Politica per la sicurezza delle informazioni

TLP: AMBER

Documento confidenziale ad uso e consumo dei soli destinatari

Politica per la sicurezza delle informazioni

SOMMARIO

Date	Rev.	Revision Content	Drawn-up	Verified	Approved
21/06/2021	1	First issue	R. Catalano	F. Lorenzo	A.M. Pertosa

1 SCOPO E CAMPO DI APPLICAZIONE

Obiettivo del presente documento è definire le linee guida per implementare e sostenere un sistema di gestione per la sicurezza delle informazioni conforme alla norma UNI EN ISO/IEC 27001:2017 al fine di garantirne la:

- **Riservatezza** – informazioni accessibili solamente ai soggetti e/o ai processi debitamente autorizzati;
- **Integrità** – salvaguardia della consistenza dell'informazione da modifiche non autorizzate;
- **Disponibilità** – facilità di accesso alle informazioni necessarie;
- **Controllo** – garanzia che i processi e strumenti per la gestione dei dati siano sicuri e testati;
- **Autenticità** – provenienza affidabile dell'informazione.
- **Privacy** – garanzia di protezione e controllo dei dati personali.

Il documento si applica al personale di Brightcyde.

2 RIFERIMENTI

2.1 Documenti di riferimento

[Ref. 1] ISO/IEC 27001:2017 - Information technology - Security techniques - Information security management systems - Requirements;

[Ref. 2] Regolamento UE n. 679/2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei Dati Personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (Regolamento Generale sulla protezione dei dati);

2.2 Allegati

Nessuno

3 ACRONIMI E DEFINIZIONI

Tabella 1 - Acronimi

Acronimo	Descrizione
DR	Disaster Recovery
BC	Business Continuity

4 ECCEZIONI

Qualsiasi deviazione richiede una valutazione del rischio che includa l'identificazione di controlli di mitigazione o compensazione e un monitoraggio formale delle eccezioni.

5 RESPONSABILITÀ DEL PERSONALE

I dipendenti e il personale sono la prima linea di difesa nella protezione e nella sicurezza delle informazioni e dei beni delle aziende associate.

I dipendenti e il personale sono responsabili del rispetto delle linee guida e dai requisiti previsti dal SGSI e devono sempre segnalare qualsiasi sospetta violazione attraverso l'appropriato processo di segnalazione.

I dipendenti e il personale devono operare in conformità con le loro responsabilità definite all'interno delle procedure e negli standard pertinenti in ogni momento (ad esempio in sede, presso i clienti o lavorando in remoto) e devono completare tutti i corsi di formazione sulla sicurezza richiesti entro i tempi specificati.

L'uso di strumenti di comunicazione elettronica, internet e dispositivi informatici portatili è consentito e incoraggiato laddove tale uso supporti gli scopi e gli obiettivi dell'azienda. I dipendenti e il personale sono responsabili dell'uso corretto di queste tecnologie per proteggere le informazioni e le risorse di Brightcyde.

Brightcyde ha documentato e condiviso una serie di procedure e standard volte a proteggere e rispettare i propri diritti di proprietà intellettuale. I dipendenti e il personale hanno la responsabilità, nei confronti dell'azienda e dei clienti, di rispettare le regole per l'utilizzo della proprietà intellettuale di Brightcyde e di terzi.

Brightcyde fornisce ai dipendenti e al personale tutti i mezzi e opportunità per lavorare a distanza al fine di soddisfare specifiche esigenze dei Clienti o aziendali. Per questo, gli utenti devono ricevere un'adeguata formazione sull'utilizzo consapevole dei dispositivi informatici.

6 CONTROLLO DEGLI ACCESSI

Un efficace controllo degli accessi riduce il rischio di modifica o distruzione accidentale o intenzionale dei dati, oltre a proteggere dall'accesso o dalla diffusione non autorizzati.
L'accesso alle informazioni deve essere commisurato al ruolo aziendale di un individuo e ai concetti di "*least-privilege*" e "*need to know*", dove i livelli minimi di accesso sono concessi in base alla loro necessità di accedere a quelle informazioni per le loro esigenze aziendali richieste, al loro ruolo e la natura delle informazioni a cui stanno cercando di accedere.
L'accesso privilegiato deve essere adeguatamente autorizzato e limitato a una durata definita con monitoraggio e supervisione adeguati.

7 PROTEZIONE E SICUREZZA DEI DATI

Ogni dipendente presente all'interno di Brightcyde è responsabile della protezione di tutte le informazioni riservate in suo possesso, compresi i dati personali dei dipendenti, dei clienti e fornitori.

La mancata protezione dei dati personali potrebbe causare un danno per l'individuo in termini di perdita finanziaria, danno alla reputazione o svantaggio sociale o economico. Tale mancanza potrebbe anche comportare gravi sanzioni finanziarie per Brightcyde come risultato di multe legali o regolamentari, danni alla reputazione e al marchio Brightcyde e potrebbe influire su future opportunità.

8 CICLO DI VITA DELLO SVILUPPO DEL SISTEMA SICURO

Pratiche di sviluppo e progettazione non sicure portano a costose vulnerabilità nel sistema che possono passare inosservate e portare ad accesso non autorizzato, modifica o distruzione dei dati.

Di conseguenza, Brightcyde richiede una gestione accurata e sicura dei processi di sviluppo dei sistemi e dei processi di change management con l'implementazione di controlli appropriati durante tutto il ciclo di vita dello sviluppo del sistema (SDLC).

Anche i sistemi acquistati o prodotti esternamente devono essere conformi agli stessi standard minimi del software sviluppato internamente.

9 DISASTER RECOVERY E BUSINESS CONTINUITY

Per minimizzare il rischio dell'interruzione del business a causa di un evento inaspettato o di una crisi, è necessario implementare un efficace piano di disaster recovery (DR) e business continuity (BC).

Il piano di Business Continuity è necessario per preparare adeguatamente Brightcyde ad un'interruzione dei servizi aziendali. Il piano deve essere implementato e testato per le funzioni aziendali critiche e le applicazioni critiche.

La pianificazione del piano di Disaster Recovery prepara proattivamente Brightcyde a rispondere nel caso di un imprevisto evento o crisi. I piani di Disaster Recovery devono essere documentati, aggiornati e prontamente disponibili a tutte le funzioni coinvolte.

10 COMPLIANCE

Stabilire un efficace programma di conformità è fondamentale per valutare se l'efficacia dei controlli è allineata alle linee guida emesse da Brightcyde in materi di Sicurezza delle Informazioni.

Una procedura formale di valutazione del rischio per la sicurezza delle informazioni deve essere implementata e aggiornata su base regolare. Il processo di valutazione del rischio per la sicurezza delle informazioni deve essere allineato con il programma annuale di conformità e i risultati delle valutazioni del rischio producono un piano d'azione annuale con dettagli sulla risoluzione delle lacune identificate.

Il piano d'azione prioritario dovrebbe essere basato sull'impatto aziendale e identificare il periodo di tempo richiesto per la correzione che è commisurato al livello di rischio.