v.2 26.09.2022

Politica della Sicurezza delle Informazioni

Information Security Policy

Codice Documento PRS004,v.2

APPROVAZIONE ULTIMA VERSIONE
Creazione/Modifica 26.09.2022
Security Governance
Approvazione: 04.10.2022
IT Chief
Controllo: 26.09.2022
Responsabile Uff. Sistemi

STORIA DELLE REVISIONI
19.06.2013 – Prima emissione v.1
26.09.2022 – Integrazione v.2

INDICE

1. SCOPO

Lo scopo del presente documento è quello di descrivere i principi generali di sicurezza delle informazioni definiti da Previnet SpA al fine di sviluppare un efficiente e sicuro Sistema di Gestione della Sicurezza delle Informazioni.

2. DESCRIZIONE

Per Previnet SpA 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, attraverso il rispetto delle seguenti proprietà:

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 Previnet SpA, 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 dei Service Level Agreement, SLA stabiliti con i clienti;
- la soddisfazione del cliente;
- il rispetto delle normative vigenti e degli standard internazionali di sicurezza;

Per questo motivo Previnet SpA ha sviluppato un sistema di gestione sicura delle informazioni seguendo i requisiti specificati della Norma ISO 27001:2013 e delle leggi cogenti come mezzo per gestire la sicurezza delle informazioni nell'ambito della propria attività.

Come obiettivo primario la protezione dei dati e delle informazioni, della struttura tecnologica, fisica, logica ed organizzativa.

The primary objective of Previnet Spa information security policy is to protect data and information and the technological, physical, logical and organizational structure responsible for their management.

1. PURPOSE

The purpose of this document is to describe the general principles to the Information Security Policy defined by Previnet SpA in order to develop an efficient and secure Information Security Management System.

2. DESCRIPTION

The primary objective of Previnet Spa information security policy is to protect data and information and the technological, physical, logical and organizational structure responsible for their management.

This means implementing and maintaining an Information Security Management System, within the scope defined for the ISMS, and complying with the following principles:

1. **Confidentiality**: ensure that information is accessible only to duly authorized subjects and / or processes;
2. **Integrity:** safeguard the consistency of the data and information from unauthorized changes;
3. **Availability:** ensure that authorized users have access to information and associated architectural elements when they request it;
4. **Control:** ensure that data management always takes place through safe and tested processes;
5. **Authenticity**: guarantee reliable sourcing of information;
6. **Privacy:** guarantee the protection and control of personal data.

The Company, as part of the services offered, by means of its technological infrastructure and compliance with the security measures established by implementing the ISMS, ensures the following:

- guarantees its customers have appointed a reliable partner to process its information assets;
- a high corporate image;
- full compliance with the Service Level Agreements, SLA are agreed with customers;
- customer satisfaction;
- compliance with current regulations and international safety standards;

In order to achieve the above, Previnet SpA has developed an Information Security Management System following the specified requirements of the ISO 27001:2013 standard and legal requirements for managing information security services within its business.

3. AMBITO DI APPLICAZIONE

La politica per la sicurezza delle informazioni di Previnet SpA 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.

4. POLITICA PER LA SICUREZZA DELLE INFORMAZIONI

La politica della sicurezza di Previnet SpA rappresenta l'impegno dell'organizzazione nei confronti di 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 Previnet SpA si ispira ai seguenti principi:

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 la sicurezza incorporata come elemento essenziale delle reti, dei sistemi informativi, delle operazioni e degli accessi alle informazioni in modo da prevenire trattamento 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 consapevolezza della necessità della sicurezza delle informazioni.
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 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 ed i clienti, attraverso un sistema intranet e specifici canali di comunicazione.

Rappresenta l'impegno dell'organizzazione nei confronti di 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.

3. APPLICATION

The information security policy is applied to all internal staff and third parties who collaborate in the management of the information, it is also applied to all the processes and resources involved in the design, implementation, go-live phases and on-going provision of services.

4. INFORMATION SECURITY POLICY

Previnet SpA's security policy represents the organization's commitment to customers and third parties to ensure the security of information, physical, logical and organizational tools suitable for processing information in all activities.

Previnet SpA's information security policy is inspired by the following principles:

a. Guarantee the organization's full knowledge of the information managed and identify their risk factors by means of a thorough risk assessment in order to facilitate the implementation of adequate levels of protection.
b. Guarantee the embedded security as an essential element of networks, information systems, operations and access to information in order to prevent unauthorized processing or processing without the necessary rights.
c. Ensure that the organization and third parties collaborate in the processing of information by adopting procedures aimed at complying with adequate levels of security.
d. Ensure that the organization and third parties that collaborate in the processing of information are aware of the need for information security.
e. Ensure that anomalies and accidents affecting the information system and corporate security levels are promptly recognized and correctly managed through efficient prevention, notification and reaction systems in order to minimize the impact on the business.
f. Ensure that access to the offices and individual company premises is done exclusively by authorized personnel, to guarantee the safety of the areas and assets present.
g. Ensure compliance with legal requirements and compliance with the safety commitments established in contracts with third parties.
h. Guarantee that abnormal events, incidents and vulnerabilities of information systems are detected in order to respect the security and availability of services and information.
i. Ensure corporate business continuity and disaster recovery, through the application of established security procedures.

The information security policy is defined in the ISMS. It is updated constantly to ensure its continuous improvement and is shared with the organization, third parties and customers, through an intranet system or other specific communication channels.

Represents the organization's commitment to customers and third parties to ensure the security of information, physical, logical and organizational tools suitable for processing information in all activities.

5. RESPONSABILITÀ 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;

5. RESPONSIBILITY FOR INFORMATION SECURITY POLICY

Management is responsible for the Information Security Management System, consistent with the evolution of business and changes in the market, evaluating possible action to be taken in the face of events such as:

- important business developments;
- new threats related to those considered in the risk analysis activity;
- significant security incidents;
- evolution in regulatory or legislative requirements regarding the secure processing of information and data.