deepcloud

NORMATIVA PER LA SICUREZZA DELL'INFORMAZIONE

ISMS MANAGER
DEEPCLOUD AG
Wittenbach

ID: DC021 - IT
Versione: 1.1
Data: 30.10.2023

Classificazione livello C1 - Pubblico

SEZIONE CONTROLLO DOCUMENTI

Modifiche al protocollo

Data	Versione	Stato (Bozza/per revisione)	Autore	Descrizione
27.8.2021	1.0	Finale	CEO/ISMS Manager	Prima versione
8.9.2021	1.1	Approvato	ISMS Manager	Aggiornamento introduzione e piccoli cambiamenti semantici (non rilevanti per il contenuto)

Revisione e approvazione/rilascio

Data	Versione	Revisione/approvazione	Autorizzazione a modificare e approvare	Osservazione:
8.9.2021	1.1	Approvazione	CEO	
10.10.2022	1.1	Revisione	ISMS Manager	Documento controllato, nessuna modifica
30.10.2023	1.1	Revisione	ISMS Manager	Correzioni minori, non rilevanti dal punto di vista del contenuto

RIFERIMENTI A DOCUMENTI ESTERNI

Data	Versione	Doc ID	Nome e descrizione	Nome documento/Link

RIFERIMENTI A DOCUMENTI INTERNI

Data	Versione	Doc ID	Nome e descrizione	Nome documento/Link

LISTA DEI DESTINATARI

Data	Nome	Nome documento/Link
20.9.2021	Pubblico	-

1. SOMMARIO

2. INTRODUZIONE

DeepCloud AG ("Azienda") considera la protezione dei dati e della struttura organizzativa (tecnologica e fisica) come l'obiettivo primario per la sicurezza delle informazioni e di conseguenza ha implementato e concepito un *Information Security Management System* (di seguito "ISMS") per garantirne il costante aggiornamento, nonché il rispetto delle seguenti misure di sicurezza che devono essere rispettate.

1. **Riservatezza**, tutte le informazioni/dati sono accessibili solo a persone e/o a processi autorizzati.
2. **Integrità**, proteggendo l'integrità e la coerenza dei database e le informazioni memorizzate da modifiche non autorizzate.
3. **Disponibilità**, fornendo le informazioni/dati richiesti agli utenti autorizzati quando richiesto.
4. **Controllo**, garantendo la gestione dei dati attraverso processi e strumenti controllati e sicuri.
5. **Autenticità**, assicurando una fonte affidabile di informazioni.
6. **Protezione dei dati**, garantendo la protezione e il controllo dei dati personali.

I servizi offerti dall'azienda attraverso la sua infrastruttura tecnologica sono garantiti dai livelli di sicurezza implementati nell'ISMS, che comprendono quanto segue:

- Affidabilità del sistema per la gestione dei processi e delle informazioni
- Massimi doveri di diligenza per l'immagine aziendale
- Pieno rispetto del Service Level Agreements come concordato con i clienti
- Soddisfazione della clientela
- Conformità con i regolamenti applicabili e lo standard di sicurezza internazionale

L'ISMS implementato nell'azienda è conforme ai requisiti dello standard ISO/IEC 27001:2013 e alle leggi rilevanti per la sicurezza delle informazioni nel contesto delle attività dell'azienda.

3. AMBITO

Questa normativa per la sicurezza dell'informazione si applica a tutti i dipendenti interni e ai terzi che svolgono un ruolo nella gestione delle informazioni, così come a tutti i processi e le risorse coinvolte nella pianificazione, nell'implementazione, nella commissione e nella fornitura continua di servizi aziendali.

4. PRINCIPI

Il termine "sicurezza" è definito in modo molto ampio nell'azienda e comprende la perdita di beni materiali e immateriali come le informazioni, nonché i rischi legati alla continuità del business aziendale. L'ISMS che è stato introdotto è stato sviluppato per identificare e prevenire tali rischi in una fase iniziale.

Il valore aggiunto della normativa per la sicurezza dell'informazione perseguita dall'azienda sta nella sua capacità di reagire prima che si verifichi un evento dannoso. Questo è possibile perché ogni membro dell'organizzazione agisce con un motivo oggettivo e usa la sua esperienza per raggiungere un alto livello di efficienza ed efficacia nella gestione della sicurezza delle informazioni.

La normativa per la sicurezza dell'informazione dell'azienda è orientata dai seguenti principi:

- Garantire la piena conoscenza delle informazioni gestite e la valutazione della loro criticità da parte dell'organizzazione per facilitare l'implementazione di un adeguato livello di protezione
- Garantire un accesso legittimo e sicuro alle informazioni per evitare un trattamento non autorizzato
- Assicurare che l'organizzazione e i terzi cooperino nel trattamento delle informazioni attuando procedure volte a mantenere un adeguato livello di sicurezza

- Assicurare che l'organizzazione e i terzi coinvolti nel trattamento delle informazioni siano pienamente consapevoli delle questioni relative alla sicurezza
- Garantire che le anomalie e gli episodi che interessano il sistema informativo e la sicurezza aziendale siano immediatamente identificati, documentati e adeguatamente gestiti attraverso efficaci sistemi di prevenzione, comunicazione e risposta per ridurre al minimo l'impatto sul business aziendale
- Assicurare che l'accesso ai locali degli uffici e ai singoli edifici dell'azienda sia consentito solo al personale autorizzato, al fine di garantire la sicurezza delle aree e dei beni corrispondenti
- Assicurare il rispetto dei requisiti legali e degli obblighi di sicurezza stabiliti nei contratti con terzi
- Assicurare il rilevamento di comportamenti anomali, eventi e vulnerabilità dei sistemi informativi per aumentare la sicurezza e la disponibilità dei servizi e delle informazioni
- Garantire la continuità del business aziendale e il recupero in caso di un grave evento attraverso l'applicazione delle procedure di sicurezza stabilite

La normativa per la sicurezza dell'informazione è formalizzata nell'ISMS, è costantemente aggiornata per garantirne il continuo perfezionamento ed è comunicata all'organizzazione, ai terzi e ai clienti attraverso i canali di comunicazione appropriati.

5. OBIETTIVI

In conformità con i principi di cui sopra, l'azienda definisce i seguenti obiettivi da perseguire in tutti i processi aziendali:

- Gestire la sicurezza delle informazioni, definendo obiettivi appropriati, fornendo risorse adeguate, preparando politiche e procedure di sicurezza specifiche da implementare in ogni dipartimento, assicurando sempre il pieno rispetto dei requisiti legali e normativi
- Comunicare le strategie, gli obiettivi e le finalità della sicurezza dell'informazione in modo che ci sia un reale scambio e accordo sui comportamenti e le misure da adottare
- Minimizzare le condizioni di rischio ed evitare le vulnerabilità al fine di proteggere le persone, i beni e l'azienda da qualsiasi minaccia, oltre a garantire gli standard aziendali, gli obiettivi, la competitività, il marchio e l'immagine aziendale
- Coinvolgere tutti i dipendenti e i fornitori attraverso attività di informazione, educazione e formazione che mirano ad aumentare la conoscenza, la competenza e la consapevolezza degli aspetti della sicurezza delle informazioni sia nella gestione delle attività quotidiane che degli incidenti che potrebbero mettere a rischio la continuità del business
- Assicurare un rapido ritorno alle normali operazioni in caso di emergenze e crisi, limitando i danni e le perdite, proteggendo le persone e i beni aziendali
- Monitorare i processi interni per verificare costantemente l'adeguatezza del sistema e individuare possibili misure di perfezionamento
- Migliorare l'ISMS per allinearsi ai mutevoli requisiti globali, aziendali e normativi

I principi di cui sopra e gli obiettivi definiti sono parte integrante del lavoro quotidiano dell'azienda. Per raggiungere questi obiettivi, tutte le misure tecniche, organizzative e operative necessarie sono prese, monitorate e riviste in un processo continuo.

6. RESPONSABILITÀ PER LA NORMATIVA PER LA SICUREZZA DELL'INFORMAZIONE

La direzione ha la responsabilità di mantenere l'ISMS aggiornato e in linea con l'evoluzione del contesto aziendale e di mercato, valutando tutte le misure in base a quanto segue:

- Sviluppi commerciali significativi
- Analisi di nuove attività di rischio
- Episodi di sicurezza rilevanti
- Cambiamenti nel contesto normativo o legale relativo al trattamento sicuro delle informazioni

La responsabilità di proteggere le persone e le risorse aziendali è dell'organizzazione. Tutti coloro che gestiscono, operano e controllano i processi aziendali devono assicurare un adeguato livello di protezione utilizzando gli strumenti e le risorse aziendali.

I responsabili delle singole funzioni e dei reparti devono quindi garantire che questa normativa per la sicurezza dell'informazione sia compresa e applicata di conseguenza da tutti i dipendenti e dai fornitori coinvolti.