INFORMATION SECURITY POLICY (English Version)

Rev.	Date	Desc.	Red.	Ver.	App.
0	16/01/2021	First emission	RSGSI	RSGSI	AU
1	18/10/2022	Update	RSGSI	RSGSI	AU

PURPOSE AND OBJECTIVES

EPV Technologies management has defined and undertakes to keep this information security management policy active at all levels of its organization.

The purpose of this policy is to guarantee the protection against all the threats, internal or external, intentional or accidental, of information within the context of its activities in accordance with the indications provided by the ISO/IEC 27001 standard and the guidelines contained in the ISO/IEC 27002 standard in their latest versions.

FIELD OF APPLICATIONS

This policy applies without distinction to all the corporate levels.

The implementation of this policy is mandatory for all EPV Technologies personnel and must be included in the regulation of the agreements with any external subject who -for any reason- may be involved in the processing of information correlated to the scope of application of the Management System for Information Security (ISMS).

The company allows the communication and dissemination of information externally only for the correct performance of company activities which must take place in compliance with the mandatory rules and regulations.

INFORMATION SECURITY POLICY

The information assets to be protected consist of the set of information managed through the services provided and located in all company offices.

It is necessary to ensure:

- the confidentiality of the information: the information must be accessible only by authorized persons.
- information integrity: i.e. protecting the accuracy and completeness of information and the methods for processing it.
- the availability of information: authorized users can effectively access the information and related assets when they request it.

The lack of adequate levels of security can lead to damage to the corporate image, lack of customer satisfaction, the risk of incurring penalties related to the violation of current regulations as well as economic and financial damages.

An adequate level of security is also essential for sharing information.

The company identifies all security needs through risk analysis which allows you to gain awareness of the level of exposure to threats of your information system. The risk assessment makes possible to evaluate the potential consequences and damages that may derive from the failure to apply security measures to the information system and what is the realistic probability of implementation of the identified threats.

The results of this assessment determine the actions necessary to manage the identified risks and the most suitable security measures.

The general principles of information security management embrace various aspects:

- There must be a constantly updated catalog of corporate assets relevant to information management and a manager must be identified for each one. Information must be classified according to its level of criticality, so as to be managed with consistent and appropriate levels of confidentiality and integrity.
- To ensure information security, every access to the systems must foresee an authentication procedure. Information access authorizations must be differentiated according to the role and tasks covered by individuals, so that each user can access only the information needed, and must be periodically reviewed.
- Procedures must be defined for the safe use of company assets and information and their management systems.
- Full awareness of information security issues must be encouraged in all personnel (employees and collaborators) starting from the moment of selection and for the entire duration of the employment relationship. In order to handle incidents in a timely manner, everyone must report any safety-related issues. Each incident must be managed as indicated in the procedures.
- It is necessary to prevent unauthorized access to the offices and individual company premises where the information is managed and the security of the equipment must be guaranteed.
- Compliance with legal requirements and information security principles in contracts with third parties must be ensured.
- Must be prepared a continuity plan that allows the company to effectively deal with an unforeseen event, guaranteeing the restoration of critical services in time, avoiding the negative consequences .
- Security aspects must be included in all phases of design, development, operation, maintenance, support and decommissioning of IT systems and services.
- Compliance with the provisions of the law, statutes, regulations or contractual obligations with any requirement relating to information security must be guaranteed,

minimizing the risk of legal or administrative sanctions, significant losses or damage to reputation.

RESPONSABILITY OF COMPLIANCE AND IMPLEMENTATION

The observance and implementation of the requirements contained in this policy involved the following:

- all personnel who, in any capacity, collaborate with EPV and are involved with the processing of data and information, aligned with the scope of the Management System;
- all personnel responsible for reporting all anomalies and violations of which they become aware;
- all external subjects who maintain relationships and collaborate with the company.

The Management System Manager, within the scope of the Management System and through appropriate rules and procedures, must:

- conduct the risk analysis with the appropriate methodologies and adopt all risk management measures;
- establish all the rules necessary for the safe conduct of all company activities;
- verify security violations and take the necessary countermeasures and control the company's exposure to the main threats and risks;
- organize training and promote staff awareness of everything related to information security;
- periodically check the effectiveness and efficiency of the Management System.

Whoever, employees, consultants and/or external collaborators of EPV Technologies, intentionally or negligently, disregards the established safety rules and in this way causes damage to the company, may be prosecuted in the appropriate offices and in full compliance with the legal and contractual obligations.

REVIEW

The Management will check periodically or in conjunction with significant changes, the effectiveness and efficiency of the Management System, in order to ensure adequate support for the introduction of all the necessary improvements and in order to favor the activation of a process continuous, with which the control and adjustment of the policy is maintained in response to changes in the corporate environment, business, legal conditions.

The Management System Manager is responsible for reviewing the policy.

The review will verify the status of preventive and corrective actions and adherence to the policy. Must take into account all changes that may affect the company's approach to information security management, including organizational changes, technical environment, resource availability, legal, regulatory or contractual conditions and the results of previous reviews .

The result of the review must include all decisions and actions relating to the improvement of the company's approach to information security management.

MANAGEMENT COMMITMENT

Management actively supports information security in the company through clear guidance, clear commitment, explicit assignments and acknowledgment of responsibilities related to information security.

The management's commitment is implemented through a structure whose tasks are:

- ensure that all information security objectives are identified and that they all meet company requirements;
- establish corporate roles and responsibilities for developing and maintaining the ISMS;
- provide sufficient resources for the planning, implementation, organization, control, review, management and continuous improvement of the ISMS;
- check that the ISMS is integrated into all company processes and that procedures and controls are effectively developed;
- approve and support all initiatives aimed at improving information security;
- activate programs for the dissemination of information security awareness and culture.

POLITICA PER LA SICUREZZA DELLE INFORMAZIONI (Versione italiana)

Rev.	Data	Descrizione	Redazione	Verifica	Approvazione
0	16/01/2021	Prima emissione	RSGSI	RSGSI	AU
1	18/10/2022	Aggiornamento	RSGSI	RSGSI	AU

SCOPO E OBIETTIVI

La direzione della EPV Technologies 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.

Lo scopo della presente politica è garantire la tutela e la protezione da tutte le minacce, interne o esterne, intenzionali o accidentali, delle informazioni nell'ambito delle proprie attività in accordo con le indicazioni fornite dallo standard ISO/IEC 27001 e dalle linee guida contenute nello standard ISO/IEC 27002 nelle loro ultime versioni.

CAMPO DI APPLICAZIONE

La presente politica si applica indistintamente a tutti gli organi e i livelli dell'azienda.

L'attuazione della presente politica è obbligatoria per tutto il personale e deve essere inserita nella regolamentazione degli accordi con 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 per la Sicurezza delle Informazioni (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.

POLITICA PER LA 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.

È necessario assicurare:

- la confidenzialità delle informazioni: ovvero le informazioni devono essere accessibili solo da chi è autorizzato.
- l'integrità delle informazioni: ovvero proteggere la precisione e la completezza delle informazioni e dei metodi per la loro elaborazione.
- la disponibilità delle informazioni: ovvero che gli utenti autorizzati possano effettivamente accedere alle informazioni e ai beni collegati nel momento in cui lo richiedono.

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.

I principi generali della gestione della sicurezza delle informazioni abbracciano vari aspetti:

- Deve esistere un catalogo costantemente aggiornato degli asset aziendali rilevanti ai fini della gestione delle informazioni e per ciascuno deve essere individuato un responsabile. Le informazioni devono essere classificate in base al loro livello di criticità, in modo da essere gestite con livelli di riservatezza ed integrità coerenti ed appropriati.
- Per garantire la sicurezza delle informazioni, ogni accesso ai sistemi deve essere sottoposto a una procedura d'identificazione e autenticazione. 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.
- Devono essere definite delle 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.
- Per poter gestire in modo tempestivo gli incidenti, tutti devono notificare qualsiasi problema relativo alla sicurezza. Ogni incidente deve essere gestito come indicato nelle procedure.
- È necessario prevenire l'accesso non autorizzato alle sedi e ai singoli locali aziendali dove sono gestite le informazioni e deve essere garantita la sicurezza delle apparecchiature.
- Deve essere assicurata la conformità con i requisiti legali e con i principi legati alla sicurezza delle informazioni nei contratti con le terze parti.
- Deve essere predisposto un piano di continuità 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.
- Gli aspetti di sicurezza devono essere inclusi in tutte le fasi di progettazione, sviluppo, esercizio, manutenzione, assistenza e dismissione dei sistemi e dei servizi informatici.

- Devono essere garantiti il rispetto delle disposizioni di legge, di statuti, regolamenti o obblighi contrattuali e di ogni requisito inerente alla sicurezza delle informazioni, riducendo al minimo il rischio di sanzioni legali o amministrative, di perdite rilevanti o danni alla reputazione.

RESPONSABILITA' DI OSSERVANZA E ATTUAZIONE

L'osservanza e l'attuazione nonché il rispetto dei requisiti contenuti nella presente policy sono responsabilità di:

- Tutto il personale che, a qualsiasi titolo, collabora con la EPV ed è in qualche modo coinvolto con il trattamento di dati ed informazioni che rientrano nel campo di applicazione del Sistema di Gestione;
- Tutto il personale è altresì responsabile della segnalazione di tutte le anomalie e violazioni di cui dovesse venire a conoscenza;
- Tutti i soggetti esterni che intrattengono rapporti e collaborano con l'azienda.

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

- condurre l'analisi dei rischi con le opportune metodologie e adottare tutte le misure per la gestione del rischio;
- stabilire tutte le norme 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.

Chiunque, dipendenti, consulenti e/o collaboratori esterni della EPV Technologies, in modo intenzionale o riconducibile a negligenza, disattenda le regole di sicurezza stabilite 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.

RIESAME

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 policy in risposta ai cambiamenti dell'ambiente aziendale, del business, delle condizioni legali.

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

Il riesame dovrà verificare lo stato delle azioni preventive e correttive e l'aderenza alla politica. Dovrà tenere conto di tutti i cambiamenti che possono influenzare l'approccio della azienda alla gestione della sicurezza delle informazioni, includendo i cambiamenti organizzativi, l'ambiente tecnico, la disponibilità di risorse, le condizioni legali, regolamentari o contrattuali e dei risultati dei precedenti riesami.

Il risultato del riesame dovrà includere tutte le decisioni e le azioni relative al miglioramento dell'approccio aziendale alla gestione della sicurezza delle informazioni.

IMPEGNO DELLA DIREZIONE

La Direzione sostiene attivamente la sicurezza delle informazioni in azienda tramite un chiaro indirizzo, un impegno evidente, degli incarichi espliciti e il riconoscimento delle responsabilità relative alla sicurezza delle informazioni.

L'impegno della direzione si attua tramite una struttura i cui compiti sono:

- garantire che siano identificati tutti gli obiettivi relativi alla sicurezza delle informazioni e che questi incontrino i requisiti aziendali;
- stabilire i ruoli aziendali e le responsabilità per lo sviluppo e il mantenimento del SGSI;
- fornire risorse sufficienti alla pianificazione, implementazione, organizzazione, controllo, revisione, gestione e miglioramento continuo del SGSI;
- controllare che il SGSI sia integrato in tutti i processi aziendali e che procedure e controlli siano sviluppati efficacemente;
- approvare e sostenere tutte le iniziative volte al miglioramento della sicurezza delle informazioni;
- attivare programmi per la diffusione della consapevolezza e della cultura della sicurezza delle informazioni.