DOCUMENTO
POLITICA AZIENDALE PER LA SICUREZZA DELLE INFORMAZIONI
("SECURITY POLICY")

INDICE

Revisione	Data	Descrizione	Redatto	Approvato
00	11.05.2021	Prima emissione	RSGQ	Direttore
01	03.04.2023	Riesame a cura della Direzione	RSI	Direttore
02	15.04.2025	Riesame a cura della Direzione	RSI	Direttore

1. CAMPO D'APPLICAZIONE, SCOPO E DESTINATARI

Brescia Infrastrutture S.r.l. si impegna a rispettare le leggi e i regolamenti applicabili relativi alla sicurezza delle informazioni. Questa Politica stabilisce i principi di base con cui Brescia Infrastrutture S.r.l. protegge le risorse informative da tutte le minacce, siano esse organizzative o tecnologiche, interne o esterne, accidentali o intenzionali.
I destinatari di questo documento sono tutti i dipendenti, permanenti o temporanei, e tutti i collaboratori e fornitori di servizi informatici (es. Brescia Mobilità S.p.A.) che lavorano per conto dell'Azienda.

2. DOCUMENTI DI RIFERIMENTO

- UNI CEI EN ISO/IEC 27001: 2017 – Tecnologie informatiche – tecniche di sicurezza – Sistemi di gestione per la sicurezza dell'informazione - requisiti.
- ISO/IEC 27701: 2019 – Security techniques – extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management – Requirements and guidelines.

3. IMPEGNI DELLA DIREZIONE

Nell'ambito di questa politica sono stati individuati i seguenti impegni della Direzione, individuali o di tutti:

1. adoperarsi per garantire la riservatezza delle informazioni;
2. mantenere l'integrità delle informazioni;
3. assicurare la disponibilità dei servizi informatici;
4. rispettare i requisiti normativi, legislativi e le regole interne;
5. formare il personale alla sicurezza delle informazioni;
6. tenere traccia e studiare qualsiasi incidente, reale o presunto, che interessi la sicurezza delle informazioni;
7. stabilire regole, elaborare piani e adottare misure per attuare la migliore politica di sicurezza delle informazioni.

La responsabilità della applicazione e del rispetto della Politica di sicurezza delle informazioni spetta a chiunque lavori per o con l'Azienda e abbia accesso ai servizi informativi dall'Azienda.
La Direzione di Brescia Infrastrutture S.r.l. assicura:

- ⇒ il monitoraggio e la verifica degli obiettivi della Politica Aziendale per la sicurezza delle informazioni;
- ⇒ il riesame della Politica Aziendale (con cadenza almeno annuale) affinché sia allineata agli eventuali e significativi cambiamenti intervenuti nell'organizzazione e/o nelle tecnologie utilizzate per la protezione delle informazioni;
- ⇒ l'impegno a garantire la continuità operativa dei processi che concorrono alla missione dell'Azienda, richiedendo all'Amministratore di Sistema di Brescia Mobilità S.p.A. il costante e puntuale aggiornamento del Piano di Continuità di Servizio (*Business Continuity Plan – BCP*).
- ⇒ l'impegno a identificare, classificare e registrare le risorse hardware e software utilizzate da Brescia Infrastrutture S.r.l., al fine di tracciare l'intero "ciclo di vita";
- ⇒ l'impegno al controllo degli accessi fisici e logici per minimizzare gli impatti delle minacce ai sistemi di elaborazione delle informazioni dovuti a danni o intrusioni, fermo restando il divieto di controllo dei lavoratori;
- ⇒ la diffusione della presente politica a tutto il personale di Brescia Infrastrutture S.r.l.

4. OBIETTIVI SPECIFICI

Brescia Infrastrutture S.r.l., nell'ambito dell'impegno al miglioramento continuo, nell'ottica della prevenzione, ha definito i seguenti obiettivi specifici in ambito sicurezza delle informazioni che l'Azienda intende perseguire nel medio / lungo termine:

1. garantire un adeguato livello di consapevolezza del personale e dei collaboratori attraverso appositi corsi di formazione, circa la loro responsabilità rispetto alla sicurezza delle informazioni;
2. garantire un adeguato livello di consapevolezza dei fornitori esterni di servizi informatici al fine di assicurare il rispetto dei requisiti di sicurezza delle informazioni;

3. mantenere allineato il sistema di gestione della sicurezza delle informazioni rispetto ai cambiamenti nelle procedure interne e delle norme di legge in materia di sicurezza delle informazioni;
4. garantire un livello adeguato dei requisiti di riservatezza, integrità e disponibilità nei servizi erogati attraverso specifici applicativi;
5. limitare l'utilizzo delle chiavette usb ai dipendenti e ai fornitori per lo scambio di documentazione digitale, incentivando l'utilizzo del cloud aziendale;
6. valutare il rischio di furto/diffusione del patrimonio intellettuale dell'Azienda e vigilare sul comportamento del personale dipendente attuando presidi e azioni di miglioramento.

Il Direttore
Ing. Alberto Merlini