INDICE

FUNZIONE	DATA	NOME	FIRMA
Direzione	26.03.2020	Tonveronachi Nicola	

SCOPO E OBIETTIVI

La direzione di CSEL S.p.A. ha definito, ha divulgato e si impegna a mantenere attiva a tutti i livelli della propria organizzazione la presente politica per la Gestione della Sicurezza delle Informazioni e la protezione delle persone fisiche con riguardo al trattamento dei dati personali.

Lo scopo della presente policy è di garantire la tutela e la protezione da tutte le minacce, interne o esterne, intenzionali o accidentali, delle informazioni e dei dati personali gestiti da CSEL S.p.A. sia come Titolare del Trattamento sia come Responsabile Esterno al Trattamento nell'ambito delle proprie attività in accordo con le indicazioni fornite dallo standard ISO/IEC 27001 e dalle linee guida contenute nello standard ISO/IEC 27002 nelle loro ultime versioni e nel rispetto delle prescrizioni previste dal Regolamento UE 2016/679.

CAMPO DI APPLICAZIONE

La presente politica si applica indistintamente a tutti gli organi e i livelli dell'Azienda.

L'attuazione della presente politica è obbligatoria per tutto il personale e deve essere inserita nella regolamentazione degli accordi con qualsiasi soggetto esterno che, a qualsiasi titolo, possa essere coinvolto con il trattamento di informazioni e dei dati personali che rientrano nel campo di applicazione del Sistema di Gestione aziendale (SGSI).

L'azienda consente la comunicazione e la diffusione delle informazioni verso l'esterno solo per il corretto svolgimento delle attività aziendali che devono avvenire nel rispetto delle regole e delle norme cogenti.

POLICY

Il patrimonio informativo e dei dati personali da tutelare è costituito dall'insieme delle informazioni gestite attraverso i servizi forniti e localizzate in tutte le sedi dell'azienda e presso i data center ove sono gestite le informazioni aziendali.

È necessario assicurare:

- la confidenzialità delle informazioni: ovvero le informazioni devono essere accessibili solo da chi è autorizzato.
- l'integrità delle informazioni: ovvero proteggere la precisione e la completezza delle informazioni e dei metodi per la loro elaborazione.
- la disponibilità delle informazioni: ovvero che gli utenti autorizzati possano effettivamente accedere alle informazioni e ai beni collegati nel momento in cui lo richiedono.
- la leicità del trattamento dei dati personali gestiti dall'organizzazione secondo quanto prescritto dall'art 6 del Regolamento UE 2016/679.
- il rispetto dei diritti degli interessati in materia di dati personali nel rispetto del CAPO III del Regolamento UE 2016/679.

La mancanza di adeguati livelli di sicurezza può comportare il danneggiamento dell'immagine aziendale, la mancata soddisfazione del cliente, il rischio di incorrere in sanzioni legate alla violazione delle normative vigenti nonché danni di natura economica e finanziaria. Un adeguato livello di sicurezza è altresì basilare per la condivisione delle informazioni.

L'azienda identifica tutte le esigenze di sicurezza tramite l'analisi dei rischi che consente di acquisire consapevolezza sul livello di esposizione a minacce del proprio sistema informativo. La valutazione del rischio permette di valutare le potenziali conseguenze e i danni che possono derivare dalla mancata applicazione di misure di sicurezza al sistema informativo e quale sia la realistica probabilità di attuazione delle minacce identificate.

I risultati di questa valutazione determinano le azioni necessarie per gestire i rischi individuati e le misure di sicurezza più idonee.

I principi generali della gestione della sicurezza delle informazioni abbracciano vari aspetti:

- Deve esistere un catalogo costantemente aggiornato degli asset aziendali rilevanti ai fini della gestione delle informazioni.
- Le informazioni devono essere classificate in base al loro livello di criticità, in modo da essere gestite con livelli di riservatezza ed integrità coerenti ed appropriati.
- Per garantire la sicurezza delle informazioni, ogni accesso ai sistemi deve essere sottoposto ad una procedura d'identificazione e autenticazione. Le autorizzazioni di accesso alle informazioni devono essere differenziate in base al ruolo ed agli incarichi ricoperti dai singoli individui, in modo che ogni utente possa accedere alle sole informazioni di cui necessita, e devono essere periodicamente sottoposte a revisione.
- Deve essere incoraggiata la piena consapevolezza delle problematiche relative alla sicurezza delle informazioni in tutto il personale (dipendenti e collaboratori) a partire dal momento della selezione e per tutta la durata del rapporto di lavoro.
- Per poter gestire in modo tempestivo gli incidenti, tutti devono notificare qualsiasi problema relativo alla sicurezza. Ogni incidente deve essere gestito come indicato nelle procedure e, laddove l'incidente porti ad una violazione di dati personali che possa compromettere le libertà e i diritti dei soggetti interessati attivare, la notifica all'Autorità Garante nel rispetto delle prescrizioni regolamentarie sul Data Breach.
- Deve essere assicurata la conformità con i requisiti legali e con i principi legati alla sicurezza delle informazioni nei contratti con le terze parti che verranno disciplinati con specifici technical agreement laddove si configurino come responsabili e/o sub_responsabili al trattamento dei dati personali ai sensi dell'art 28 del Regolamento UE 2016/679.
- Deve essere predisposto un piano di continuità che permetta all'azienda di affrontare efficacemente un evento imprevisto, garantendo il ripristino dei servizi critici in tempi e con modalità che limitino le conseguenze negative sulla missione aziendale.

- Gli aspetti di sicurezza devono essere inclusi in tutte le fasi di progettazione, sviluppo, esercizio, manutenzione, assistenza e dismissione dei sistemi e dei servizi informatici.
- Devono essere garantiti il rispetto delle disposizioni di legge, di statuti, regolamenti o obblighi contrattuali e di ogni requisito inerente la sicurezza delle informazioni, riducendo al minimo il rischio di sanzioni legali o amministrative, di perdite rilevanti o danni alla reputazione.

RIESAME

La Direzione verificherà periodicamente e regolarmente o in concomitanza di cambiamenti significativi l'efficacia e l'efficienza del Sistema di Gestione della Sicurezza delle Informazioni, in modo da assicurare un supporto adeguato all'introduzione di tutte le migliorie necessarie e in modo da favorire l'attivazione di un processo continuo, con cui viene mantenuto il controllo e l'adeguamento della policy in risposta ai cambiamenti dell'ambiente aziendale, del business, delle condizioni legali.

L'amministratore di sistema e il Resp. del Sistema di gestione hanno la responsabilità del riesame della politica della sicurezza delle informazioni.

Il riesame dovrà verificare lo stato delle azioni preventive e correttive e l'aderenza al presente documento di politica. Dovrà tenere conto di tutti i cambiamenti che possono influenzare l'approccio dell'azienda alla gestione della sicurezza delle informazioni, includendo i cambiamenti organizzativi, l'ambiente tecnico, la disponibilità di risorse, le condizioni legali, regolamentari o contrattuali e dei risultati dei precedenti riesami. Particolare attenzione sarà prestata agli incidenti segnalati relativi alla sicurezza delle informazioni e alle tendenze relative alle minacce e vulnerabilità.

Il risultato del riesame dovrà includere tutte le decisioni e le azioni relative al miglioramento dell'approccio aziendale alla gestione della sicurezza delle informazioni, dei controlli e nell'allocazione delle risorse e delle responsabilità. Il risultato del riesame dovrà includere tutte le decisioni e le azioni relative al miglioramento dell'approccio aziendale alla gestione della sicurezza delle informazioni, dei controlli e nell'allocazione delle risorse e delle responsabilità.

IMPEGNO DELLA DIREZIONE

La direzione, impegnata direttamente nel miglioramento continuo del sistema di gestione della sicurezza delle informazioni, sostiene attivamente la sicurezza dell'azienda tramite un chiaro indirizzo, un impegno evidente, degli incarichi espliciti e il riconoscimento delle responsabilità relative alla sicurezza delle informazioni.

L'impegno della direzione si attua tramite una struttura i cui compiti sono:

- garantire che siano identificati tutti gli obiettivi relativi alla sicurezza delle informazioni e che questi incontrino i requisiti aziendali;
- stabilire i ruoli aziendali e le responsabilità per lo sviluppo e il mantenimento del SGSI;

- fornire risorse sufficienti alla pianificazione, implementazione, organizzazione, controllo, revisione, gestione e miglioramento continuo del SGSI;
- controllare che il SGSI sia integrato in tutti i processi aziendali e che procedure e controlli siano sviluppati efficacemente;
- monitorare i cambiamenti dell'esposizione alle minacce delle informazioni chiave dell'azienda e analizzare gli incidenti alla sicurezza, rivedendo i criteri per l'accettazione del rischio e i livelli di rischio accettabili;
- approvare e sostenere tutte le iniziative volte al miglioramento della sicurezza;
- attivare programmi per la diffusione della consapevolezza e della cultura della sicurezza delle informazioni.