INFO DOCUMENTO

TITOLO DEL DOCUMENTO

PR 5.2 - Information Security Management System Policy

CODICE DOCUMENTO
PR 5.2

DATA
27 Settembre 2024

REVISIONE
3

CAMPO DI APPLICAZIONE

DISTRIBUTION

Restricted	[ ]
Internal only	[ ]
Stakeholder	[ ]
Public	[●]

LISTA DELLE REVISIONI

REVISIONI

Revisioni	Data	Descrizione	Autore
1	01/02/2023	Documento originale – versione ITA	eCore
2	19/07/2024	Rinominato documento	Mirko Bersani
3	27/09/2024	Aggiornata Vision	Mirko Bersani

eCore Holding s.r.l
via Pastore 3
29017 Fiorenzuola d'Arda (Piacenza) Italy
Tel 0523.985811 www.ecoreholding.it

1. Scopo del documento

Lo scopo di questo documento è quello di descrivere i principi generali della sicurezza delle informazioni definiti da eCore, al fine di sviluppare un sistema di gestione della sicurezza delle informazioni (ISMS) efficiente e sicuro.

2. Information Security Policy

eCore è la holding di queste aziende:

- ELFO S.r.l. (sviluppo software custom)
- Reimagine S.r.l. (Vendita di prodotti e servizi digitali)

In linea con il Purpose[i] di ELFO S.r.l. e la Vision [ii]di Reimagine, **eCore Holding** (di seguito **eCore**) si impegna a preservare la riservatezza, l'integrità e la disponibilità di tutte le informazioni fisiche ed elettroniche all'interno della propria organizzazione, al fine di garantirne l'alta disponibilità, la conformità normativa e contrattuale e l'immagine commerciale.

I requisiti di sicurezza delle informazioni continueranno a essere allineati agli obiettivi di **eCore** e questo ISMS è inteso come un meccanismo abilitante per la condivisione delle informazioni, per le operazioni digitali, per la gestione dei dati e per la riduzione a livelli accettabili dei rischi legati alle informazioni.

L'attuale piano strategico aziendale ed il modello di gestione del rischio di **eCore** forniscono il contesto per l'identificazione, la valutazione e il controllo dei rischi legati alle informazioni attraverso la creazione e il mantenimento di un ISMS.

Lo Steering Committee di eCore ha assegnato ad ELFO la responsabilità di svolgere tutte le attività relative alla ISO 27001 per tutte le società del gruppo.

La Valutazione dei rischi, la Dichiarazione di applicabilità e il Piano di trattamento dei rischi, identificano le modalità di controllo dei rischi legati alle informazioni. Il Chief Operating Officer (COO) sarà responsabile della gestione e del mantenimento della valutazione dei rischi. Qualora necessario, possono essere effettuate ulteriori valutazioni del rischio per determinare i controlli appropriati per rischi specifici.

Nello specifico, la continuità operativa, i controlli operativi dell'infrastruttura ICT, il controllo degli accessi ai sistemi e la segnalazione degli incidenti di sicurezza delle informazioni sono fondamentali per questa politica. Gli obiettivi di controllo per ciascuna di queste aree sono contenuti nel presente documento e sono supportati da specifiche politiche e procedure documentate.

Tutti i dipendenti e i collaboratori di **eCore** ed alcune figure esterne identificate nell'ISMS sono tenuti a rispettare questa politica e l'ISMS che la implementa. Tutti i dipendenti/collaboratori, ed alcune figure esterne, riceveranno i requisiti necessari e saranno tenuti a sostenere un'adeguata formazione. Le conseguenze della violazione della politica di sicurezza delle informazioni sono definite nella politica disciplinare dell'Organizzazione, nei contratti e negli accordi con terzi.

L'ISMS è soggetto a revisione e miglioramento continui e sistematici.

Lo Steering Committee di **eCore** ha istituito un **Information Security Committee**, presieduto dal Chief Operating Officer (COO), dal Chief Innovation Officer (CIO), dal Chief Technology Officer (CTO) e dal Team ICT per supportare il framework ISMS e rivedere periodicamente la politica di sicurezza.

eCore si impegna a ottenere la certificazione del proprio ISMS in base allo standard internazionale ISO/IEC 27001:2022.

Questa politica sarà rivista almeno una volta all'anno, per rispondere a qualsiasi cambiamento nella valutazione del rischio o nel piano di trattamento del rischio.

In questa politica, la "sicurezza delle informazioni (information security)" è definita come:

Preservare la disponibilità, la riservatezza e l'integrità delle risorse fisiche (beni) e delle informazioni dell'organizzazione eCore.

Preservare

Significa che la direzione, tutti i dipendenti e il personale a tempo pieno o part-time, i liberi professionisti, i consulenti di progetto e tutte le parti esterne hanno, e saranno resi consapevoli, delle loro responsabilità (definite nelle loro job description o nei loro contratti) di preservare la sicurezza delle informazioni, di segnalare le violazioni della sicurezza (in linea con la politica e le procedure) e di agire in conformità con i requisiti dell'ISMS. Tutti i dipendenti riceveranno una formazione sulla sicurezza delle informazioni ed i dipendenti più specializzati riceveranno una formazione specializzata sulla sicurezza delle informazioni.

la disponibilità,

Si intende che le informazioni e gli asset associati devono essere accessibili agli utenti autorizzati quando necessario e quindi fisicamente sicuri. La rete informatica deve essere resiliente ed **eCore** deve essere in grado di rilevare e rispondere rapidamente agli incidenti (come virus e altre minacce informatiche) che minacciano la disponibilità di asset, sistemi e informazioni.

la riservatezza

Si intende garantire che le informazioni siano accessibili solo a chi è autorizzato ad accedervi e quindi impedire l'accesso non autorizzato, sia deliberato che accidentale, alle informazioni e alle conoscenze proprietarie di eCore e ai suoi sistemi, compresi la rete, il sito web, la rete extranet e il sistema di monitoraggio.

e l'integrità

Ovvero la salvaguardia della correttezza e della completezza delle informazioni e dei metodi di elaborazione, ovvero la prevenzione della distruzione deliberata o accidentale, parziale o completa, o della

modifica non autorizzata, sia delle risorse fisiche che dei dati elettronici. Devono essere previsti adeguati piani di emergenza, compresi quelli per reti, sistemi, siti web, extranet e piani di backup dei dati, nonché la segnalazione di incidenti di sicurezza. **eCore** deve rispettare tutte le leggi pertinenti in materia di dati nelle giurisdizioni in cui opera.

delle risorse fisiche (beni)

Gli asset fisici di **eCore** sono sotto il suo controllo e sotto il controllo delle procedure/policy che riguardano i sistemi cloud, le applicazioni, le informazioni di processo, i rack, i server, i laptop ed i personal computer, , gli smartphone, i sistemi di archiviazione di dati fisici e digitali.

e delle informazioni

Le risorse informative comprendono le informazioni archiviate elettronicamente su server, intranet, servizi cloud, PC, laptop, telefoni cellulari e tutte le informazioni trasmesse elettronicamente con qualsiasi mezzo. In questo contesto, i "dati" comprendono anche l'insieme di istruzioni che indicano al sistema (o ai sistemi) come manipolare le informazioni (ovvero i software: sistemi operativi, applicazioni, utilità, ecc.)

dell'organizzazione eCore.

[i] Vogliamo ri-progettare i confini delle possibilità delle applicazioni software nelle organizzazioni complesse. Lavoriamo quotidianamente per spostare l'orizzonte dell'innovazione dei nostri clienti partendo dai loro obiettivi di crescita.
Vogliamo condividere eccellenza tecnologica, competenza e passione per costruire relazioni memorabili.

[ii] Realizzare prodotti software, per semplificare i processi aziendali.