POLITICA PER LA SICUREZZA DELLE INFORMAZIONI

Lo scopo della presente politica è descrivere i principi generali di sicurezza delle informazioni definiti da Circet Italia al fine di sviluppare un efficiente e sicuro Sistema di Gestione della Sicurezza delle Informazioni ai sensi della ISO 27001:2022.
La sicurezza delle informazioni ha come obiettivo primario la protezione dei dati e delle informazioni, della struttura tecnologica, fisica, logica ed organizzativa, responsabile della loro gestione.

La sicurezza delle informazioni si concretizza nelle caratteristiche di:

- Riservatezza: assicurare che l'informazione sia accessibile solo a chi è autorizzato all'accesso;
- Integrità: salvaguardare l'accuratezza e la completezza dell'informazione e dei metodi per processarla;
- Disponibilità: assicurare che gli utenti autorizzati abbiano accesso all'informazione e agli asset associati quando richiesto.

AMBITO DI APPLICAZIONE

La politica per la sicurezza delle informazioni si applica a tutto il personale interno ed alle terze parti (es: fornitori di servizi, manutenzioni, supporto…) che collaborano alla gestione delle informazioni ed a tutti i processi e alle risorse coinvolte nella progettazione, realizzazione, avviamento ed erogazione continuativa nell'ambito dei servizi.
La presente politica si applica a tutti i processi inclusi nel SGSI (Sistema Di Gestione Della Sicurezza Delle Informazioni).

OBIETTIVI

Nell'ambito della gestione dei servizi offerti Circet Italia assicura:

- la garanzia di aver incaricato partner affidabili al trattamento del proprio patrimonio informativo;
- 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 internazionali di sicurezza.

PRINCIPI

La politica della sicurezza delle informazioni si ispira ai seguenti principi:

a. garantire il controllo degli accessi;
b. stabilire la classificazione (e il trattamento) delle informazioni;
c. garantire la sicurezza fisica e ambientale del proprio luogo di lavoro;
d. adottare temi destinati all'utente finale, quali ad esempio:
    1. uso accettabile degli asset;
    2. best practices riguardanti scrivania e schermo puliti;
    3. adeguato trasferimento delle informazioni;
    4. uso regolamentato dei dispositivi mobili e telelavoro;
    5. limitazioni all'installazione e all'utilizzo di software;
e. stabilire ed effettuare backup ad intervalli regolari;
f. stabilire procedure per il trasferimento di informazioni in modo protetto;
g. prevedere protezioni dai malware;

h. individuare, monitorare e gestire le vulnerabilità tecniche riscontrate;
i. prevedere, se necessario, controlli crittografici;
j. garantire la sicurezza delle comunicazioni;
k. rispettare le normative vigenti in ambito privacy e protezione dei dati personali;
l. fornire indicazioni sull'uso di sistemi (generativi) di IA (accessibili al pubblico) da parte dei dipendenti definendo le attività consentite e quelle vietate;
m. regolamentare i rapporti con i fornitori in ottica ISO 27001.

ATTUAZIONE E RESPONSABILITÀ

La politica della sicurezza delle informazioni di Circet Italia rappresenta l'impegno dell'organizzazione nei confronti dei dipendenti, dei clienti e di terze parti a garantire la sicurezza delle informazioni, degli strumenti fisici, logici e organizzativi atti al trattamento delle informazioni in tutte le attività.
La presente politica è resa disponibile a tutte le parti interessate, sia interne che esterne. Per sensibilizzare e coinvolgere dipendenti, subappaltatori, fornitori, clienti e stakeholder rilevanti la politica è pubblicata sul sito www.circet.it. Infatti, tutti sono responsabili della sicurezza delle informazioni sotto il proprio controllo, con il supporto del team IT, che fornisce consulenza e assistenza nel rispetto della presente politica.
Circet Italia definisce, con cadenza almeno annuale, il contesto in cui opera, gli attori coinvolti, le opportunità e i possibili rischi impattati sul proprio Sistema di Gestione per la Sicurezza delle Informazioni.
L'Amministratore Delegato è responsabile dell'attuazione e del monitoraggio della presente politica.

SAN GIOVANNI TEATINO, 6 GIUGNO 2025

Fabrizio Perletta
Chief Executive Officer

ISO 27001:2022