Information Security Policy

Vetimec's Management with this document sets out the Information Security Policy specifying the objectives and commitments arising from it.
The general objectives for the Information Security Management System are as follows:

- to create and implement an Information Security Management System in compliance with all mandatory regulations, laws and decrees in force, and with the maturity standards to which the company has decided to adhere or to which Customers require adherence;
- to create a continuously improving market image and guarantee Customers "business continuity" without the risk of interruption caused by potential information security incidents;
- to reduce the damage caused by potential incidents.

These objectives are in line with the company's objectives, strategy and business plans.
The aim is to perfect procedures ensuring that the organisation operates more efficiently, improves the control and safety of its activities and achieves increasingly challenging objectives.
Vetimec provides products that rely on resources, including information. The use of information resources shall be consistent with good working practices and procedures, as well as legal, regulatory and contractual requirements, and shall ensure the confidentiality, integrity and availability of all information resources of Vetimec and its Customers.
Information is an extremely important asset of Vetimec and enables it to fulfil its commercial functions and obligations towards its counterparties.
Vetimec's Information Security Management System ensures that it meets the legal, regulatory and contractual requirements for information security, including those provided for by the personal data protection legislation (EU Reg 2016/679, Legislative Decree 101/18 and Legislative Decree 196/03) and the Italian Data Protection Authority.
In terms of Information Security, in detail:

- the approach will be risk-based in accordance with ISO/IEC 27001:2013 and best practice;
- the procedures will establish risk assessment criteria aligned with Vetimec's current approved strategic business risk management policies.

It is the Management's precise intention and task to consolidate internal awareness towards the increasingly challenging objectives of information security, to strengthen the company's image and seriousness, above all through the search for transparency towards its Customers, the professionalism that is acknowledged to the company and an increasingly personalised and exclusive style.
It is therefore Vetimec's firm intention to implement and follow this Information Security Policy so that it is permeated and implemented at all company levels. The Company undertakes to train its collaborators in this sense.
This Policy represents the commitment on which the Information Security Management System is based.
All business processes (primary and support) are affected by the guidelines and directions defined in this document.
All stakeholders must take appropriate security measures in line with the principles set out in this policy.
Failure to comply with or violation of the principles set out in this policy may result in disciplinary action against employees under the National Collective Bargaining Agreement, as well as taking all permitted civil and criminal legal actions, and for external stakeholders in the review of the contractual relationship between the parties up to and including termination of the contract.
In particular, the Management confers on the Information Security Management System Manager (ISMSM) the responsibility for ensuring the application of the provisions and establishments of the Information Security System and for keeping the Management informed of the results of periodic audits.
Vetimec's Management will periodically review the company's current practices, policies and guidelines during the Management Review to recommend any changes or improvements to ensure that appropriate security measures are in place.
This Policy is a controlled document and is available to employees on the server on a read-only basis and to all stakeholders on the website. The Information Security Management System Manager (ISMSM) must ensure that all changes are disseminated and obsolete copies are removed and/or archived.
Together with this policy Vetimec has drawn up specific policies to regulate the following topics: incident management, business continuity management, password management, change management, Regulation on the correct Use of Company Assets, management of information backup and recovery.

Calderara di Reno (BO), 20/01/2022

On behalf of the Management of Vetimec

Dr. Silvia Pasquali

Politica per la Sicurezza delle Informazioni

La Direzione di Vetimec con la predisposizione del presente documento, intende definire la Politica per la Sicurezza delle Informazioni precisandone gli obiettivi e gli impegni da essa derivanti.
Gli obiettivi generali per il Sistema di Gestione della Sicurezza delle Informazioni sono i seguenti:

- creare ed implementare un Sistema di Gestione della Sicurezza delle Informazioni nel rispetto di tutte le norme cogenti, delle leggi e dei decreti in vigore, e degli standard di maturità ai quali l'azienda ha deciso di aderire oppure ai quali i Clienti richiedono l'adesione;
- creare una immagine di mercato in continuo miglioramento e garantire ai Clienti la "business continuity" senza rischi di interruzione originati da potenziali incidenti sulla sicurezza delle informazioni;
- ridurre i danni causati dai potenziali incidenti.

Tali obiettivi sono in linea con gli obiettivi aziendali, la strategia ed i piani aziendali dell'organizzazione.
Lo scopo è rappresentato dal perfezionamento delle procedure che possano garantire all'organizzazione di operare con maggiore efficienza, migliorare il controllo e la sicurezza delle attività e di raggiungere obiettivi sempre più sfidanti.
Vetimec fornisce prodotti che si basano su risorse, incluse le informazioni. L'uso delle risorse informative deve essere in linea con le buone pratiche e procedure di lavoro, nonché con i requisiti legali, normativi e contrattuali e deve garantire la riservatezza, l'integrità e la disponibilità di tutte le risorse informative di Vetimec e dei suoi Clienti.
L'informazione è un asset estremamente importante di Vetimec e consente alla stessa di adempiere alle proprie funzioni e obblighi commerciali nei confronti delle controparti.
Il Sistema di Gestione per la Sicurezza delle Informazioni di Vetimec garantisce che la stessa soddisfi i requisiti legali, regolamentari e contrattuali in materia di sicurezza delle informazioni, compresi quelli previsti dalla legge sulla protezione dei dati personali (Reg UE 2016/679, D.lgs. 101/18 e D.lgs. 196/03) e dal Garante Privacy.
In termini di Sicurezza dell'Informazione, nel dettaglio:

- l'approccio sarà basato sul rischio conformemente alla norma ISO/IEC 27001:2013 ed alle migliori pratiche;
- le procedure stabiliranno criteri di valutazione del rischio allineati con le attuali politiche di gestione del rischio strategico aziendale approvate da Vetimec.

È precisa intenzione e compito della Direzione consolidare la consapevolezza interna verso gli obiettivi sempre più sfidanti della sicurezza delle informazioni, rafforzare l'immagine e la serietà aziendale, soprattutto attraverso la ricerca di trasparenza verso i propri Clienti, della professionalità che è riconosciuta alla società e di uno stile sempre più personalizzato ed esclusivo.
È quindi ferma volontà di Vetimec implementare e seguire la presente Politica per la Sicurezza delle Informazioni affinché questa sia permeata ed attuata a tutti i livelli aziendali. La Società si impegna ad effettuare la formazione dei propri collaboratori in tal senso.
Questa Politica rappresenta l'impegno sul quale il Sistema per la Sicurezza delle Informazioni si basa.
Tutti i processi aziendali (primari e di supporto) sono interessati dalle linee guida e dagli indirizzi definiti nel presente documento.
È fatto obbligo a tutte le parti interessate di adottare adeguate misure di sicurezza in linea con i principi della presente politica.
Il mancato rispetto o la violazione dei principi di cui alla presente politica potrà dar luogo nei confronti del personale dipendente a provvedimenti disciplinari previsti dal CCNL, nonché all'applicazione di tutte le azioni civili e penali consentite, e per le parti interessate esterne alla revisione del rapporto contrattuale tra le parti fino alla risoluzione del contratto.
In particolare, la Direzione conferisce al Responsabile del Sistema di Gestione per la Sicurezza delle Informazioni (RSGSI) la responsabilità di assicurare l'applicazione di quanto previsto e stabilito dal Sistema per la Sicurezza delle Informazioni e di tenere informata la Direzione stessa dei risultati scaturiti dai periodici Audit.
L'Alta Direzione riesaminerà periodicamente, in fase di Riesame della Direzione, le pratiche, le politiche e le linee guida correnti dell'azienda per raccomandare eventuali modifiche o miglioramenti al fine di garantire l'applicazione di misure di sicurezza appropriate.
La presente Politica è un documento controllato e viene mantenuto a disposizione del personale dipendente sul server in sola lettura e di tutte le parti interessate sul sito web. Il Responsabile del Sistema di Gestione per la Sicurezza delle Informazioni (RSGSI) deve garantire che tutte le modifiche siano diffuse e che le copie obsolete siano rimosse e/o archiviate.
Assieme alla presente politica Vetimec ha redatto specifiche politiche atte a regolamentare le seguenti tematiche: gestione degli incident, gestione della business continuity, gestione delle password, gestione del cambiamento, Regolamento sul corretto Utilizzo degli Strumenti Aziendali, gestione del backup e ripristino delle informazioni.

Calderara di Reno (BO), 20/01/2022

La Direzione

Dott.ssa Silvia Pasquali