

ALLEGATO 1 AL MANUALE ISO 27001

FORTNES

CREDIT MANAGEMENT

POLITICA DELLA SICUREZZA DELLE INFORMAZIONI

APPROVATO DA		
Roberto ROMANO		
Francesco CIRILLO		
Marco FERRARA MINOLFI		

FORTNES S.P.A.

PIAZZA UMBERTO I, 1 - 84121 - SALERNO

TEL +39 089 273683 - +39 089 2576093

FAX +39 089 2022201

INDICE

1	MOTIVAZIONI	Pag. 3
2	SCOPO	Pag. 3
3	DESCRIZIONE	Pag. 3
4	AMBITO DI APPLICAZIONE	Pag. 4
5	POLITICA PER LA SICUREZZA DELLE INFORMAZIONI	Pag. 4
6	RESPONSABILITÀ DELLA POLITICA DI SICUREZZA DELLE INFORMAZIONI	Pag. 5

1. MOTIVAZIONI

FORTNES S.p.a. è un'Agenzia di Recupero del Credito per conto terzi. Fornisce altresì ai propri clienti servizi di *back office* amministrativo nonché consulenza ed assistenza per operazioni di cessione di crediti.

Data la natura delle proprie attività, FORTNES S.p.a. 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.

Nell'ambito delle attività svolte e della sicurezza delle informazioni FORTNES S.p.a. attribuisce, inoltre, fondamentale importanza alla motivazione e fidelizzazione del personale ed alla sua professionalità.

2. SCOPO

Scopo del presente documento è quello di descrivere i principi generali e la Politica di sicurezza delle informazioni definiti da FORTNES S.p.a. al fine di sviluppare un efficiente e sicuro *Sistema di Gestione della Sicurezza delle Informazioni*.

3. DESCRIZIONE

Per FORTNES S.p.a. la Sicurezza delle Informazioni ha come obiettivo primario la protezione dei dati e delle informazioni, della struttura tecnologica, fisica, logica ed organizzativa, responsabile della loro gestione. Questo significa ottenere e mantenere un sistema di gestione sicura delle informazioni, nell'ambito del campo di applicazione definito per l'ISMS (*Information Security Management System*), attraverso il rispetto dei seguenti principi:

1. **Riservatezza:** assicurare che l'informazione sia accessibile solamente ai soggetti e/o ai processi debitamente autorizzati;
2. **Integrità:** salvaguardare la consistenza dell'informazione da modifiche non autorizzate;
3. **Disponibilità:** assicurare che gli utenti autorizzati abbiano accesso alle informazioni e agli elementi architetturali associati quando ne fanno richiesta;
4. **Controllo:** assicurare che la gestione dei dati avvenga sempre attraverso processi e strumenti sicuri e testati;
5. **Autenticità:** garantire una provenienza affidabile dell'informazione.
6. **Privacy:** garantire la protezione ed il controllo dei dati personali.

Nell'ambito della gestione dei servizi offerti da FORTNES S.p.a., attraverso la propria infrastruttura tecnologica, l'osservanza dei livelli di sicurezza stabiliti attraverso l'implementazione dell'ISMS, assicura:

- La garanzia di aver incaricato un *partner* affidabile al trattamento del proprio patrimonio informativo;
- Un'elevata immagine aziendale;
- La completa osservanza delle *Service Level Agreement* stabilite con i clienti;
- La soddisfazione del cliente per quanto attiene alla qualità dell'informazione;
- Il rispetto delle normative vigenti e degli *stand ard* internazionali di sicurezza.

Per questo motivo, FORTNES S.p.a. ha sviluppato un sistema di gestione sicura delle informazioni, seguendo i requisiti specificati della norma UNI CEI EN ISO/IEC 27001:2017 e delle leggi cogenti come mezzo per gestire la sicurezza delle informazioni nell'ambito della propria attività.

4. AMBITO DI APPLICAZIONE

La politica per la sicurezza delle informazioni di FORTNES S.p.a. si applica a tutto il personale interno ed alle terze parti che collaborano alla gestione delle informazioni ed a tutti i processi e risorse coinvolte nella progettazione, realizzazione, avviamento ed erogazione continuativa nell'ambito dei servizi offerti.

5. POLITICA PER LA SICUREZZA DELLE INFORMAZIONI

La politica della sicurezza di FORTNES S.p.a. rappresenta l'impegno dell'organizzazione nei confronti di Committenti, Clienti e terze parti a garantire la sicurezza delle informazioni, degli strumenti fisici, logici e organizzativi atti al trattamento delle informazioni in tutte le attività.

La politica della sicurezza delle informazioni di FORTNES S.p.a. intende conseguire i seguenti obiettivi:

- a. Garantire all'organizzazione la piena conoscenza delle informazioni gestite e la valutazione della loro criticità, al fine di agevolare l'implementazione degli adeguati livelli di protezione.
- b. Garantire l'accesso sicuro alle informazioni, in modo da prevenire trattamenti non autorizzati o realizzati senza i diritti necessari.
- c. Garantire che l'organizzazione e le terze parti collaborino al trattamento delle informazioni adottando procedure volte al rispetto di adeguati livelli di sicurezza.
- d. Garantire che l'organizzazione e le terze parti che collaborano al trattamento delle informazioni, abbiano piena consapevolezza delle problematiche relative alla sicurezza.
- e. Garantire che le anomalie e gli incidenti aventi ripercussioni sul sistema informativo e sui livelli di sicurezza aziendale siano tempestivamente riconosciuti e correttamente gestiti attraverso efficienti sistemi di prevenzione, comunicazione e reazione al fine di minimizzare l'impatto sul business.
- f. Garantire che l'accesso alle sedi ed ai singoli locali aziendali avvenga esclusivamente da personale autorizzato, a garanzia della sicurezza delle aree e degli asset presenti.
- g. Garantire la conformità con i requisiti di legge ed il rispetto degli impegni di sicurezza stabiliti nei contratti con le terze parti.
- h. Garantire la rilevazione e la minimizzazione di eventi anomali, incidenti e vulnerabilità dei sistemi informativi al fine di rispettare la sicurezza e la disponibilità dei servizi e delle informazioni.
- i. Garantire la *business continuity* aziendale e il *disaster recovery*, attraverso l'applicazione di procedure di sicurezza stabilite.

La politica della sicurezza delle informazioni è formalizzata nell'ISMS, viene costantemente aggiornata per assicurare il suo continuo miglioramento ed è condivisa con l'organizzazione, le terze parti, i Committenti ed i clienti, attraverso un sistema *intranet* e specifici canali di comunicazione.

6. RESPONSABILITA' DELLA POLITICA DI SICUREZZA DELLE INFORMAZIONI

La Direzione è responsabile del sistema di gestione sicura delle informazioni, in coerenza con l'evoluzione

del contesto aziendale e di mercato, valutando eventuali azioni da intraprendere a fronte di eventi come:

- Evoluzioni significative del *business*;
- Nuove minacce rispetto a quelle considerate nell'attività di analisi del rischio;
- Significativi incidenti di sicurezza;
- Evoluzione del contesto normativo o legislativo in materia di trattamento sicuro delle informazioni.

