di un contratto o per il perseguimento del legittimo interesse del titolare del trattamento, nel rispetto delle normative applicabili.
- **Controllo degli accessi:** L'accesso alle PII nel cloud è limitato al personale autorizzato e viene implementato il principio del privilegio minimo.
- **Minimizzazione dei dati:** L'organizzazione raccoglie e conserva solo le PII necessarie per gli scopi specificati.
- **Sicurezza:** Vengono implementate misure di sicurezza appropriate per proteggere le PII da accessi non autorizzati, divulgazione, modifica o distruzione.
- **Trasparenza:** L'organizzazione informa gli individui su come vengono raccolte, utilizzate e protette le loro PII nel cloud.
- **Diritti degli individui:** L'organizzazione rispetta i diritti degli individui in relazione alle loro PII, come il diritto di accesso, rettifica e cancellazione.