Borgaro Torinese, 20/11/2023

Politica per la Sicurezza delle informazioni

Il sistema di Gestione della Sicurezza della Informazioni | SGSI

Per dare attuazione alla propria politica della sicurezza delle informazioni, **VIGEL S.p.A., ha sviluppato e si impegna a mantenere un sistema di gestione sicura delle informazioni conforme ai requisiti specificati della Norma UNI CEI EN ISO/IEC 27001:2017 e dal framework TISAX® (Trusted Information Security Assessment eXchange)** e delle leggi cogenti come mezzo per gestire la sicurezza delle informazioni nell'ambito della propria attività.

Nell'ambito della gestione delle proprie informazioni, Vigel assicura:

- il rispetto delle normative vigenti e degli standard internazionali di sicurezza per la propria infrastruttura tecnologica e organizzativa;
- l'osservanza dei livelli di sicurezza stabiliti attraverso l'implementazione di un sistema di gestione della sicurezza delle informazioni (SGSI);
- la verifica di conformità del SGSI rispetto ai requisiti previsti dalle norme/framework di riferimento sopra citate e la gestione di eventuali non conformità attraverso opportune azioni correttive, considerate anche come strumento per il controllo dei processi e per il loro miglioramento, e qualora ve ne siano i presupposti, attraverso azioni disciplinari ai sensi del CCNL;
- la selezione di partner affidabili dal punto di vista della gestione in sicurezza delle informazioni e della protezione dei dati personali.

La presente politica per la sicurezza delle informazioni, in ultima revisione, è diffusa attraverso la pubblicazione sul sito aziendale ("https://www.vigel.com") e l'affissione nelle bacheche poste all'interno dell'azienda e si applica a tutto il personale interno e quello delle terze parti che collaborano alla gestione delle informazioni ed a tutti i processi e risorse coinvolte nelle attività produttive di Vigel.

La presente politica della sicurezza di Vigel rappresenta in concreto l'impegno dell'organizzazione nei confronti di clienti e delle terze parti a garantire la sicurezza delle informazioni, degli strumenti fisici, logici e organizzativi atti al trattamento delle informazioni in tutte le proprie attività.

In sintesi, la politica della sicurezza delle informazioni di Vigel garantisce che:

1. l'organizzazione abbia piena conoscenza delle informazioni gestite e valuti di volta in volta la loro criticità, al fine di agevolare l'implementazione di adeguati livelli di protezione;
2. l'accesso alle informazioni avvenga in modo sicuro e adatto a prevenire i trattamenti non autorizzati o realizzati senza i diritti necessari;
3. l'organizzazione e le terze parti collaborino al trattamento delle informazioni adottando procedure volte al rispetto di adeguati livelli di sicurezza;
4. l'organizzazione e le terze parti che collaborano al trattamento delle informazioni siano adeguatamente formate e abbiano piena consapevolezza delle problematiche relative alla sicurezza;
5. le anomalie e gli incidenti aventi ripercussioni sul sistema informativo, sui servizi 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;
6. l'accesso alla sede ed ai singoli locali aziendali avvenga esclusivamente da personale autorizzato, a garanzia della sicurezza delle aree e degli asset presenti;
7. la conformità con i requisiti di legge ed il rispetto degli impegni di sicurezza stabiliti nei contratti con le terze parti;
8. 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;

9. la business continuity aziendale e il disaster recovery, attraverso l'applicazione di procedure di sicurezza stabilite;
10. i trattamenti dei 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, avvenga nel rispetto del Regolamento Europeo sulla Protezione dei Dati Personali GDPR 679/2016.

La politica della sicurezza delle informazioni viene costantemente aggiornata e verificata, attraverso un riesame da parte della Direzione, per assicurare il suo continuo miglioramento ed è condivisa con l'organizzazione, le terze parti ed i clienti, attraverso le modalità espresse precedentemente.

Dichiarazione di impegno

Vigel si impegna a garantire:

- **la riservatezza delle informazioni** attraverso la definizione puntuale delle responsabilità interne per la gestione dei servizi e delle informazioni ad essi connesse; il controllo degli accessi fisici e logici agli archivi elettronici e cartacei esclusivamente da parte di personale autorizzato e competente;

- **l'integrità delle informazioni** attraverso il controllo degli accessi fisici e logici agli archivi elettronici esclusivamente da parte di personale autorizzato e competente e la gestione dei back-up dei dati e delle configurazioni dei sistemi informativi;

- **la disponibilità delle informazioni** attraverso l'identificazione dei ruoli e delle funzioni, i diritti di accesso alle informazioni e agli assets aziendali per la gestione dei servizi al Cliente;

- che dipendenti, fornitori, partner, appaltatori e ogni altra terza parte coinvolta con il trattamento di informazioni che rientrano nel campo di applicazione del Sistema di Gestione della Sicurezza delle Informazioni, accettino **gli obblighi e le responsabilità** di propria pertinenza, al fine di proteggere le informazioni, i beni e le risorse di Vigel;

- che ogni **accesso**, di tipo fisico o informatico, sia autorizzato, **controllato** e monitorato sulla base dei seguenti criteri: (a) l'accesso è autorizzato al personale abilitato solo per le informazioni necessarie (principio della conoscenza minima o necessità di sapere); (b) l'accesso è autorizzato al personale abilitato solo per le informazioni relative alle attività specifiche (funzione di lavoro-correlati); (c) l'accesso alla struttura e ai locali è autorizzato al personale abilitato. L'accesso ai locali di Vigel è autorizzato, controllato e monitorato in linea con la politica aziendale.

- che ogni dipendente, fornitore, imprenditore e terza parte sia **consapevole** del proprio ruolo e dell'impatto delle proprie azioni sulla sicurezza delle informazioni.

- che ogni risorsa sia adeguatamente **formata** e addestrata sulle politiche e sulle procedure relative alla gestione della sicurezza delle informazioni.

- che i trattamenti delle informazioni, delle attività, delle risorse e delle soluzioni inerenti la protezione delle informazioni di Vigel o gestiti dalla stessa per conto dei propri clienti sono **conformi alle leggi e ai regolamenti** applicabili di natura cogente, contrattuale e volontaria.

- che ogni attività e risorsa di Vigel o affidata da questa a terze parti, nonché ogni informazione pertinente l'ambito del SGSI, è **protetta** contro i problemi legati alla riservatezza, l'integrità e la disponibilità, in proporzione al loro valore e nel rispetto delle leggi vigenti.

- che tutto il **personale** Vigel sia **responsabilizzato** all'obbligo di: (a) garantire il rispetto delle norme, leggi e regolamenti vigenti, di natura cogente, contrattuale e volontaria rese applicabili negli ambiti del SGSI; (b) proteggere la riservatezza, l'integrità e la disponibilità delle informazioni gestite da Vigel, la proprietà intellettuale e il patrimonio di Vigel o da questa affidati a terze parti; (c) aver cura dei beni materiali, i sistemi e le 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 Responsabile della Sicurezza delle informazioni e/o altre autorità competenti in caso di effettive o sospette violazioni della sicurezza; (f) segnalare qualsiasi necessità di modifiche alle procedure relative alla gestione della sicurezza delle informazioni. | Compatibilmente con le autorità assegnate nella gestione della sicurezza ciascuno deve: (g) garantire la conformità con la politica di sicurezza, requisiti, standard e/o procedure definiti; (h) individuare e definire i diritti di accesso agli assets per le loro specifiche attività e responsabilità;

(i) richiedere alle terze parti di essere formalmente in linea con gli accordi di riservatezza; (l) operare in conformità ai livelli di rischio che sono stati definiti per il proprio ambito di pertinenza.

- che tutto il **personale** 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 sicurezza della Vigel; (n) garantire e monitorare il rispetto delle politiche di sicurezza delle informazioni, requisiti, norme e procedure definiti da Vigel nell'ambito del SGSI; (o) monitorare gli assets aziendali, al fine di garantire il rispetto del livello di controllo previsto per l'asset da proteggere ed il rispetto delle leggi e regolamenti applicabili; (p) rendere effettive l'insieme di regole, funzioni, strumenti, oggetti e controlli, resi coerenti e funzionali agli scopi dell'organizzazione e coerenti con gli ambiti del SGSI, che garantiscano che nella struttura, organizzazione, ambiente informatico, singolo elaboratore, sia costantemente osservato il rispetto dei requisiti del SGSI; (q) garantire che il personale di Vigel e i terzi siano formati e informati circa la politica, i requisiti, standard e/o procedure per la gestione della sicurezza delle informazioni, nonché resi consapevoli delle conseguenze in caso di mancato rispetto della politica e requisiti stabiliti in tali ambiti;
  (r) sostenere l'adozione di misure adeguate a 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, garantire l'adozione dei piani di continuità in conformità ai requisiti definiti dal SGSI.

- Inoltre, che i **soggetti terzi** che gestiscono in modo diretto o indiretto gli assets sensibili di Vigel e dei Clienti, **sono obbligati**, nello svolgimento di processi/attività, a:
  (u) formalizzare il proprio impegno alla riservatezza e non divulgazione delle informazioni tratte negli ambiti di competenza; (v) proteggere le risorse e le informazioni fisiche e intellettuali a cui possono accedere nella effettuazione delle attività assegnate; (z) garantire la piena osservanza ai requisiti del SGSI nei comportamenti e nell'operatività.

In conclusione, Vigel si impegna a:

adottare un sistema di gestione sicura delle informazioni conforme ai requisiti specificati della Norma ISO/IEC 27001:2017 e dal framework TISAX® (Trusted Information Security Assessment eXchange);

mantenere costantemente monitorato il grado di conformità del sistema alle norme e leggi applicabili di natura cogente e volontaria, e gli obblighi contrattuali pertinenti l'ambito di applicazione del SGSI;

revisionare la Politica per la Sicurezza delle Informazioni ogni qualvolta si verifichino cambiamenti significativi, al fine di garantirne l'idoneità, l'adeguatezza e l'efficacia;

garantire mezzi e risorse idonee al suo mantenimento e miglioramento continuo, in particolare per quanto attiene la mitigazione/riduzione dei livelli di rischio sulla sicurezza delle informazioni e l'adozione di misure idonee a prevenire – ovvero gestire adeguatamente – situazioni anomale e di emergenza;

rendere consapevoli tutte le persone che dell'organizzazione degli obblighi e delle responsabilità di ciascuno nella gestione della sicurezza delle informazioni e delle conseguenze in caso di eventi, dolosi e colposi, relativi all'utilizzazione non autorizzata, modifica o distruzione di informazioni critiche.

La Presidenza