# POLITICA DELLA SICUREZZA DELLE INFORMAZIONI

La **Elios Engineering Srl** mira a garantire un adeguato livello di sicurezza dei dati e delle informazioni nell'ambito delle attività aziendali connesse alla formazione ed ai servizi di consulenza attraverso l'identificazione, la valutazione ed il trattamento dei rischi ai quali i servizi stessi sono soggetti.

Il Sistema di Gestione per la Sicurezza delle Informazioni di Elios Engineering S.r.l. definisce un insieme di misure organizzative, tecniche e procedurali a garanzia del soddisfacimento dei sotto elencati requisiti di sicurezza di base:

- **Riservatezza:** assicurare che le informazioni siano trattate esclusivamente da coloro che dispongono delle autorizzazioni a farlo;
- **Integrità:** le informazioni devono essere protette da alterazioni involontarie e devono poter essere modificate solo ed esclusivamente da persone autorizzate a farlo;
- **Disponibilità:** l'informazione deve essere accessibile e utilizzabile quando richiesto dai processi e dagli utenti che dispongono dei relativi privilegi;
- **Autenticità:** deve essere garantita la provenienza affidabile delle informazioni;
- **Privacy:** deve essere garantita la protezione ed il controllo dei dati personali;

Con la presente politica Elios intende formalizzare i seguenti obiettivi nell'ambito della sicurezza delle informazioni:

- Preservare al meglio l'immagine dell'azienda quale fornitore affidabile, competente nella gestione delle informazioni affidatele dai clienti
- Assicurare la conoscenza complessiva delle informazioni gestite o elaborate nello svolgimento delle proprie attività professionali e valutazione della loro criticità in modo da poter implementare livelli adeguati di protezione
- Proteggere il patrimonio informativo dei propri clienti anche nello svolgimento delle attività di consulenza, assicurando il rispetto delle specifiche contrattuali e legislative e la tutela delle informazioni connesse alle vulnerabilità, onde evitare di poter rappresentare Elios stessa una vulnerabilità per i clienti che le si affidano;
- Garantire che le parti interessate abbiano la piena consapevolezza delle problematiche relative alla sicurezza delle informazioni e collaborino al rispetto della politica relativa adottando le procedure relative al rispetto dei livelli di sicurezza
- Assicurare che il personale risponda con tempestività e consapevolezza agli incidenti di sicurezza potenziali riconoscendone la natura, prevenendone l'accadimento, informando e reagendo con tempestività in modo da minimizzarne gli impatti
- Garantire che gli accessi alle strutture e agli asset siano impediti alle persone esterne o non autorizzate
- Garantire la conformità della gestione delle informazioni e del trattamento dei dati personali alla normativa vigente e cogente;
- Assicurare la rilevazione delle anomalie e il trattamento delle vulnerabilità dei sistemi e delle procedure, assicurando la disponibilità e l'integrità delle informazioni.
- Garantire il recupero delle informazioni a seguito di eventi avversi e la continuità dei servizi adottando strumenti, tecnologie, competenze e procedure adeguate

## Accettazione Applicabilità

La presente politica si applica indistintamente a tutti i dipendenti, collaboratori, fornitori, partner e tutte le altre terze parti coinvolte nelle attività istituzionali. Tutti devono accettare i loro obblighi e le responsabilità individuali, al fine di proteggere le informazioni, i beni e le risorse. L'attuazione della presente politica 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.

## Accesso

Gli accessi alle informazioni, beni e risorse della Elios Engineering, devono essere controllati e monitorati sulla base dei seguenti criteri:

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

Elios consente la comunicazione e la diffusione delle informazioni verso l'esterno solo per il corretto svolgimento delle attività aziendali che devono avvenire nel rispetto delle regole e delle norme cogenti

## Valutazione

Elios Engineering definisce il giusto rapporto tra:

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

## Consapevolezza

La Direzione aziendale assicura che ogni dipendente, collaboratore, fornitore o terza parte sia consapevole della Politica per la Sicurezza delle Informazioni e che i suoi comportamenti e gli strumenti utilizzati siano adeguati e in linea con la politica di sicurezza.

## Formazione

La Direzione aziendale garantisce che ogni risorsa sia addestrata sulle politiche organizzative applicate e le procedure relative alla sicurezza delle informazioni.

## Rispetto delle Leggi e Regolamenti Obbligatori

Tutti i trattamenti delle informazioni e le procedure per la sicurezza di Elios Engineering sono conformi alle leggi e ai regolamenti obbligatori. Elios tutela la sicurezza delle informazioni nel pieno rispetto delle leggi e dei regolamenti, considerando appieno il D. Lgs. 196/2003 così come modificato dal D. Lgs. 101/2018, dal Regolamento europeo (UE) 2016/679 del Parlamento europeo e del Consiglio del 27/04/2016 (GDPR) e dal CCNL. Elios si impegna altresì a mantenere un idoneo controllo 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

Tutte le informazioni, beni e risorse sono 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. 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. 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. Elios non effettua attività di sviluppo sw, per tanto, non è soggetta ad una separazione fisica o logica degli ambienti connessi allo sviluppo, test ed operatività.

## Relazioni con i Fornitori

Elios Engineering adotta la politica di responsabilizzare i propri fornitori rispetto a tale politica. Gli indicatori SLA e gli accordi con i fornitori sono rivisti periodicamente e comunque a valle di ogni revisione della valutazione dei rischi.

## Contenuto della Politica

Il SGSI si applica a tutte le attività connesse alla formazione ed ai servizi di consulenza erogati da Elios, sia connessi alla sicurezza sul lavoro che alla consulenza Direzionale o sistemica. Tutte le informazioni, che vengono acquisite o elaborate 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.

In conformità alla norma ISO/IEC 27001 periodicamente viene svolta 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. Elios fa una valutazione del rischio, viene valutata la soglia di rischio accettabile, il trattamento di mitigazione dei rischi oltre tale soglia e il rischio residuo in seguito al trattamento.

Tale analisi sarà ponderata anche rispetto al valore di business dei singoli beni da proteggere e dovrà identificare chiaramente le azioni da intraprendere che saranno classificate secondo una scala di priorità che rispetti gli obiettivi aziendali, il budget a disposizione e la necessità di mantenere la conformità alle norme e leggi vigenti.

Detta analisi dovrà essere effettuata anche a fronte di eventi che possano modificare il profilo di rischio complessivo del sistema.

## 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.

La Direzione promuove la sicurezza garantendo la congruità dei singoli budget destinati alla sicurezza, definisce le politiche e le linee strategiche da adottare.

Il Sistema di Gestione della Sicurezza delle Informazioni in particolare prevede di:

- emanare tutte le norme necessarie 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;

- pianificare un percorso formativo, specifico e periodico in materia di sicurezza per il personale;
- 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.

Tutti i soggetti esterni che intrattengono rapporti con Elios devono garantire il rispetto dei requisiti di sicurezza esplicitati dalla presente politica di sicurezza.

Tutti devono:

- proteggere la riservatezza, l'integrità e la disponibilità delle informazioni e delle risorse intellettuali di Elios o affidate a Elios da terze parti;
- proteggere i beni materiali, i sistemi informatici e le risorse di Elios o affidate a Elios 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.

I Responsabili 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;
- 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 delle informazioni da parte dei propri dipendenti.

Il Responsabile del SGSI deve:

- garantire e monitorare il rispetto delle politiche di sicurezza, requisiti, norme e procedure definite
- garantire che il personale sia formato e consapevole sulla Politica, sui requisiti, sugli standard e sulle procedure definite per garantire la sicurezza delle informazioni e delle risorse;

Il Responsabile della Sicurezza IT deve:

- implementare la gestione della sicurezza sulla base delle politiche di sicurezza emesse;
- rivedere le informazioni e le risorse fisiche sotto la sua responsabilità, al fine di definire il livello di controllo adeguato da attuare perché il controllo di sicurezza sia proporzionato al valore delle informazioni e delle risorse da proteggere e nel rispetto delle leggi e dei regolamenti obbligatori;
- definire i requisiti di sicurezza di cui è necessario tenere conto nella definizione del budget per il mantenimento e lo sviluppo dei sistemi informativi aziendali;
- controllare con regolarità lo stato dei sistemi informativi aziendali, per garantire la conformità con gli standard e le politiche di sicurezza.

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. La diffusione della conoscenza e l'applicazione di tali norme sono assicurate dall'impegno costante della Direzione.

Rev. 2 Scafati, 25.11.2022

Il Responsabile del Sistema (per redazione)

L'Amministratore Unico (per approvazione)