# Politica per la Sicurezza delle Informazioni

| MODIFICHE | | | |
|---|---|---|---|
| **EDIZIONE** | **DATA** | **NATURA** | **DESCRIZIONE REVISIONE** |
| 00 | 15.05.23 | Prima edizione | - |
| 01 | 19.03.26 | Prima revisione | Aggiunti riferimenti specifici a gestione delle utenze privilegiate ed ai processi di logging e di patching |
| | | | |
| | | | |

# Sommario

## 1 Scopo

La presente Politica per la Sicurezza delle Informazioni definisce i principi, gli obiettivi e le responsabilità necessari a garantire la tutela e la protezione del patrimonio informativo aziendale da tutte le minacce, interne ed esterne, intenzionali o accidentali.

La politica è redatta in conformità ai requisiti della norma **ISO/IEC 27001:2022**.

La direzione di KFI ha definito, ha divulgato e si impegna a mantenere attiva a tutti i livelli della propria organizzazione la presente politica per la gestione della Sicurezza delle Informazioni.

## 2 Campo di applicazione

La politica si applica indistintamente a:

- tutti i processi aziendali e alle sedi operative;
- tutti gli organi e livelli dell'Azienda;
- tutto il personale, indipendentemente dal ruolo o dalla tipologia contrattuale;
- fornitori, partner e soggetti esterni che trattano informazioni rientranti nel perimetro del SGSI.

L'attuazione della presente politica è obbligatoria e deve essere inserita nella regolamentazione degli accordi con terze parti e qualsiasi soggetto esterno che, a qualsiasi titolo, possa essere coinvolto con il trattamento di informazioni che rientrano nel campo di applicazione del Sistema di Gestione (SGSI).

L'azienda 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.

## 3 Obiettivi della sicurezza delle informazioni

Il patrimonio informativo da tutelare è costituito dall'insieme delle informazioni gestite attraverso i servizi forniti e localizzate in tutte le sedi dell'azienda.

L'azienda si impegna a garantire un livello di sicurezza adeguato perseguendo i seguenti obiettivi relativi alle informazioni gestite:

- **Confidenzialità**: accesso alle informazioni consentito solo a soggetti autorizzati.
- **Integrità**: protezione dell'accuratezza e completezza delle informazioni e dei processi utilizzati per la loro elaborazione.
- **Disponibilità**: accesso alle informazioni e ai servizi garantito agli utenti autorizzati nel momento in cui lo richiedono e secondo le tempistiche necessarie.
- **Conformità**: rispetto delle normative vigenti, degli obblighi contrattuali e delle policy interne.
- **Resilienza**: capacità di prevenire, rilevare, rispondere e ripristinare i servizi in caso di incidenti.
- **Riduzione del rischio**: identificazione, valutazione e trattamento dei rischi tramite metodologie strutturate.
- **Consapevolezza**: diffusione continua della cultura della sicurezza a tutti i livelli aziendali.

## 4 Principi generali

La mancanza di adeguati livelli di sicurezza può comportare il danneggiamento dell'immagine aziendale, la mancata soddisfazione del cliente, il rischio di incorrere in sanzioni legate alla violazione delle normative vigenti nonché danni di natura economica e finanziaria. Un adeguato livello di sicurezza è altresì basilare per la condivisione delle informazioni.

L'azienda identifica tutte le esigenze di sicurezza tramite l'analisi dei rischi, che consente di acquisire consapevolezza sul livello di esposizione a minacce del proprio sistema informativo. La valutazione del rischio permette di valutare le potenziali conseguenze e i danni che possono derivare dalla mancata applicazione di misure di sicurezza al sistema informativo e quale sia la realistica probabilità di attuazione delle minacce identificate: i risultati di questa valutazione determinano le azioni necessarie per gestire i rischi individuati e le misure di sicurezza più idonee.

L'azienda adotta dunque un approccio sistemico alla gestione della sicurezza delle informazioni basato sui seguenti principi:

- mantenimento di un catalogo costantemente aggiornato degli asset aziendali rilevanti ai fini della gestione delle informazioni con indicazione dei relativi responsabili;
- classificazione delle informazioni in base al loro livello di criticità, in modo da essere gestite con livelli di riservatezza ed integrità coerenti ed appropriati;
- accesso ai sistemi basato su procedure di identificazione, autenticazione ed autorizzazione: le autorizzazioni di accesso alle informazioni devono essere differenziate in base al ruolo ed agli incarichi ricoperti dai singoli individui, in modo che ogni utente possa accedere alle sole informazioni di cui necessita, e devono essere periodicamente sottoposte a revisione;
- definizione di procedure per l'utilizzo sicuro dei beni aziendali e delle informazioni e dei loro sistemi di gestione;
- deve essere incoraggiata la piena consapevolezza delle problematiche relative alla sicurezza delle informazioni in tutto il personale (dipendenti e collaboratori), a partire dal momento della selezione e per tutta la durata del rapporto di lavoro;
- obbligo di segnalazione di qualsiasi problema relativo alla sicurezza degli incidenti e gestione dei relativi incidenti secondo quanto indicato nelle procedure formalizzate;
- protezione fisica delle sedi e delle apparecchiature, prevenendo l'accesso non autorizzato a sedi e singoli locali aziendali dove sono gestite le informazioni;
- integrazione dei requisiti di sicurezza nel ciclo di vita dei sistemi, considerando tutte le fasi di progettazione, sviluppo, esercizio, manutenzione, assistenza e dismissione dei sistemi e dei servizi informatici;
- conformità con i requisiti legali e con i principi legati alla sicurezza delle informazioni nei contratti con le terze parti;
- predisposizione di un piano di continuità operativa, che permetta all'azienda di affrontare efficacemente un evento imprevisto, garantendo il ripristino dei servizi critici in tempi e con modalità che limitino le conseguenze negative sulla missione aziendale;
- devono essere garantiti il rispetto delle disposizioni di legge, di statuti, regolamenti o obblighi contrattuali e di ogni requisito inerente la sicurezza delle informazioni, riducendo al minimo il rischio di sanzioni legali o amministrative, di perdite rilevanti o danni alla reputazione.

# 5 Gestione del rischio

L'azienda conduce periodicamente un'analisi dei rischi per:

- identificare minacce e vulnerabilità dei sistemi e dell'organizzazione;
- stimare probabilità e impatti di accadimenti negativi legati alla concretizzazione delle minacce suddette;
- definire misure di trattamento del rischio adeguate;
- monitorare l'evoluzione del rischio nel tempo.

I risultati dell'analisi determinano le azioni necessarie per la mitigazione dei rischi individuati.

# 6 Gestione delle utenze e degli accessi

## 6.1 Principi generali

- Ogni utente deve essere identificato univocamente.
- Le autorizzazioni sono assegnate secondo il principio del privilegio minimo (" least privilege"), ovvero ogni utente deve avere solo i permessi minimi indispensabili per svolgere le proprie attività.
- Le autorizzazioni sono riesaminate periodicamente.
- Gli account devono essere disattivati tempestivamente in caso di cessazione del rapporto.

## 6.2 Gestione delle utenze privilegiate

Le utenze con privilegi elevati (es. relative agli amministratori dei sistemi informatici, cd. "Amministratori di Sistema" o "AdS") sono soggette a controlli specifici:

- rilascio previa autorizzazione formale;
- utilizzo esclusivo per attività amministrative;
- tracciamento completo delle attività;
- separazione tra account personali e amministrativi;
- revisione periodica delle autorizzazioni;
- autenticazione forte ("Multi-Factor Authentication", o "MFA") obbligatoria.

# 7 Logging, monitoraggio e gestione degli incidenti

## 7.1 Logging e monitoraggio

L'azienda garantisce la registrazione e il monitoraggio degli eventi rilevanti:

- registrazione degli accessi e delle attività critiche;
- protezione dei log da alterazioni e accessi non autorizzati;
- conservazione dei log per periodi definiti;
- revisione periodica dei log per individuare anomalie.

### 7.2 Gestione degli incidenti

In relazione ad eventi o incidenti legate alla sicurezza delle informazioni l'azienda stabilisce che:

- tutto il personale deve segnalare tempestivamente i suddetti incidenti o anomalie;
- i suddetti incidenti sono gestiti secondo procedure formalizzate;
- ogni incidente è analizzato per identificarne cause, impatti ed azioni correttive.

## 8 Gestione delle patch e delle vulnerabilità

L'azienda mantiene aggiornati sistemi, applicazioni e dispositivi tramite un processo strutturato di "patch management" che garantisce:

- Il monitoraggio delle vulnerabilità note;
- la valutazione del rischio associato;
- l'applicazione tempestiva delle "patch" secondo opportune priorità;
- il test delle "patch" critiche prima della loro distribuzione sui sistemi;
- la documentazione delle attività di aggiornamento;
- la verifica periodica dell'efficacia del processo.

## 9 Gestione dei backup

KFI garantisce la protezione e la disponibilità dei dati attraverso un sistema strutturato di backup, progettato per prevenire perdite accidentali, guasti tecnici o eventi di sicurezza ed avente e seguenti caratteristiche:

- i backup sono eseguiti con frequenza adeguata alla criticità delle informazioni e dei servizi;
- sono conservati in modo sicuro e periodicamente verificati per assicurarne l'integrità e la possibilità di ripristino;
- le modalità operative, il periodo di mantenimento degli stessi ("retention") e le responsabilità sono definite in appositi standard tecnici e procedure dedicate.

## 10 Gestione delle modifiche (Change Management)

Le modifiche ai sistemi informativi, alle infrastrutture e ai servizi digitali dell'azienda sono gestite tramite:

- un processo controllato che garantisce valutazione preventiva dei rischi, approvazione formale, tracciabilità e verifica post-implementazione;
- ogni modifica deve essere pianificata, documentata e testata per ridurre l'impatto su sicurezza, continuità operativa e qualità del servizio;
- le procedure operative definiscono le categorie di modifica, i flussi autorizzativi e i criteri di emergenza per l'installazione delle relative modifiche ("emergency change").

## 11 Sicurezza fisica

Tramite specifiche misure tecniche e organizzative l'azienda assicura:

- la prevenzione dell'accesso non autorizzato alle sedi e ai locali sensibili;
- la protezione delle apparecchiature e dei supporti informativi;
- il controllo degli accessi fisici di dipendenti e collaboratori (es. utilizzo di badge).

## 12 Rapporti con terze parti

In relazione ai rapporti con terze parti (es. fornitori, partner):

- i requisiti di sicurezza devono essere inclusi nei contratti con fornitori e partner;
- le terze parti devono rispettare la presente politica e le procedure correlate;
- devono essere valutati i rischi derivanti da fornitori e servizi esterni.

## 13 Continuità operativa

Per garantire la continuità operativa anche in presenza di eventi imprevisti e permettere un rapido ripristino dei servizi critici:

- l'azienda mantiene un piano di continuità operativa e disaster recovery;
- Il piano garantisce il ripristino dei servizi critici entro tempistiche accettabili in relazione all'impatto che un'interruzione avrebbe sul business, cioè rispetto a quanto l'azienda può tollerare prima che si verifichino danni operativi, economici, normativi o reputazionali;
- il piano è testato e aggiornato periodicamente.

## 14 Formazione e consapevolezza

Per incoraggiare la piena consapevolezza delle problematiche relative alla sicurezza delle informazioni:

- tutto il personale riceve formazione iniziale e periodica sulla sicurezza;
- la consapevolezza è promossa tramite campagne ed iniziative dedicate.

## 15 Ruoli e responsabilità

L'osservanza e l'attuazione della presente politica sono responsabilità di diversi soggetti.

### 15.1 Personale dell'azienda

Tutto il personale che, a qualsiasi titolo, collabora con l'azienda ed è in qualche modo coinvolto con il trattamento di dati ed informazioni che rientrano nel campo di applicazione del Sistema di Gestione, deve:

- rispettare la politica e le procedure;
- proteggere le informazioni trattate;
- segnalare anomalie e violazioni di cui dovesse venire a conoscenza.

### 15.2 Terze parti

Tutti i soggetti esterni che intrattengono rapporti e collaborano con l'azienda devono:

- garantire il rispetto dei requisiti contenuti nella presente politica;

- trattare le informazioni secondo le regole aziendali.

### 15.3 Responsabile del Sistema di Gestione

Nell'ambito del Sistema di Gestione e attraverso norme e procedure appropriate, Il Responsabile del Sistema di Gestione deve:

- condurre l'analisi dei rischi con le opportune metodologie e adottare tutte le misure per la gestione del rischio;
- definire norme e procedure necessarie alla conduzione sicura di tutte le attività aziendali;
- verificare le violazioni alla sicurezza e adottare le contromisure necessarie e controllare l'esposizione dell'azienda alle principali minacce e rischi;
- organizzare la formazione e promuovere la consapevolezza del personale per tutto ciò che concerne la sicurezza delle informazioni;
- verificare periodicamente l'efficacia e l'efficienza del Sistema di Gestione.

## 16 Riesame e miglioramento continuo

La Direzione verificherà periodicamente e regolarmente, o in concomitanza di cambiamenti significativi, l'efficacia e l'efficienza del Sistema di Gestione, in modo da assicurare un supporto adeguato all'introduzione di tutte le migliorie necessarie e in modo da favorire l'attivazione di un processo continuo, con cui viene mantenuto il controllo e l'adeguamento della presente politica in risposta ai cambiamenti dell'ambiente aziendale, del business e delle condizioni legali.

Il Responsabile del Sistema di Gestione ha la responsabilità del riesame della politica.

## 17 Sanzioni

Chiunque, dipendenti, consulenti e/o collaboratori esterni dell'Azienda, disattenda le regole di sicurezza stabilite, in modo intenzionale o riconducibile a negligenza, e in tal modo provochi un danno all'azienda, potrà essere perseguito nelle opportune sedi e nel pieno rispetto dei vincoli di legge e contrattuali.