Politica del sistema di gestione della sicurezza delle informazioni (“ISMS”)

Nome della ditta:	C2Compliance S.r.l.
Titolare della policy:	Direzione
Data effettiva:	15/12/2023

Scopo

Questa politica fornisce un quadro da applicare quando si stabilisce, si implementa, si mantiene e si migliora continuamente il sistema di gestione della sicurezza delle informazioni (“ISMS”), come definito nella*01-ISMS Ambito di applicazione dell'ISMS*, in conformità ai requisiti della norma ISO/IEC 27001 (“ISO 27001”).

Comando

Leadership e impegno

C2Compliance S.r.l. si impegna a stabilire, implementare, mantenere e migliorare continuamente l’ISMS. L’impegno della leadership è dimostrato dal Responsabile del ISMS[1] nello svolgimento delle proprie responsabilità come definite nel documento *03-Ruoli, responsabilità e autorità del ISMS*.C2Compliance S.r.l. stabilirà una politica di sicurezza delle informazioni e fisserà obiettivi di sicurezza delle informazioni che sono pienamente in linea con la nostra direzione strategica.C2Compliance S.r.l. garantirà che siano disponibili risorse sufficienti per l’istituzione, l’implementazione, il mantenimento e il miglioramento efficaci del nostro ISMS. Queste risorse includeranno:

- Sostegno finanziario
- Personale qualificato
- Strutture e infrastrutture tecniche

Politica sulla sicurezza delle informazioni

L'alta direzione stabilisce e sostiene una politica dedicata alla sicurezza delle informazioni. Questa politica:

1. In linea con lo scopo e la missione dell'organizzazione.
2. Incorpora i nostri obiettivi di sicurezza delle informazioni o pone le basi per determinare tali obiettivi.
3. Dimostra l'impegno a soddisfare tutti i requisiti di sicurezza delle informazioni pertinenti.

4. Sottolinea la nostra continua dedizione al miglioramento del nostro sistema di gestione della sicurezza delle informazioni.

Per trasparenza e consapevolezza:

1. Questa politica è documentata e facilmente accessibile.
2. Viene comunicato attivamente a tutti i livelli interni di C2Compliance S.r.l.
3. Inoltre, garantiamo che questa politica sia disponibile alle parti esterne interessate, dimostrando il nostro impegno per la sicurezza delle informazioni.

Ruoli, responsabilità e autorità

C2Compliance S.r.l. ha definito i ruoli, le responsabilità e le autorità coinvolte nella definizione, implementazione, mantenimento e miglioramento continuo dell'ISMS.C2Compliance S.r.l. ha inoltre definito come verranno misurate le prestazioni e le competenze e come verranno affrontate le lacune di competenze. Per ulteriori dettagli si rimanda al documento *03-Ruoli, responsabilità e autorità del ISMS*.

Pianificazione

Pianificazione generale per l'ISMS

C2Compliance S.r.l. dà priorità all'identificazione dei rischi e delle opportunità principali, all'integrazione delle soluzioni nel nostro sistema e al monitoraggio e al miglioramento continui del nostro approccio.

Valutazione del rischio per la sicurezza delle informazioni

Il nostro metodo coerente per la valutazione dei rischi garantisce l'identificazione delle principali minacce alla sicurezza. Valutiamo regolarmente e diamo priorità a questi rischi e conserviamo la documentazione di tutti i nostri risultati. Per ulteriori dettagli si rimanda al documento *04-Processo di valutazione e trattamento dei rischi del ISMS*.

Trattamento del rischio per la sicurezza delle informazioni

C2Compliance S.r.l. si impegna a selezionare le giuste soluzioni per i rischi identificati, a implementare i necessari controlli di sicurezza e a documentare accuratamente le nostre scelte ottenendo al contempo le approvazioni essenziali. Per ulteriori dettagli si rimanda al documento *04-Processo di valutazione e trattamento dei rischi del ISMS*.

Impostazione e raggiungimento degli obiettivi di sicurezza

C2Compliance S.r.l. Stabilisce obiettivi di sicurezza chiari e misurabili. Abbiamo sviluppato un piano completo che descrive dettagliatamente come raggiungerli, assegnando le risorse e le responsabilità necessarie e monitorando continuamente i nostri progressi per apportare le modifiche necessarie. Gli obiettivi di sicurezza delle informazioni vengono rivisti annualmente da C2Compliance S.r.l. con il Responsabile del ISMS si basa su una chiara comprensione dei requisiti aziendali. Gli attuali obiettivi di sicurezza delle informazioni sono i seguenti:

1. Proteggi la riservatezza, la disponibilità e l'integrità dei dati dell'azienda, dei clienti e dei dipendenti
2. Rispettare le leggi, i regolamenti e gli obblighi contrattuali dei clienti applicabili
3. Ottenere e mantenere la certificazione ISO 27001

I piani d'azione per raggiungere questi obiettivi vengono mantenuti e rivisti annualmente dal Consiglio di governance dell'ISMS. Fare riferimento al documento *10-Piano degli obiettivi di sicurezza delle informazioni del ISMS* per ulteriori dettagli.

Pianificazione delle modifiche all'ISMS

Quando i cambiamenti sono ritenuti essenziali, C2Compliance S.r.l. garantisce che siano pianificati sistematicamente, prestando un'attenta considerazione al loro potenziale impatto sulla nostra sicurezza generale e sull'organizzazione.

Supporto

Risorse:

C2Compliance S.r.l. si impegna a allocare le risorse necessarie per impostare, eseguire, mantenere e migliorare costantemente il nostro sistema di gestione della sicurezza delle informazioni.

Competenza:

1. Identifichiamo le competenze necessarie per i ruoli che influiscono sulle nostre prestazioni di sicurezza delle informazioni.
2. Il personale viene valutato in base all'istruzione, alla formazione e all'esperienza per garantire che possieda le competenze richieste.
3. Quando necessario, C2Compliance S.r.l. fornirà formazione, tutoraggio o riassegnazione o cercherà competenze esterne, mantenendo allo stesso tempo la prova di tali competenze.

Consapevolezza:

1. Tutto il personale viene informato della nostra politica di sicurezza delle informazioni e viene completata la formazione annuale di sensibilizzazione.
2. Comprendono il loro ruolo nel successo del sistema di gestione della sicurezza delle informazioni e le ripercussioni della non conformità.

Comunicazione:

1. C2Compliance S.r.l. Identifica e agisce in base alla necessità di comunicazioni sia interne che esterne relative alle nostre pratiche di sicurezza delle informazioni.
2. Le decisioni comprendono cosa, quando, come e con chi comunicare.

Le politiche di sicurezza delle informazioni pertinenti saranno comunicate a tutto il personale interessato almeno una volta all'anno dopo la revisione e l'approvazione o dopo che si siano verificate modifiche significative alla politica. La politica sarà resa disponibile sul sito web aziendale. Per ulteriori dettagli si rimanda al documento *06-Piano di comunicazione sulla sicurezza delle informazioni del ISMS*.

Controllo delle informazioni documentate

Informazioni documentate:

Il nostro sistema comprende informazioni esplicitamente richieste e qualsiasi altra documentazione che riteniamo cruciale per l'efficacia delle nostre misure di sicurezza.

La creazione e gli aggiornamenti della documentazione tengono conto dei meccanismi di identificazione, formato e approvazione adeguati.

Per mantenere l'integrità della nostra documentazione, disponiamo di protocolli per controllare la distribuzione, l'accesso, l'archiviazione, le modifiche e la conservazione.

La documentazione esterna, ritenuta essenziale, viene identificata e gestita in modo efficace all'interno del nostro sistema.

C2Compliance S.r.l. ha definito una procedura per il controllo e la protezione delle informazioni documentate. Per maggiori dettagli si rinvia al documento 05-ISMS per il controllo delle informazioni documentate.

Operazione

Pianificazione e controllo operativo

C2Compliance S.r.l. pianificherà, eseguirà e supervisionerà i processi vitali per soddisfare i requisiti e le azioni delineate nella Clausola 6.C2Compliance S.r.l. manterrà le informazioni documentate necessarie. Le modifiche pianificate saranno supervisionate e le implicazioni dei cambiamenti non pianificati saranno valutate. Verranno intraprese azioni adeguate per contrastare eventuali effetti negativi. Saranno disciplinati processi, prodotti o servizi di provenienza esterna cruciali per il sistema di gestione della sicurezza delle informazioni di C2Compliance S.r.l.

Valutazione del rischio per la sicurezza delle informazioni

C2Compliance S.r.l. effettuerà valutazione del rischio a intervalli programmati o alla luce di modifiche significative, rispettando i criteri evidenziati al punto 6.1.2 a). Una registrazione dei risultati di queste valutazioni del rischio sarà conservata.

Trattamento del rischio per la sicurezza delle informazioni

C2Compliance S.r.l. si impegna a dare esecuzione al piano di trattamento dei rischi legati alla sicurezza delle informazioni. Per ragioni di responsabilità, verranno conservate informazioni documentate sugli esiti del trattamento del rischio.

Valutazione delle prestazioni

Audit interno

C2Compliance S.r.l. effettua annualmente audit interni del proprio ISMS e ha definito una procedura di audit interno ISMS. Per ulteriori dettagli si rimanda al documento *07-Procedura ISMS per gli audit interni*.

Controllo di gestione

C2Compliance S.r.l. ha definito una procedura di revisione della gestione del ISMS[2] costituito dagli input e dagli output necessari per garantire che l'ISMS dell'azienda funzioni in modo efficace, come previsto, e sia in continuo miglioramento. Per ulteriori dettagli si rimanda al*08-Procedura ISMS per il Riesame della Direzione*.

Miglioramento

Miglioramento continuo

C2Compliance S.r.l. si impegna a migliorare continuamente la pertinenza, la sufficienza e l'efficienza del nostro sistema di gestione della sicurezza delle informazioni.

Non conformità e azioni correttive

In caso di deviazione dagli standard stabiliti, C2Compliance S.r.l. si impegna a:

- Affrontare la non conformità, gestirne gli effetti e implementare le correzioni necessarie.
- Valutare la causa principale, assicurandosi che non si ripeta o emerga in altre aree.
- Agire in base a eventuali modifiche richieste e convalidare l'efficacia di tali modifiche.

- Tutte le misure adottate saranno proporzionate alla gravità delle non conformità identificate.

Per trasparenza e due diligence, C2Compliance S.r.l. documenterà:

- Le specificità di eventuali non conformità e le misure correttive applicate.
- Gli esiti di tali azioni correttive.

C2Compliance S.r.l. ha definito un'azione correttiva e una procedura di miglioramento continuo del ISMS[3] quando vengono rilevate non conformità. Le non conformità possono essere identificate durante audit interni, audit esterni, riesami della direzione o monitoraggio continuo dell'ISMS. Per ulteriori dettagli si rimanda al documento *09-Procedura ISMS per azioni correttive e miglioramento continuo*.

Violazione delle norme

Tutto il personale (inclusi dipendenti, appaltatori e terze parti applicabili) di C2Compliance S.r.l. deve mantenere la sicurezza, la riservatezza, la disponibilità, l'integrità e la privacy delle risorse per C2Compliance S.r.l. Le violazioni delle politiche e delle procedure ISMS possono essere considerate gravi violazioni della fiducia, che possono comportare azioni disciplinari fino alla risoluzione del rapporto di lavoro o del contratto e procedimenti giudiziari in conformità con le leggi federali, statali e locali applicabili.

Copertura ISO 27001

ISO270014.1; 4.2; 4.3; 5.1

Cronologia delle versioni

Versione	Data	Descrizione	Autore	Approvato da
1	15/12/2023	Politica di gestione della sicurezza delle informazioni	Direzione	Responsabile ISMS