Le società eFM considerano i dati e le informazioni un bene fondamentale e prezioso, sia nel caso che siano di proprietà aziendale sia che appartengano a soggetti terzi, per cui viene posta la massima attenzione ed impegno nel garantire il paradigma di Riservatezza, Integrità e Disponibilità (RID) delle informazioni trattate.

Al fine di garantire la protezione del patrimonio informativo coerentemente con le scelte strategiche di eFM, risulta quindi fondamentale identificare in modo chiaro gli obiettivi e i principi di sicurezza in accordo con la propensione al rischio definita a livello aziendale.

Obiettivi del Sistema di Gestione

La presente Politica Generale di eFM del Sistema di Gestione per la Sicurezza delle Informazioni (SGSI) descrive gli obiettivi e i principi generali che eFM adotta e applica nel trattamento delle informazioni al fine di supportare i requisiti della propria offerta di servizi garantendo il rispetto di prescrizioni legali o regolamentari e l'allineamento alle strategie delineate in materia di gestione dei rischi.

Gli obiettivi definiti in questa Politica Generale sono qui delineati in termini generali e vengono tradotti in termini concreti in relazione a specifiche aree tematiche mediante obiettivi operativi nell'ambito del Sistema di Gestione per la Sicurezza delle Informazioni adottato.

L'impegno di eFM contenuto nella presente Politica Generale può identificarsi nei seguenti punti, fondamentali:

- Considerare la sicurezza delle informazioni elemento fondamentale nell'erogazione dei propri specifici servizi di business.
- Salvaguardare il patrimonio nei suoi aspetti finanziari, fisici, di proprietà intellettuale e di reputazione e garantire la riservatezza e la correttezza delle informazioni trattate anche in relazione all'evoluzione delle minacce cyber.
- Garantire la continuità del servizio per rispettare i vincoli derivanti da normative vigenti e da obblighi contrattuali oltre che per assicurarne l'affidabilità nei confronti della clientela.
- Ottemperare alle leggi e alle disposizioni regolamentari in materia di sicurezza delle informazioni che disciplinano l'attività svolta e indicare a dipendenti e collaboratori esterni i principi da seguire.

Applicazione della Politica

La presente Politica si applica a tutti i processi e a tutte le risorse, umane e infrastrutturali, anche esterne, coinvolte nella gestione delle informazioni trattate da eFM, per quanto di competenza di ciascuna di esse.

In particolare, i destinatari del documento sono:

- Gli organi di amministrazione delle società di eFM, che approvano la Politica e assicurano un adeguato impegno e le risorse necessarie, manageriali ed economiche, per consentire l'effettiva attuazione dei principi definiti.

- I dipendenti di eFM, che hanno il compito di attuare quanto definito nella presente Politica, ciascuno per gli ambiti di propria competenza.
- Tutte le terze parti che, nell'ambito di rapporti con eFM, hanno la possibilità di accedere al patrimonio informativo aziendale.

Questa Politica è disponibile a tutto il personale eFM tramite la Intranet aziendale alla quale il personale può accedere con il solo requisito di avere un account Active Directory.

Al fine di garantire l'integrità, la riservatezza e la disponibilità sia del patrimonio informativo interno che di quello affidatogli più in generale da tutte le parti interessate, la Direzione di eFM ha deciso di implementare un Sistema di Gestione per la Sicurezza delle Informazioni conforme ai requisiti della ISO/IEC 27001:2022 e di stabilire, attuare e mantenere una Politica per la sicurezza delle informazioni che abbia i seguenti principi di riferimento:

- **Attenzione focalizzata sul Cliente e sulle parti interessate:**

  eFM si impegna a comprendere le necessità dei clienti e pianifica le proprie attività per soddisfarle appieno. Allo stesso modo opera nel rispetto delle richieste e dei requisiti del mercato di riferimento, del paese in cui opera, adempiendo a leggi e regolamenti di tutte le parti coinvolte nei processi ritenuti critici.

- **Attenzione alla protezione dei dati personali gestiti in cloud**

  eFM si impegna al pieno rispetto della normativa europea e nazionale applicabile alla protezione dei dati ed in particolare si impegna nel valutare i rischi collegati ai dati gestiti nel cloud attraverso i servizi tramite esso erogati. A tal fine, adotta tutti gli strumenti tecnologici ed organizzativi a garanzia che tutti i rischi individuati siano mitigati tramite adeguate contromisure.

- **Approccio per processi**

  eFM identifica le diverse attività della propria organizzazione come processi da pianificare, controllare e migliorare costantemente e attiva al meglio le risorse per la loro realizzazione. eFM gestisce i propri processi perché siano univoci gli obiettivi da perseguire e i risultati attesi, le responsabilità connesse e le risorse impiegate.

- **Leadership**

  eFM si assume la responsabilità dell'efficacia del proprio SGSI, rendendo disponibili tutte le risorse necessarie e assicurandosi che gli obiettivi pianificati siano compatibili con il contesto e gli indirizzi strategici. La Direzione di eFM comunica l'importanza del SGSI e coinvolge attivamente tutte le parti interessate, coordinandole e sostenendole.

- **Valutazione dei rischi e delle opportunità**

  eFM pianifica i propri processi con un approccio risk-based thinking (RBT) al fine di attuare le azioni più idonee per valutare e trattare rischi associati ai processi e per sfruttare e rinforzare le opportunità identificate. eFM promuove a tutti i livelli un adeguato senso di proattività nella gestione dei rischi e delle opportunità.

- **Coinvolgimento del personale e degli stakeholder**

eFM è consapevole che il coinvolgimento del personale e di tutti gli stakeholder, unito all'attiva partecipazione di tutti i collaboratori, sono un elemento strategico primario. Per questo motivo la Direzione promuove lo sviluppo delle professionalità interne e l'attenta selezione delle collaborazioni esterne al fine di dotarsi di risorse umane competenti e motivate.

- **Miglioramento**

  eFM si pone come obiettivo permanente il miglioramento delle prestazioni del proprio SGSI. Per rendere tangibile quanto indicato, la Direzione, oltre a rendere disponibili le risorse necessarie, stabilisce obiettivi misurabili i quali, analizzati periodicamente, consentono di valutare nel medio periodo i miglioramenti e/o i benefici derivanti dall'applicazione del proprio SGSI.

- **Sicurezza delle Informazioni**

  L'obiettivo del sistema di gestione della sicurezza delle informazioni di eFM è di garantire un adeguato livello di sicurezza dei dati e delle informazioni nell'ambito dello sviluppo ed erogazione dei servizi aziendali tramite l'identificazione, la valutazione ed il trattamento dei rischi ai quali i servizi stessi sono soggetti.

Il Sistema di Gestione della Sicurezza delle Informazioni di eFM definisce un insieme di misure organizzative, tecniche procedurali a garanzia del soddisfacimento dei sottoelencati requisiti di sicurezza di base che sono di seguite definite:

- **Riservatezza**: ovvero la proprietà dell'informazione di essere nota solo a chi ne ha i privilegi;
- **Integrità**: ovvero la proprietà dell'informazione di essere modificata solo ed esclusivamente da chi ne possiede i privilegi;
- **Disponibilità**: ovvero la proprietà dell'informazione di essere accessibile e utilizzabile quando richiesto dai processi e dagli utenti che ne godono i privilegi.

Tutto il personale che a qualsiasi titolo collabora con eFM è responsabile dell'osservanza della presente Politica (Policy) e a partecipare alla segnalazione delle anomalie, anche formalmente non codificate, di cui dovesse venire a conoscenza.

Tutti i soggetti esterni che intrattengono rapporti con eFM devono garantire il rispetto dei requisiti della sicurezza esplicitati dalla presente Politica di Sicurezza anche tramite la sottoscrizione di un "patto di riservatezza" all'atto del conferimento dell'incarico allorquando questo tipo di vincolo non è espressamente previsto nel contratto stesso.

La presente Politica si applica alle funzioni coinvolte nel Campo di Applicazione del SGSI. L'attuazione della presente Politica è obbligatoria per le risorse eFM coinvolte nel Campo di Applicazione 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. eFM consente la comunicazione e diffusione delle informazioni verso l'esterno solo per il corretto svolgimento delle attività aziendali che avvengono sempre nel rispetto delle regole nonché delle norme e leggi cogenti.

Riassumendo, **per tutti i sistemi sotto SGSI, è necessario assicurare che**:

- le informazioni siano accessibili esclusivamente alle persone autorizzate, sia interne che esterne all'azienda, garantendo livelli di servizio e complessità compatibili con i requisiti funzionali dei sistemi interessati;
- qualunque sia il formato delle informazioni trattate, sia garantita la loro disponibilità, integrità e riservatezza nel rispetto dei requisiti legislativi applicabili;
- sia effettuato un monitoraggio costante nel cambiamento degli asset e della tecnologia al fine di identificare tempestivamente nuove vulnerabilità;
- sia effettuato un costante aggiornamento sui siti specializzati in tematiche di sicurezza e forum per la pronta individuazione di nuove tipologie di minacce;
- sia prestata particolare attenzione alle variazioni dei requisiti normativi, quelli contrattuali ed alle relative priorità in relazione a nuovi sviluppi che si potranno erogare;
- sia garantita la continuità operativa attraverso interventi mirati, sia organizzativi che tecnologici, e che tali interventi siano definiti, costantemente aggiornati e verificati;
- tutto il personale sia addestrato sulla sicurezza, che sia informato dell'obbligatorietà delle politiche aziendali in merito e che sia altresì sensibilizzato sulle conseguenze derivanti dalla violazione delle politiche aziendali;
- siano effettuate valutazioni periodiche dell'efficacia del SGSI e della formazione del personale attraverso simulazioni nell'ambito di applicazione (vulnerability assessment, test di conoscenza delle policy e simulazioni di violazioni delle stesse);
- siano introdotte metriche per la valutazione delle prestazioni del sistema;
- siano separate le mansioni relative alle attività critiche (es. sviluppo e collaudo con produzione);
- siano ridotti il più possibile i rischi alla fonte;
- qualsiasi violazione della sicurezza, reale o presunta, sia comunicata ed investigata;
- siano prontamente identificati e gestiti gli incidenti sulla sicurezza ed attivate le autorità competenti per quelli che hanno impatto su requisiti di legge violati;
- sia evitato l'utilizzo di software non autorizzati;
- siano effettuati riesami periodici del SGSI relativamente a:
  - verifica dell'attualità e dell'efficacia dei controlli applicati per le minacce e le vulnerabilità individuate nel piano del trattamento dei rischi;
  - incidenza dei controlli attuati sull'efficacia gestionale;
  - modifiche apportate dalla tecnologica (vulnerabilità nuove o modificate, riduzione dei rischi per nuove conoscenze acquisite in base al progresso tecnologico);
  - modifiche apportate alla configurazione dei sistemi e degli applicativi sotto SGSI;
  - rivalutazione periodica del rischio.
  - corretta gestione dei dati personali secondo GDPR.

Roma, 01 gennaio 2025

L'Amministratore Delegato
Daniele Di Fausto