OpenCity Labs S.r.l.

Via S. Francesco d'Assisi 10 - 38122 Trento
P.IVA e C.F.: 02649840226
e-mail: amministrazione@opencitylabs.it
pec: opencitylabs@pec.it
web: www.opencitylabs.it
tel: +39 0461 917437

Politica 01

Politica della sicurezza delle informazioni

Versione	Stato	Data	Redazione	Approvazione
0.0	Approvata	30/05/2023	Gabriele Francescotto	Gabriele Francescotto

La presente Politica descrive i principi generali di sicurezza delle informazioni definiti da OpenCity al fine di sviluppare un efficiente e sicuro Sistema di Gestione della Sicurezza delle Informazioni.

Opencity ritiene che la sicurezza delle informazioni rappresenti un fattore critico di successo per quanto riguarda i processi di progettazione, sviluppo ed erogazione dei propri servizi.

Per OpenCity la sicurezza delle informazioni ha come obiettivo primario la protezione dei dati e delle informazioni, della struttura tecnologica, fisica, logica ed organizzativa. Questo significa ottenere e mantenere, nell'ambito del campo di applicazione definito un Sistema di Gestione per la Sicurezza dell'Informazione (SGSI). Per **sicurezza delle informazioni** si intende l'insieme delle politiche e delle misure di controllo volte:

1. ad assicurare **Riservatezza, Integrità e Disponibilità** delle informazioni
2. a minimizzare i **Rischi relativi alla sicurezza** delle informazioni

Nell'ambito della gestione dei servizi offerti da OpenCity gli obiettivi generali del SGSI sono quindi:

- garantire i migliori standard, ottimizzando e razionalizzando i processi e gli strumenti aziendali;
- garantire l'efficacia del SGSI;
- mantenere un'elevata immagine aziendale;
- la completa osservanza dei livelli di servizio stabiliti con i clienti;
- la soddisfazione del cliente;
- il rispetto delle normative vigenti e degli standard nazionali e internazionali di sicurezza.

Per questo motivo OpenCity ha sviluppato un sistema di gestione sicura delle informazioni seguendo i requisiti specificati della Norma ISO 27001:2022 e delle leggi cogenti come mezzo per gestire la sicurezza delle informazioni nell'ambito della propria attività.

La politica per la sicurezza delle informazioni di OpenCity si applica a tutto il personale interno ed alle terze parti che collaborano alla gestione delle informazioni ed a tutti i processi e risorse coinvolte nella progettazione, realizzazione, avviamento ed erogazione continuativa nell'ambito del campo di applicazione del SGSI che viene definito come

Sviluppo e erogazione di Saas (Software as a service).

Con la presente Politica della sicurezza la Direzione di OpenCity si impegna a garantire la sicurezza delle informazioni, degli strumenti fisici, logici e organizzativi atti al trattamento delle informazioni in tutti i processi aziendali attraverso modalità organizzative e operative volte ad ottenere elevati livelli di Cybersecurity basata sulle funzioni Identify, Protect, Detect, Respond, Recover.

In particolare la Direzione si impegna a:

1. Definire ruoli, responsabilità e profili di accesso in relazione ai processi aziendali.
2. Definire politiche, procedure e strumenti gestionali finalizzati a mantenere adeguati livelli di protezione
3. Garantire che l'organizzazione e le terze parti abbiano la piena conoscenza delle informazioni gestite e la valutazione della loro criticità, al fine di agevolare l'implementazione degli adeguati livelli di protezione.
4. Garantire l'accesso sicuro alle informazioni, in modo da prevenire trattamenti non autorizzati o realizzati senza i diritti necessari.
5. Garantire che l'organizzazione e le terze parti collaborino al trattamento delle informazioni adottando procedure volte al rispetto di adeguati livelli di sicurezza.
6. Garantire che l'organizzazione e le terze parti che collaborano al trattamento delle informazioni, abbiano piena consapevolezza delle problematiche relative alla sicurezza.
7. Garantire la rilevazione di eventi anomali, incidenti e vulnerabilità dei sistemi informativi al fine di rispettare la sicurezza e la disponibilità dei servizi e delle informazioni.
8. Garantire che le anomalie e gli incidenti aventi ripercussioni sul sistema informativo e sui livelli di sicurezza aziendale siano tempestivamente riconosciuti e correttamente gestiti attraverso efficienti sistemi di prevenzione, comunicazione e reazione al fine di minimizzare l'impatto sul business.
9. Garantire che l'accesso alle sedi ed ai singoli asset aziendali avvenga esclusivamente da parte di personale autorizzato.

10. Garantire il rispetto della norma ISO 27001, dei requisiti di legge ed il rispetto degli impegni di sicurezza stabiliti nei contratti con le terze parti.
11. Garantire la business continuity aziendale e il disaster recovery, attraverso l'applicazione di procedure di sicurezza stabilite.
12. Promuovere il miglioramento continuo del sistema di gestione per la sicurezza delle informazioni

La Politica della sicurezza delle informazioni viene costantemente aggiornata per assicurare il miglioramento continuo ed è condivisa con l'organizzazione, le terze parti ed i clienti, attraverso un sistema intranet e specifici canali di comunicazione.

La Direzione è responsabile del sistema di gestione sicura delle informazioni, in coerenza con l'evoluzione del contesto aziendale e di mercato, valutando eventuali azioni da intraprendere a fronte di eventi come:

- evoluzioni significative del business;
- nuove minacce rispetto a quelle considerate nell'attività di analisi del rischio;
- significativi incidenti di sicurezza;
- evoluzione del contesto normativo o legislativo in materia di trattamento sicuro delle informazioni.