

INFO
DOCUMENTO

TITOLO DEL DOCUMENTO

PR 5.2 - Information Security & Quality Management System Policy

CODICE DOCUMENTO
PR 5.2

DATA
09/10/2026

REVISIONE
5

CAMPO DI
APPLICAZIONE

DISTRIBUTION

Restricted []

Internal only []

Stakeholder []

Public [●]

LISTA DELLE
REVISIONI

REVISIONI

Revisioni	Data	Descrizione	Autore
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
4	27/07/2026	Aggiornato capitolo 2 (esclusione Reimagine e Adeguati ruoli da organigramma)	Paolo Braggion
5	09/10/2026	Integrazione dei requisiti relativi alla Politica della Qualità in conformità alla norma ISO 9001:2015	Paolo Braggion

Indice

1. Scopo del documento	3
2. Information Security Policy	3
3. I nostri principi	5

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.

Il documento costituisce la Politica per la Sicurezza delle Informazioni ai sensi della ISO/IEC 27001:2022 (punto 5.2) e, per le parti che lo riguardano, richiama e integra la Politica per la Qualità definita ai sensi della ISO 9001:2015 (punto 5.2). Si applica a tutte le società del gruppo e a tutti i processi, le sedi, le persone e gli asset inclusi nel campo di applicazione dei sistemi di gestione.

2. Information Security Policy

eCore è la holding di ELFO S.r.l. (sviluppo software custom)

In linea con il Purpose di ELFO S.r.l. e **eCore Holding** (di seguito **eCore**) si impegna a:

- fornire prodotti e servizi software di elevata qualità che soddisfino costantemente i requisiti dei clienti, le aspettative delle parti interessate e i requisiti cogenti applicabili;
- 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; la sicurezza delle informazioni è considerata parte integrante della qualità dei servizi erogati. Pertanto, la tutela di riservatezza, integrità e disponibilità dei dati dei clienti e dei processi aziendali contribuisce direttamente alla conformità dei prodotti e dei servizi e alla soddisfazione degli stakeholder;
- promuovere la cultura del miglioramento continuo del Sistema di Gestione Integrato per la Qualità e la Sicurezza delle Informazioni;
- pianificare e monitorare con continuità gli Obiettivi per la Qualità e la Sicurezza delle Informazioni, definiti e riesaminati annualmente dalla Steering Committee.

I requisiti di sicurezza delle informazioni e gli obiettivi per la qualità continueranno a essere allineati agli obiettivi di **eCore** e questo Sistema di Gestione Integrato (Qualità e Sicurezza) è inteso come un meccanismo abilitante per la condivisione delle informazioni, per le operazioni digitali, per la gestione dei dati, per la soddisfazione del cliente e per la riduzione a livelli accettabili dei rischi legati alle informazioni e ai processi aziendali.

L'attuale piano strategico aziendale ed il modello di gestione del rischio e delle opportunità di **eCore** forniscono il contesto per l'identificazione, la valutazione e il controllo dei rischi legati alle informazioni e all'erogazione dei servizi attraverso la creazione, il mantenimento e il miglioramento continuo di un Sistema di Gestione Integrato. Tale contesto è coerente con l'analisi del contesto dell'organizzazione, delle parti interessate e dei rischi e delle opportunità effettuata nell'ambito del Sistema di Gestione Integrato, secondo un approccio basato sul rischio (risk-based thinking).

Principi della Politica per la Qualità richiamati

Nell'ambito del sistema di gestione integrato, **eCore** applica i seguenti principi, in coerenza con la Politica per la Qualità:

- orientamento al cliente: comprendere e soddisfare le esigenze e le aspettative dei clienti e delle altre parti interessate, tutelandone le informazioni;
- approccio per processi e basato sul rischio: gestire i processi aziendali, inclusi quelli che trattano informazioni, individuando e trattando rischi e opportunità;
- conformità: rispettare i requisiti cogenti, normativi e contrattuali applicabili, comprese tutte le leggi pertinenti in materia di dati nelle giurisdizioni in cui **eCore** opera;
- coinvolgimento e competenza delle persone: assicurare consapevolezza, formazione e responsabilizzazione di tutto il personale;
- miglioramento continuo: migliorare in modo sistematico l'efficacia del sistema di gestione, dei processi e dei controlli di sicurezza;
- gestione dei fornitori e delle parti esterne: assicurare che processi, prodotti e servizi forniti dall'esterno siano controllati anche sotto il profilo della sicurezza delle informazioni.

Governance e responsabilità

Lo Steering Committee di **eCore** ha assegnato ad ELFO la responsabilità di svolgere tutte le attività relative alla ISO 27001 e alla ISO 9001 per tutte le società del gruppo.

La Valutazione dei rischi, la Dichiarazione di applicabilità, il Piano di trattamento dei rischi e la mappatura dei processi identificano le modalità di controllo dei rischi legati alle informazioni e ai livelli di servizio/prodotto. Sono definiti obiettivi misurabili, monitorati e riesaminati periodicamente, in coerenza con gli obiettivi per la qualità. 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, la segnalazione degli incidenti di sicurezza delle informazioni, la soddisfazione del cliente (Customer Satisfaction), il controllo dei processi esternalizzati e il rispetto delle specifiche di progetto sono fondamentali per questa politica.

Gli obiettivi di controllo e gli indicatori di prestazione per ciascuna di queste aree sono contenuti nel presente documento e sono supportati da specifiche politiche, procedure e istruzioni operative documentate.

Tutti i dipendenti e i collaboratori di **eCore** ed alcune figure esterne identificate nell'Sistema di Gestione Integrato sono tenuti a rispettare questa politica e il sistema che la implementa. Tutti i dipendenti/collaboratori, ed alcune figure esterne, riceveranno i requisiti necessari e saranno tenuti a sostenere un'adeguata formazione nell'ambito del piano di formazione e di sviluppo delle competenze. Le conseguenze della violazione della politica di sicurezza delle informazioni e delle procedure di qualità sono definite nella politica disciplinare dell'Organizzazione, nei contratti e negli accordi con terzi.

L'Sistema di Gestione Integrato è soggetto a revisione e miglioramento continui e sistematici.

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

eCore si impegna a mantenere il proprio Sistema di Gestione Integrato conforme agli standard internazionali UNI EN ISO 9001:2015 e ISO/IEC 27001:2022.

Questa politica sarà rivista almeno una volta all'anno, o in occasione del riesame della Direzione, per rispondere a qualsiasi cambiamento nella valutazione del rischio, nel piano di trattamento del rischio, nel contesto dell'organizzazione o nelle esigenze del mercato e delle parti interessate.

La presente Politica Integrata è comunicata, compresa e applicata all'interno dell'organizzazione ed è resa disponibile alle parti interessate rilevanti.

In questa politica, la "sicurezza delle informazioni (information security)" e la "Qualità" sono definite come:

- *Preservare la disponibilità, la riservatezza e l'integrità delle risorse fisiche (beni) e delle informazioni dell'organizzazione **eCore**.*
- *Garantire la conformità dei processi, dei prodotti software e dei servizi digitali forniti, puntando alla costante soddisfazione del cliente e all'eccellenza operativa.*

3. I nostri principi

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 e gli standard qualitativi, di segnalare le violazioni della sicurezza e le non conformità di processo/prodotto (in linea con la politica e le procedure) e di agire in conformità con i requisiti dell'Sistema di Gestione Integrato. Tutti i dipendenti riceveranno una formazione sulla sicurezza delle informazioni e sulla gestione della qualità ed i dipendenti più specializzati riceveranno una formazione specializzata.

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, a garanzia della continuità nell'erogazione di prodotti e servizi ai clienti.

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**, ai dati e alle proprietà dei clienti 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 e anomalie del software. **eCore** deve rispettare tutte le leggi pertinenti in materia di dati e di qualità dei prodotti/servizi 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**.

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.

dell'organizzazione eCore.

Vogliamo condividere eccellenza tecnologica, competenza e passione per costruire relazioni memorabili.

"Realizzare prodotti software, per semplificare i processi aziendali garantendo i più elevati standard qualitativi e di sicurezza delle informazioni."