Manuale del Sistema di Gestione Integrato

Allegato 1

Politica per la qualità

Politica per la sicurezza delle informazioni

Rev.	Data	Causale	Redazione	Verifica	Approvazione AU
01	18.01.2023	Aggiornamento par 7 sui compiti RGSI e Resp. Infrastruttura; eliminazione del resp. Security informatica e unificazione figura RGSI	RGQ/RGSI	RGQ/RGSI	R. Minasola
00	30.03.2022	Prima edizione	RGQ/RGSI	RGQ/RGSI	R. Minasola

INDICE

1. INTRODUZIONE

ELMI opera nel settore dell'**Information Technology come System Integrator,** offrendo consulenza professionale con l'obiettivo di supportare le aziende private e pubbliche nello sviluppo di progetti innovativi e di soluzioni tecnologicamente avanzate.

La Elmi è una PMI Innovativa. La ricerca dei prodotti e delle best practices più innovative, ma anche più solide e strutturate, fanno della ELMI un'azienda altamente qualificata nella Ricerca e Sviluppo. Attualmente, l'azienda è fortemente focalizzata ai temi della *Digital Transformation* con particolare riferimento alle aree tecnologiche inerenti alle aree *Blockchain, Internet of Things, Big Data e Analytics, Intelligenza Artificiale*.

Data la natura delle proprie attività, Elmi considera la sicurezza delle informazioni un fattore irrinunciabile per la protezione del proprio patrimonio informativo ed un fattore di valenza strategica facilmente trasformabile in vantaggio competitivo.
Elmi pone particolare attenzione ai temi riguardanti la sicurezza durante il ciclo di vita di progettazione e sviluppo dei propri servizi e prodotti, che devono essere ritenuti un bene primario dell'azienda.

Il presente documento riporta la politica definita dalla direzione di Elmi s.r.l. in merito alla gestione della qualità e della sicurezza delle informazioni, dei dati e degli asset fisici, al fine di garantire la sicurezza delle stesse e dei dati trattati dall'azienda, in termini di riservatezza, integrità e disponibilità.

2. SCOPO DEL DOCUMENTO

Il presente documento definisce le linee guida in base alle quali è stato definito l'intero Sistema di Gestione Integrato per la Qualità e per la Gestione della Sicurezza delle Informazioni (SGI) di Elmi. Ogni piano e procedura inerente il trattamento della qualità e della sicurezza delle informazioni o che possa avere impatto con la qualità e/o con la sicurezza delle informazioni, deve uniformarsi alla politica delineata nel presente documento.

3. OBIETTIVI DI QUALITA'

La direzione della **Elmi *srl*** al fine di mantenere e migliorare la qualità aziendale vuole comunicare a tutti i dipendenti gli **obiettivi di miglioramento continuo** aziendale.

La Direzione vuole perseguire tutti gli obiettivi indicati per applicare un SGI conforme alla norma UNI EN ISO 9001:2015.
Il principale obiettivo è il mantenimento degli standard produttivi e gestionali consolidati a seguito della implementazione del sistema qualità.

L'obiettivo dovrà essere perseguito mediante:

- la costante e puntuale registrazione di tutte le attività effettuate nei tempi e nei modi richiesti dalla Direzione;
- l'analisi costante dei dati registrati su tutti i tipi di attività;
- la realizzazione di specifici audit interni da parte del RGQ.

Altro obiettivo prioritario è il monitoraggio e la costante valutazione della **soddisfazione del cliente**:

L'obiettivo dovrà essere perseguito mediante:

- Il costante invio dei questionari di soddisfazione del cliente;
- L'emissione di specifici metodi di valutazione della soddisfazione quali - ad esempio - interviste telefoniche, valutazioni presso i clienti, etc.;

- L'analisi puntuale dei dati ottenuti.

- ❑ **il rispetto degli impegni contrattuali espliciti ed impliciti** attraverso la esatta definizione dei requisiti tecnici e cogenti applicabili al contratto, il rispetto dei tempi di consegna;
- ❑ **un costante miglioramento nella definizione e nel controllo dei costi legati a ciascuna commessa**;
- ❑ **il consolidamento della presenza aziendale nel mercato di riferimento** aumentando l'offerta di prodotti a seguito delle evoluzioni dell'offerta in campo informatico;
- ❑ l'acquisizione costante di **nuovi clienti nei nuovi settori che verranno nel tempo sviluppati ed il mantenimento dei clienti storici**;
- ❑ **il miglioramento costante dell'indice di successo del processo commerciale**;
- ❑ la minimizzazione dei reclami;
- ❑ **il rispetto della normativa sulla sicurezza sui luoghi di lavoro**;
- ❑ **il rispetto della normativa in materia di protezione dei dati personali, con adeguamento al regolamento GDPR 2016/679, in vigore dal 25 Maggio 2018**;
- ❑ il rispetto di tutte le prescrizioni relative alla **protezione dei dati personali**;
- ❑ il miglioramento continuo delle competenze di tutte le figure aziendali attraverso il **costante aggiornamento formativo**.

La Direzione intende responsabilizzare a vario titolo tutti i dipendenti dell'azienda nel contribuire ad ottenere tutti gli obiettivi esposti.

4. OBIETTIVI DI SICUREZZA DELLE INFORMAZIONI

L'obiettivo in ottica Sicurezza delle Informazioni della Elmi è garantire un adeguato livello di sicurezza dei dati e delle informazioni nell'ambito della progettazione, sviluppo ed erogazione dei servizi di Data Center, attraverso l'identificazione, la valutazione e il trattamento dei rischi ai quali i servizi stessi sono soggetti.
Il Sistema di Gestione integrato di Elmi definisce un insieme di misure organizzative, tecniche e procedurali a garanzia del soddisfacimento dei sotto elencati requisiti di sicurezza di base:

- **Riservatezza** Confidentiality: affinché tutte le informazioni siano accessibili solo alle persone autorizzate;
- **Integrità** Integrity: per prevenire le modifiche indebite, accidentali o fraudolente alle informazioni;
- **Disponibilità** Availability: per assicurare che gli utenti possano accedere ai dati sulla base dei propri profili specifici di abilitazione in tempi congruenti con le proprie esigenze operative.

Inoltre, con la presente politica, in conformità con quanto già attuato nell'ambito del sistema di gestione della qualità, Elmi intende formalizzare i seguenti obiettivi nell'ambito della sicurezza delle informazioni:

- Preservare al meglio l'immagine dell'azienda quale fornitore affidabile e competente;
- Proteggere al meglio il patrimonio informativo proprio e dei propri clienti;
- Adottare le misure atte a garantire in pieno coinvolgimento del personale e la sua professionalità ed aumentarne il livello di sensibilità e la competenza su temi di sicurezza.
- Rispondere pienamente alle indicazioni delle normative vigenti.

5. AMBITO DI APPLICAZIONE DELLA POLITICA DELLA SICUREZZA DELLE INFORMAZIONI

La Politica per la Sicurezza si applica a tutte le attività svolte da Elmi, ed in particolare all'attività di Product Management, ossia alle attività di progettazione, sviluppo e manutenzione di soluzioni informatiche.

Si applica indistintamente a tutti gli organi dell'Azienda. L'attuazione della presente politica è obbligatoria per tutto il personale Elmi, così come per i Consulenti, e va inserita nell'ambito della regolamentazione degli accordi nei confronti di qualsiasi soggetto esterno che, a qualsiasi titolo, possa venire a conoscenza delle informazioni gestite in azienda.

Il SGI (Sistema di Gestione integrato per la qualità e per la Sicurezza delle Informazioni) si applica a tutte le attività di analisi, progettazione, sviluppo e manutenzione dei prodotti e servizi, ed ai dati ad esse collegati che riguardano il Data Center di Elmi.

Consapevole del fatto che i propri servizi per soggetti esterni possono comportare l'affidamento di dati e informazioni critiche, l'unità organizzativa tecnica opera secondo normative di sicurezza internazionalmente riconosciute.
Per questo motivo si intende adottare le misure, sia tecniche che organizzative, necessarie a garantire al meglio l'integrità, la riservatezza e la disponibilità sia del patrimonio informativo interno che di quello affidato dai propri Clienti.
Su tali basi Elmi ha deciso di porre in essere un Sistema di Gestione integrato per la Qualità e per la Sicurezza delle Informazioni (SGI) definito secondo regole e criteri previsti dalle "best practice" e dagli standard internazionali di riferimento in conformità alle indicazioni della norma internazionale ISO/IEC 27001:2017 Sicurezza delle Informazioni, Tecnologie informatiche – Tecniche per la Sicurezza – Sistemi di Gestione per la Sicurezza delle informazioni.

6. POLICY

Tutte le informazioni, che vengono create o utilizzate dall'Azienda, sono da salvaguardare e debbono essere protette, secondo la classificazione attribuita, dalla loro creazione, durante il loro utilizzo, fino alla loro eliminazione. Le informazioni debbono essere gestite in modo sicuro, accurato e affidabile, e debbono essere prontamente disponibili per gli usi consentiti.
È qui da intendersi con "utilizzo dell'informazione" qualsiasi forma di trattamento che si avvalga di supporti elettronici, cartacei o consenta, in una qualsiasi forma, la comunicazione verbale.
Relativamente all'ambito della progettazione e sviluppo, tale sistema prevede – in conformità alla norma ISO/IEC 27001:2017 – che il Responsabile per la Sicurezza delle Informazioni svolga periodicamente un'analisi dei rischi che tenga in considerazione gli obiettivi strategici espressi nella presente politica, degli incidenti occorsi durante tale periodo e dei cambiamenti strategici, di business e tecnologici avvenuti; l'analisi dei rischi ha lo scopo di valutare il rischio associato ad ogni asset da proteggere rispetto alle minacce individuate.

Di seguito sono riportate le policy definite da Elmi in merito alla sicurezza delle informazioni.

Accettazione

Policy destinate ai Dipendenti, collaboratori, fornitori, partner, appaltatori e tutte le altre terze parti coinvolte nelle attività istituzionali di Elmi con obblighi, responsabilità individuali e istruzioni al fine di proteggere le informazioni, i beni e le risorse di Elmi o affidati a Elmi da terzi.

Accesso

Policy per la gestione e il controllo degli Accessi alle informazioni, beni e risorse della Elmi o affidateLe da terzi; gli accessi devono essere controllati e monitorati sulla base dei seguenti criteri:

- L'accesso è autorizzato solo per le informazioni necessarie (principio della conoscenza minima);
- L'accesso è autorizzato solo per le informazioni riguardanti specifiche attività.

Valutazione

Policy per la gestione e il controllo dei rischi, delle contromisure e degli scenari d'incidente.
Elmi definisce il giusto rapporto tra:

- le spese necessarie per l'attuazione delle misure al fine di proteggere le informazioni, i beni e le risorse di Elmi o affidati a Elmi da terzi;
- i rischi legati all'utilizzo non autorizzato, modifiche o distruzione.

Consapevolezza

Policy atte a garantire la consapevolezza di ogni dipendente, collaboratore, fornitore o terza parte della Politica per la Sicurezza di Elmi, dei comportamenti e degli strumenti adeguati.

Formazione

Policy per la gestione e il controllo della formazione, addestramento e delle campagne di Security Awareness relativamente alle politiche organizzative applicate e alle procedure relative alla sicurezza delle informazioni.

Rispetto delle leggi e regolamenti obbligatori

Policy atte a garantire la conformità dell'SGI di Elmi alle leggi e ai regolamenti obbligatori.
La Elmi tutela la sicurezza delle informazioni nel pieno rispetto delle leggi e dei regolamenti, anche per quel che riguarda lo specifico riferimento alla protezione dei dati personali ex reg. UE 2016/679 e D.lgs 196/2003 e s.m.i. e al CCNL.
Elmi si impegna altresì a mantenere un inventario delle licenze software acquistate dall'azienda e a verificare periodicamente l'uso di software con diritti di licenza da parte dei propri dipendenti e collaboratori, contrastando la violazione di tali diritti.

Protezione

Policy atte a garantire che tutte le informazioni, beni e risorse di Elmi o affidate da Elmi da terzi parti, siano protette contro i rischi legati al rispetto della riservatezza, dell'integrità e della disponibilità in proporzione al loro valore e in conformità con le leggi vigenti.
Le registrazioni rilevanti sono protette da perdita, distruzione, falsificazione, accessi e divulgazione non autorizzati, in conformità con i requisiti legali, normativi, contrattuali e di business, attraverso appositi strumenti tecnici e procedure operative descritte nel Piano di Sicurezza Fisica, nel Piano di Sicurezza Logica e nella Procedura di controllo degli accessi.
I sistemi informatici che utilizzano canali di comunicazione pubblici (es.: rete Internet) sono configurati per eseguire la cifratura e la decifratura delle informazioni trasmesse. Per comunicazioni tra sistemi interni le chiavi crittografiche possono essere generate dai sistemi dedicati a tale operazione a cura dell'Area dei Sistemi Informativi Aziendali. Le chiavi crittografiche utilizzate su sistemi che comunicano con terze parti, sono generate e gestite da Certification Authority esterne. Entrambe le modalità garantiscono il medesimo livello di protezione, garantendo l'autenticità, la riservatezza e l'integrità delle informazioni trasmesse. Il processo di gestione del ciclo di vita delle chiavi crittografiche, a cura dell'Area dei Sistemi Informativi Aziendali, è descritto nel Piano di Sicurezza Logica.
L'uso di strumenti crittografici viene attuato nell'ambito del pieno rispetto della normativa vigente e in conformità con regolamenti ed accordi con terze parti.
I sistemi utilizzati per la gestione di informazioni aziendali sono dislocati in locali sicuri, ad accesso controllato. La protezione è garantita da apposite contromisure per prevenire la violazione della riservatezza e della integrità sia fisica che logica, descritte rispettivamente nel Piano di Sicurezza Fisica e nel Piano di Sicurezza Logica.
Elmi adotta una politica di separazione degli ambienti IT dedicati allo sviluppo, al test/collaudo e all'esercizio dei propri sistemi informativi, al fine di ridurre i rischi di accesso non autorizzato alle informazioni e di modifiche o di indisponibilità dei sistemi di esercizio.
È tutelata la sicurezza delle informazioni che vengono gestite al di fuori del sistema informativo aziendale, attraverso specifiche politiche di comportamento comunicate attraverso il Regolamento Aziendale.

Sicurezza nella progettazione e sviluppo di soluzioni Software

Elmi adotta un insieme di strumenti descritti nel Piano di Sicurezza Logica e nel Piano di Sicurezza Fisica, per garantire la sicurezza del processo di sviluppo, al fine di assicurare l'integrità, la disponibilità e la riservatezza dei deliverable realizzati nell'ambito di tale processo.

Relazioni con i fornitori

Elmi adotta la politica di responsabilizzare i propri fornitori e le terze parti con cui collabora per le proprie attività, mediante specifici accordi di non disclosure agreement.
Gli indicatori SLA e gli accordi NDA con i fornitori sono rivisti periodicamente e comunque a valle di ogni revisione della valutazione dei rischi.

Impegno al rispetto dei requisiti applicabili

L'impegno della direzione e di tutti coloro che a vario titolo sono coinvolti dalle attività del sistema di gestione è quello di rispettare tutti i requisiti previsti dalla Norma Internazionale ISO 27001:2017. Per questo, la direzione assume l'impegno di esercitare la leadership secondo quanto stabilito da tale Norma.

Impegno per il miglioramento continuo del sistema di gestione

Il patrimonio informativo del cliente e quello relativo al know-how della nostra organizzazione costituiranno d'ora innanzi i punti focali dell'impegno di tutti. Un impegno assunto da tutti e da ciascuno.
Tale impegno sarà manifestato attraverso le "performance di sicurezza" che dovranno dare evidenza di quanto la nostra organizzazione ed il nostro sistema di gestione della sicurezza delle informazioni siano efficaci nel registrare un miglioramento continuo.

7. RESPONSABILITÀ

Tutto il personale che, a qualsiasi titolo, collabora con l'azienda è responsabile dell'osservanza di questa policy e della segnalazione di anomalie, anche non formalmente codificate, di cui dovesse venire a conoscenza.
Tutti devono:

- proteggere la riservatezza, l'integrità e la disponibilità delle informazioni e delle risorse intellettuali di Elmi o affidate a Elmi da terze parti;
- proteggere i beni materiali, i sistemi informatici e le risorse di Elmi o affidati a Elmi da terze parti;
- proteggere ogni informazione, attività e risorsa sotto la propria responsabilità;
- contattare la Direzione, le autorità competenti e/o adeguate in caso di violazioni della sicurezza effettive o presunte;
- contattare la Direzione e il Responsabile della Sicurezza, in caso di qualsiasi modifica necessaria della politica di sicurezza, dei requisiti di sicurezza, degli standard, delle procedure.

La violazione dei principi e dei comportamenti a tutela della sicurezza delle informazioni saranno perseguite da Elmi in misura proporzionata alla gravità delle infrazioni commesse ed in linea con quanto stabilito dal CCNL CONFAPI, dal Reg. Ue 2016/679 GDPR e dal D.Lgs.196/03 (Codice in materia di protezione dei dati personali).

Il **responsabile della sicurezza delle informazioni** si occupa di:

- garantire e monitorare il rispetto delle politiche di sicurezza, requisiti, norme e procedure definite;
- garantire che il personale di Elmi sia formato e consapevole sulla Politica, sui requisiti, sugli standard e sulle procedure definite per garantire la sicurezza delle informazioni e delle risorse;
- tenere sotto controllo i documenti del SGSI, ivi inclusa la tipologia di classificazione dei documenti affinché l'organizzazione aziendale possa condurre, in modo sicuro, le proprie attività;
- adottare criteri e metodologie per l'analisi e la gestione del rischio;
- suggerire le misure di sicurezza organizzative, procedurali e tecnologiche a tutela della sicurezza e continuità delle attività di Elmi;
- controllare periodicamente l'esposizione dei servizi aziendali alle principali minacce;
- verificare gli incidenti di sicurezza e adottare le opportune contromisure;
- promuovere la cultura relativa alla sicurezza delle informazioni;
- interfacciarsi con la Società di consulenza per la certificazione;
- effettuare audit periodici sull'applicazione delle procedure;
- implementazione delle procedure ed aggiornamento;
- controllare i livelli della sicurezza delle informazioni nell'ambito dei processi produttivi;
- riscontrare le non conformità – reporting ed azioni – addestramento degli uomini – azioni sui prodotti e e le attrezzature;
- predisporre i programmi di audit interni e controllo dell'esecuzione delle verifiche ispettive interne;
- gestire dei rapporti con l'ente di certificazione.
- Effettuare periodici Assessment della sicurezza: valutare lo stato dell'arte della sicurezza in azienda e individuare un piano strategico per aumentare la capacità di reagire alle cyber minacce
- Contribuire insieme al Titolare del trattamento, referente privacy e al resp. della qualità, all'elaborazione di security policy
- Definire regole e standard per la gestione della sicurezza
- Definire architetture per la gestione della sicurezza e monitoraggio delle scelte strutturali;
- Aggiornarsi periodicamente con corsi e webinar sulle tipologie di minacce e di attacco;
- Monitorare la sicurezza: controllare il traffico di rete e il traffico sui diversi canali
- Rispondere in tempi brevi in caso di data breach per limitarne gli effetti, in base al ruolo definito nella procedura di gestione delle violazioni

- Condurre indagini forensi in caso di data breach, collaborando con risorse interne o specialisti esterni.

Comitato per la sicurezza delle informazioni: viene istituito un comitato per la sicurezza delle informazioni. Tale comitato è composto da:

- Responsabile security informatica
- Responsabile del sistema qualità
- Referente organizzativo privacy
- Amministratore di sistema
- Responsabile della Protezione dei dati

Il comitato ha il compito di fissare gli obiettivi, assicurare un indirizzamento chiaro e condiviso con le strategie aziendali e un supporto visibile alle iniziative di sicurezza. Promuove la sicurezza garantendo la congruità dei singoli budget destinati alla sicurezza, coerentemente con le politiche e le linee strategiche aziendali definite.

I **Responsabili di area** devono:

- essere in linea con la politica di sicurezza, i requisiti, gli standard e le procedure definite;
- identificare e definire i diritti di accesso delle risorse per le loro attività e responsabilità specifiche;
- richiedere alle terze parti di essere in linea con gli accordi di riservatezza (accordo di non divulgazione);
- definire un livello di rischio accettabile in seguito alla realizzazione di una valutazione dei rischi;
- vigilare sull'adempimento di quanto previsto dalla Politica per la sicurezza da parte dei propri dipendenti
- verificare il rispetto delle normativa (in particolare relativa alla protezione dei dati) nelle attività della propria area e nel trattamento delle informazioni;
- rendere consapevoli le risorse umane che lo collaborano circa le conseguenze in caso di mancato rispetto della politica di qualità e sicurezza.

Tutti i soggetti esterni che intrattengono rapporti con Elmi devono garantire il rispetto dei requisiti di sicurezza esplicitati dalla presente politica di sicurezza anche attraverso la sottoscrizione di un "patto di riservatezza" all'atto del conferimento dell'incarico, allorquando questo tipo di vincolo non sia espressamente citato nel contratto.
Le responsabilità di cui al presente capitolo sono generali e riguardano l'intera organizzazione di Elmi.

8. RIESAME

Elmi verificherà periodicamente l'efficacia e l'efficienza del SGI, garantendo l'adeguato supporto per l'adozione delle necessarie migliorie al fine di consentire l'attivazione di un processo di miglioramento continuo, che terrà sotto controllo il variare delle condizioni aziendali/ambientali o degli obiettivi di business aziendali, al fine di garantire il suo corretto adeguamento.

Qualsiasi modifica all'organizzazione o ai processi aziendali, alle strutture e ai sistemi di elaborazione delle informazioni che hanno effetto sulla sicurezza delle informazioni, deve essere valutata e autorizzata dalla Direzione Aziendale.

L'approccio di Elmi nella gestione della sicurezza delle informazioni e della sua implementazione (obiettivi dei controlli, controlli, politiche, processi e procedure per la sicurezza delle informazioni) viene rivista annualmente nell'ambito dei processi di riesame della Direzione, o in modo indipendente dalla periodicità annuale, quando intervengono cambiamenti significativi.

Palermo, 18/01/2023

Approvato dalla Direzione
L'amministratore unico
Dott Rosario Minasola