

INDICE

INDICE	1
SCOPO E OBIETTIVI	2
CAMPO DI APPLICAZIONE	2
POLICY	2
RIESAME	3
IMPEGNO DELLA DIREZIONE.....	3

Redatto/Verificato
da

Approvato

Funzione
Information Security Manager
Direzione

SCOPO E OBIETTIVI

LA Cassa Edile di Roma e Provincia definisce e si impegna a mantenere attiva a tutti i livelli della propria organizzazione la politica per la Gestione della Sicurezza delle Informazioni.

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 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.

CAMPO DI APPLICAZIONE

La presente politica si applica indistintamente a tutti gli organi e i livelli della Cassa Edile di Roma e Provincia, viene divulgata al personale interno ed inserita nella regolamentazione degli accordi con i soggetti esterni che, a qualsiasi titolo, possano essere coinvolti con il trattamento di informazioni che rientrano nel campo di applicazione del Sistema di Gestione della Sicurezza delle Informazioni (SGSI).

POLICY

Il patrimonio informativo da tutelare è costituito dall'insieme delle informazioni gestite attraverso i servizi forniti e localizzati presso la Cassa Edile di Roma e Provincia ove sono gestite le informazioni aziendali.

È prioritario assicurare:

- la confidenzialità delle informazioni: le informazioni devono essere accessibili solo da chi è autorizzato.
- l'integrità delle informazioni: la protezione delle informazioni e dei metodi per la loro elaborazione.
- la disponibilità delle informazioni: le informazioni devono essere sempre disponibili e reperibili dal personale autorizzato che ne fa richiesta.

I principi della gestione della sicurezza delle informazioni comprendono:

- un catalogo costantemente aggiornato degli asset aziendali rilevanti ai fini della gestione delle informazioni;
- una classificazione delle informazioni in base al loro livello di criticità, in modo da essere gestite con livelli di riservatezza ed integrità coerenti ed appropriati.

L'impegno della Cassa Edile si evidenzia in una serie di procedure rispettate a garanzia della sicurezza delle informazioni. In particolare:

- Ogni accesso ai sistemi viene sottoposto ad una procedura d'identificazione a doppio fattore e relativa autenticazione. Le autorizzazioni di accesso alle informazioni sono 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 vengono periodicamente sottoposte a revisione.
- Viene 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.
- La gestione tempestiva degli incidenti, la notifica di problematiche relative alla sicurezza può essere effettuata da chiunque. Ogni incidente viene gestito nell'immediato ed analizzato come definito da procedura emessa;

- Viene assicurata la conformità con i requisiti legali e con i principi legati alla sicurezza delle informazioni nei contratti con le terze parti;
- Viene predisposto un piano di continuità che permette alla Cassa Edile 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 vengono inclusi in tutte le fasi di progettazione, sviluppo, esercizio, manutenzione, assistenza e dismissione dei sistemi e dei servizi informatici.
- Vengono 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 con il supporto del Responsabile del Sistema verifica periodicamente e regolarmente o in concomitanza di cambiamenti significativi l'efficacia del Sistema di Gestione per la Sicurezza delle Informazioni, in modo da assicurare un supporto adeguato all'introduzione di migliorie necessarie a favorire l'attivazione di un processo continuo di crescita. Costantemente viene mantenuto il controllo e l'adeguamento delle policy in risposta ai cambiamenti dell'ambiente interno, del business, delle condizioni legali. Il risultato del riesame include tutte le decisioni e le azioni relative al miglioramento della 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 all'interno della Cassa Edile di Roma e Provincia tramite un chiaro indirizzo, un impegno evidente, degli incarichi espliciti e il riconoscimento delle responsabilità relative.

L'impegno della Direzione e del Responsabile del Sistema di gestione per la Sicurezza delle Informazioni 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 della Cassa Edile;
- 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;
- controllare che il Sistema sia integrato in tutti i processi interni e che procedure ed i controlli siano sviluppati efficacemente;
- monitorare i cambiamenti dell'esposizione alle minacce delle informazioni chiave e analizzare gli incidenti alla sicurezza, rivedendo nel tempo 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.