Borgaro Torinese, 18/06/2025

POLITICA PER LA SICUREZZA DELLE INFORMAZIONI

Per dare attuazione alla propria **Politica per la Sicurezza delle Informazioni**, VIGEL Spa ha sviluppato e si impegna a mantenere costantemente aggiornato un **Sistema di Gestione per la protezione delle Informazioni** (**SGSI**) conforme alle prescrizioni della norma tecnica **ISO/IEC 27001:2022**, del **framework TISAX®** e delle norme giuridiche cogenti in materia.

In particolare, nell'ambito della gestione delle proprie informazioni, VIGEL assicura:

1) Il rispetto delle norme giuridiche e tecniche vigenti e degli standard internazionali di sicurezza che impattano sulla propria infrastruttura tecnologica e organizzativa;
2) L'osservanza dei livelli di sicurezza prefissati attraverso l'implementazione e il mantenimento di un **Sistema di Gestione della Sicurezza delle Informazioni** (**SGSI**);
3) La verifica di conformità del SGSI rispetto ai requisiti previsti dalle norme o framework di riferimento sopra citati e la gestione di eventuali non conformità o incidenti attraverso opportune azioni correttive, considerate anche come strumento per il controllo e il miglioramento dei processi, e qualora ve ne siano i presupposti, anche attraverso azioni disciplinari ai sensi del CCNL;
4) La selezione di partner affidabili dal punto di vista della gestione in sicurezza delle informazioni e della protezione dei dati personali, secondo le previsioni del Regolamento (UE) 2016/679;
5) La protezione e la valorizzazione dell'ambiente, minimizzando l'impatto delle attività aziendali sullo stesso, con particolare attenzione agli effetti sul cambiamento climatico ("*climate change*").

La presente **Politica per la Sicurezza delle Informazioni**, diffusa in edizione digitale attraverso la pubblicazione sul sito web istituzionale e in edizione cartacea tramite affissione nelle bacheche aziendali, si applica a tutto il personale interno e a quello di terze parti che a diverso titolo tratta, archivia e trasmette informazioni nello svolgimento dei processi aziendali e rappresenta concretamente l'impegno dell'organizzazione nei confronti dei propri dipendenti e collaboratori, dei clienti e delle terze parti, finalizzato a garantire la gestione sicura delle informazioni e degli strumenti fisici, logici e organizzativi atti al trattamento delle informazioni stesse, in tutte le proprie attività e processi.

In sintesi, la presente **Politica per la Sicurezza delle Informazioni** è finalizzata al perseguimento dei seguenti obiettivi:

1) L'organizzazione abbia piena conoscenza delle informazioni gestite e ne valuti la rispettiva criticità, al fine di progettare e implementare adeguati livelli di protezione;
2) L'accesso alle informazioni avvenga in modo sicuro e adeguato al fine di prevenire eventuali trattamenti non autorizzati o realizzati senza i necessari diritti d'accesso;
3) Il personale interno e quello delle terze parti che concorre al trattamento delle informazioni sia consapevole e adeguatamente formato rispetto alle problematiche relative alla sicurezza delle stesse e adotti procedure volte all'osservanza di adeguati livelli di protezione;
4) Le eventuali anomalie, incidenti o vulnerabilità aventi ripercussioni sul sistema informativo, sui servizi e sui livelli di sicurezza aziendale siano tempestivamente rilevati e adeguatamente trattati, attraverso efficienti sistemi di prevenzione, comunicazione e reazione, al fine di minimizzare l'impatto sul business, e in particolare sulla sicurezza e sulla disponibilità dei servizi e delle informazioni;
5) La "*business continuity*" aziendale e il "*disaster recovery*", attraverso l'applicazione di procedure di sicurezza definite e periodicamente testate;
6) L'accesso fisico ai locali aziendali avvenga esclusivamente da parte di personale autorizzato, a garanzia della sicurezza delle aree e degli asset in esse conservati;
7) L'osservanza dei requisiti di legge e il rispetto degli impegni di sicurezza previsti nei contratti con le terze parti;
8) I trattamenti di dati personali, sia nei casi in cui Vigel operi in qualità di Titolare che nei casi in cui operi per conto terzi in qualità di Responsabile del Trattamento, avvengano nel rispetto del Regolamento Europeo sulla Protezione dei Dati Personali (GDPR 679/2016).

La presente Politica per la Sicurezza delle Informazioni viene periodicamente sottoposta a monitoraggio ed eventuale revisione attraverso un processo di Riesame da parte della Direzione, per assicurarne l'adeguatezza e promuovere il suo continuo miglioramento, ed è condivisa con l'organizzazione, le terze parti e i clienti, attraverso le modalità sopra descritte.

Per realizzare i principi e gli obiettivi sopra individuati, Vigel si impegna ad attuare misure organizzative e operative finalizzate a garantire:

1) **La riservatezza delle informazioni** trattate, archiviate e trasmesse, attraverso la definizione puntuale di responsabilità interne e procedure operative per la gestione dei servizi e delle informazioni ad essi connesse e attuando un puntuale controllo degli accessi fisici e logici agli archivi elettronici e cartacei, limitati in via esclusiva al solo personale autorizzato;

2) **L'integrità delle informazioni**, applicando procedure di backup e di "*disaster recovery*" e restringendo gli accessi fisici e logici alle informazioni al solo personale autorizzato;

3) **La disponibilità delle informazioni** attraverso l'identificazione puntuale di ruoli, funzioni aziendali e relativi diritti di accesso alle informazioni e agli *asset* necessari per lo svolgimento dei processi aziendali interni ed esterni;

4) Che in linea generale ogni accesso, di tipo fisico o digitale, sia autorizzato, controllato e monitorato sulla base dei seguenti criteri:
   a) l'accesso è autorizzato al personale abilitato per le sole informazioni strettamente necessarie allo svolgimento della propria attività (principio della conoscenza minima o necessità di sapere);
   b) l'accesso è autorizzato al personale abilitato solo per le informazioni relative alle specifiche attività svolte;
   c) l'accesso all'infrastruttura ICT e agli spazi fisici è consentito al solo personale autorizzato in linea con la Politica aziendale;

5) Che dipendenti, fornitori, partner, appaltatori e ogni altra terza parte coinvolta nel trattamento di informazioni rientranti nel campo di applicazione del Sistema di Gestione della Sicurezza delle Informazioni siano consapevoli del proprio ruolo e dell'impatto delle proprie azioni sulla sicurezza delle informazioni, e accettino conseguentemente gli obblighi e le responsabilità di propria pertinenza, al fine di proteggere le informazioni, i beni e le risorse dell'organizzazione;

6) Che le risorse umane siano informate in merito ai principi enunciati dalla presente Politica e adeguatamente formate e addestrate rispetto alle procedure di lavoro che impattano sulla gestione sicura delle informazioni;

7) Che i trattamenti delle informazioni, delle attività, delle risorse e delle soluzioni inerenti alla protezione delle informazioni proprie dell'organizzazione o gestiti dalla stessa per conto dei propri clienti siano conformi alle norme giuridiche, tecniche o regolamentari applicabili di natura cogente, contrattuale o volontaria;

8) Che ogni attività e risorsa dell'organizzazione o affidata da questa a terze parti, nonché ogni informazione pertinente l'ambito del SGSI, sia protetta rispetto a minacce attinenti alla riservatezza, all'integrità e alla disponibilità, in proporzione al loro valore e nel rispetto delle norme vigenti;

9) Che tutto il personale di Vigel sia responsabilizzato in merito all'obbligo di:
(a) rispettare le norme giuridiche e regolamentari vigenti, di natura cogente, contrattuale e volontaria applicabili nel perimetro del SGSI; (b) proteggere la proprietà intellettuale, la riservatezza, l'integrità e la disponibilità delle informazioni gestite direttamente da Vigel o affidate a terze parti; (c) aver cura dei beni materiali, dei sistemi e delle risorse di Vigel; (d) salvaguardare e gestire in modo appropriato ogni informazione e dato afferenti le attività di propria competenza; (e) contattare la Direzione, il Comitato per la Gestione della Sicurezza delle Informazioni e/o altre autorità competenti in caso di effettive o sospette violazioni della sicurezza; (f) segnalare qualsiasi necessità di modifiche o integrazioni alle procedure relative alla gestione della sicurezza delle informazioni.

Compatibilmente con i propri ruoli e le relative responsabilità attinenti alla gestione della sicurezza delle informazioni, ciascuno deve inoltre:
(g) garantire la conformità con la presente Politica, i requisiti, gli standard e/o le procedure definite; (h) individuare e definire i diritti di accesso agli assets secondo le loro specifiche attività e responsabilità; (i) richiedere formalmente alle terze parti il rispetto degli accordi di riservatezza; (l) operare in conformità ai livelli di rischio che sono stati definiti per il proprio ambito di pertinenza.

Tutto il personale a cui sono assegnate responsabilità specifiche nella gestione della sicurezza delle informazioni ha altresì il dovere di:
(m) implementare la sicurezza sulla base delle politiche di Vigel; (n) garantire e monitorare il rispetto della presente Politica, dei requisiti, norme e procedure rilevanti nell'ambito del SGSI; (o) monitorare gli assets aziendali e proteggerli adeguatamente secondo le norme tecniche e giuridiche applicabili; (p) applicare regole, funzioni, strumenti, oggetti e controlli coerenti e funzionali agli scopi dell'organizzazione e che garantiscono il rispetto dei requisiti del SGSI; (q) garantire che il personale di Vigel e i terzi siano informati e formati circa la Politica, i requisiti, standard e/o procedure per la gestione della sicurezza delle informazioni, nonché siano resi consapevoli delle conseguenze in caso di mancato rispetto della Politica e dei requisiti stabiliti in tali ambiti; (r) adottare misure adeguate per garantire il controllo sugli aspetti che hanno impatto sulla sicurezza delle informazioni; (s) contenere il livello di rischio negli ambiti di pertinenza; (t) mantenere attive le misure da adottarsi in caso di incidenti derivanti dal verificarsi di condizioni anomale e di emergenza, e attivare i "piani di continuità" previsti dal SGSI.

Inoltre, i soggetti terzi che gestiscono in modo diretto o indiretto gli assets sensibili di Vigel e dei clienti, sono obbligati, nello svolgimento di tali processi e attività, a:

(u) formalizzare il proprio impegno alla riservatezza e non divulgazione delle informazioni trattate negli ambiti di competenza; (v) proteggere le risorse e le informazioni fisiche e intellettuali a cui possono accedere nell' effettuare le attività assegnate; (z) garantire la piena osservanza delle prescrizioni del SGSI.

LA PRESIDENZA