

Information & Cyber Security Policy

Società:

Esprinet S.p.A, Esprinet Iberica S.L.U., V-Valley S.r.l, V-Valley Advanced Solutions España S.A., Zeliatech S.r.l.

Sede:

Tutte le sedi

Sottosistema:

ISO9001; D. Lgs. 231/01; Código Penal; NIS2; GDPR; ISO/IEC 27001 (SGSI Esprinet S.p.A., sede di Vimercate)

Nome file:

LIG01006- Information & Cyber Security Policy

Responsabilità per il documento:

Rev.	Data	Nota di Revisione	Redatto	Controllato	Approvato
00	07/11/24	Prima emissione	C.Pedrazzini CIO	A. Biffi Risk Manager	A.Cattani CEO
01	22/10/26	Aggiornamento societario, cambio CEO e aggiunta ruoli di responsabilità	C.Pedrazzini CIO / SGSI	A. Biffi Risk Manager	G.Testa CEO

PRESA VISIONE SOCIETA' DEL GRUPPO

 V-Valley <small>enhancing your business</small> Sergio Grassi Legale Rappresentante	 Zeliatech <small>THE GREEN SIDE OF ESPRINET</small> Sergio Grassi Legale Rappresentante	 idMAINT Sergio Grassi Legale Rappresentante	 BLUDIS <small>VALUE ADDED DISTRIBUTOR</small> Maurizio Erban Legale Rappresentante	 sifar Sergio Grassi Legale Rappresentante
--	--	---	--	---

Sommario

PRESA VISIONE SOCIETA' DEL GRUPPO	1
1. SCOPO	3
2. CAMPO DI APPLICAZIONE.....	3
3. REGOLE COMPORTAMENTALI.....	3
3.1. MONITORAGGIO E REVISIONE	3
3.2. DISTRIBUZIONE DELLA POLITICA	4
4. NORMATIVE E DOCUMENTI DI RIFERIMENTO	4
4.1. RIFERIMENTI ESTERNI	4
4.2. RIFERIMENTI INTERNI	5
5. RESPONSABILITÀ	5
6. DEFINIZIONI.....	6
7. PRINCIPI GENERALI RELATIVI ALLA SICUREZZA DELLE INFORMAZIONI	8
7.1. USO SICURO DEGLI STRUMENTI INFORMATICI	8
7.2. SECURITY E PRIVACY BY DESIGN	9
7.3. NEED TO KNOW.....	9
7.4. SISTEMI DI INTELLIGENZA ARTIFICIALE.....	9
7.5. SEPARAZIONE DEI RUOLI	9
8. FRAMEWORK DI GESTIONE DELLA SICUREZZA DELLE INFORMAZIONI	9
8.1. STRATEGIE DI SICUREZZA	10
8.2. CLASSIFICAZIONE E GESTIONE DEGLI ASSET IT	10
8.3. GESTIONE DEL RISCHIO INFORMATICO	11
8.4. FORMAZIONE E AWARENESS (PERSONALE E SICUREZZA)	11
8.5. GESTIONE DELLE SECURITY OPERATIONS.....	12
8.6. ASPETTI DI SICUREZZA CORRELATI AGLI ACCESSI LOGICI	13
8.7. GESTIONE DEGLI STRUMENTI CRITTOGRAFICI	14
8.8. GESTIONE DELLE VULNERABILITÀ	15
8.9. SICUREZZA DEI DISPOSITIVI AZIENDALI	15
8.10. GESTIONE DEGLI INCIDENTI INERENTI LA SICUREZZA DELLE INFORMAZIONI.....	15
8.11. GESTIONE DEGLI ASPETTI DI BUSINESS CONTINUITY	16
8.12. GESTIONE DELLA SICUREZZA FISICA	16
8.13. GESTIONE DELLE TERZE PARTI	17
8.14. CONFORMITÀ.....	17
8.15. PROTEZIONE DEI DATI PERSONALI	17
9. PROVVEDIMENTI DISCIPLINARI	18
10. ARCHIVIO	18

1. SCOPO

In considerazione del ruolo centrale assunto dalle informazioni nel contesto aziendale, il Gruppo Esprinet (di seguito: "Esprinet" o "il Gruppo") ha predisposto la presente Politica che detta le linee guida per tutto il Gruppo al fine di garantire un'adeguata protezione delle informazioni e del sistema informativo nel suo complesso, attraverso l'adozione di un approccio unico, consistente e standardizzato.

Il mancato perseguimento degli obiettivi di protezione del patrimonio informativo potrebbe, infatti, comportare per Esprinet forti impatti sul business e sull'operatività aziendale, derivanti dai rischi cui il patrimonio informativo aziendale è esposto (es. perdite economiche, danni di immagine, perdita di competitività sul mercato, sanzioni relative al mancato rispetto delle normative vigenti, ecc.).

2. CAMPO DI APPLICAZIONE

La presente Politica si applica a tutte le risorse (sistemi tecnologici, procedure organizzative, attività, ecc.) coinvolte nella gestione delle informazioni di tutte le società del Gruppo.

Ciascuna Società è tenuta a recepire la presente Politica, in accordo con le proprie procedure di approvazione interne.

Restano al di fuori dell'ambito di applicazione della presente Politica gli aspetti riguardanti la sicurezza sul luogo di lavoro, la tutela della salute delle persone, la tutela ambientale e, in generale, la protezione dei beni materiali ed immateriali non afferenti al patrimonio informativo di Esprinet.

3. REGOLE COMPORTAMENTALI

Tutte le attività devono essere svolte nel rispetto dei principi di attribuzione di responsabilità e di rappresentanza, di separazione dei ruoli e dei compiti, di lealtà, correttezza, trasparenza e tracciabilità degli atti.

Nello svolgimento delle attività, i Destinatari della presente Politica devono conoscere e rispettare:

- la normativa locale applicabile alle attività svolte;
- le disposizioni contenute nel presente documento;
- il Codice Etico e il Modello di organizzazione, gestione e controllo;
- le procedure e le linee guida di Esprinet,
- la documentazione attinente il sistema di organizzazione, gestione e controllo della Società.

3.1. MONITORAGGIO E REVISIONE

Il presente documento dovrebbe essere rivisto e, se necessario aggiornato ogni volta che si verifica un cambiamento importante che potrebbe influire sul contenuto dello stesso.

3.2. DISTRIBUZIONE DELLA POLITICA

La presente Politica è comunicata a tutti i dipendenti ed in via generale, a tutti coloro che, in virtù di un rapporto di lavoro subordinato, parasubordinato o in qualsiasi forma costituito, o di un rapporto di fornitura (dipendenti, collaboratori, fornitori, business partner, stagisti, personale somministrato ed altro), sia coinvolto nella gestione di componenti del sistema informativo e nel trattamento di informazioni di proprietà di Esprinet.

Esprinet riconosce la formazione e l'informazione dei dipendenti come strumenti chiave per il riconoscimento e l'attuazione di questa Politica.

4. NORMATIVE E DOCUMENTI DI RIFERIMENTO

La conformità ai requisiti di sicurezza definiti dalla normativa vigente e dagli Standard e dalle Best Practice di maggiore diffusione a livello internazionale, risulta imprescindibile nell'ambito del raggiungimento degli obiettivi individuati nella presente Politica.

4.1. RIFERIMENTI ESTERNI

Riferimenti normativi:

- Regolamento Europeo 2016/679 (GDPR): Regolamento generale per la protezione dei dati personali.
- D. Lgs. 231/2001 o il Decreto Legislativo 8 giugno 2001, n. 231 (Italia); Codice Penale spagnolo o Ley Orgánica 10/1995, de 23 de noviembre (Spagna); Codice Penale portoghese o Decreto-Lei n.º 48/95 (Portogallo); Codice Penale marocchino o Dahir 1-59-413 (Marocco). Questi normativi introducono e disciplinano la responsabilità "amministrativa" degli enti, nell'ipotesi di commissione, da parte di soggetti apicali o sottoposti, dei reati espressamente indicati nel Decreto medesimo, dai quali l'ente ha tratto un interesse o un vantaggio.
- Modello di organizzazione, gestione e controllo ai sensi del D. Lgs. 231/2001 o Modello 231: documento adottato dalla Società, ai sensi degli articoli 6 e 7 del D. Lgs. 231/2001, al fine di prevenire la realizzazione dei reati ivi indicati da parte del personale apicale o subordinato, così come descritto nello stesso Modello 231 e nei relativi allegati o documenti equivalenti adottati dalle controllate di Esprinet. Codice Penale spagnolo o Ley Orgánica 10/1995, de 23 de noviembre (Spagna); Codice Penale portoghese o Decreto-Lei n.º 48/95 (Portogallo); Codice Penale marocchino o Dahir 1-59-413 (Marocco)

Standard e Best Practice:

- **ISO/IEC 27001** (Tecnologie Informatiche - Tecniche di sicurezza - Sistemi di gestione della Sicurezza dell'Informazione - Requisiti): Standard internazionale che definisce i requisiti per pianificare, attuare, operare, monitorare, riesaminare, mantenere e migliorare il sistema di gestione per la Sicurezza delle Informazioni delle Aziende.

- **NIST CSF** (National Institute of Standards and Technology - Cybersecurity Framework): standard internazionale che fornisce alle organizzazioni una guida su come prevenire, rilevare e rispondere agli attacchi Cyber e gestire i relativi rischi.
- **UNI EN ISO 9001** (Sistemi di gestione per la qualità – Requisiti): Standard internazionale per il miglioramento della qualità

4.2. RIFERIMENTI INTERNI

- Procedura per la gestione del data breach
- Procedura assegnazione TOKEN-OTP (One Time Password) per Accesso VPN
- Procedura in tema di predisposizione e divulgazione dei comunicati di cui all'art. 114 TUF e art. 66 RE e altre comunicazioni al pubblico
- Linee guida uso dei videotermini, notebook, smartphone e lettori a radiofrequenza
- Policy comunicazioni marketing
- Politica aziendale relativa all'utilizzo degli strumenti informatici e alla sicurezza delle informazioni
- Regolamento Smart Working
- Codice di Comportamento Fornitori: documento che definisce le linee guida alle quali devono attenersi gli appaltatori, i consulenti, i professionisti, i fornitori caratteristici nonché i business partner (di seguito i "Destinatari") delle Società del Gruppo Esprinet ed eventuali subappaltatori, operanti come persone fisiche ovvero in forma organizzata d'impresa
- Codice Etico: documento, ufficialmente voluto e approvato dal vertice del Gruppo, contenente i principi generali di comportamento - ovvero, raccomandazioni, obblighi e/o divieti - cui i Destinatari devono attenersi nell'esercizio della propria attività e la cui violazione può essere specificamente sanzionata

5. RESPONSABILITÀ

Una governance efficace della Sicurezza delle Informazioni non può prescindere dalla puntuale definizione dei ruoli e delle responsabilità assunte in tale ambito.

Il Gruppo Esprinet attribuisce puntualmente ed in modo non ambiguo i ruoli e le responsabilità in materia di sicurezza al proprio personale. L'accountability è condizione necessaria per il raggiungimento ed il mantenimento nell'ambito di Esprinet e delle Società del Gruppo degli obiettivi di sicurezza definiti. A tale scopo, le Società del Gruppo provvedono a verificare nel continuo che l'operato del personale sia conforme con quanto definito.

In ogni caso, per garantire l'applicazione della presente Politica ed il raggiungimento degli obiettivi di sicurezza, tutto il personale è comunque coinvolto e responsabilizzato nell'efficace realizzazione del Framework inerente alla gestione della Sicurezza delle Informazioni.

Le attività inerenti alla Sicurezza delle Informazioni, inclusi i dati personali, prevedono il coinvolgimento delle funzioni di seguito riportate:

- Alta Direzione
- Funzione Risk Management
- Funzione Internal Audit
- Funzione HR
- Funzione IT (Comprensivo del Servizio CISO)
- Tutti i Direttori di Funzione ed i Responsabili di ufficio che effettuano il trattamento dei dati personali nell'ambito della propria Direzione in qualità di delegati di funzione per conto del Titolare.
- Gli autorizzati al trattamento, ovvero i soggetti ai quali è attribuito il compito del trattamento dei dati conformemente alle disposizioni ricevute dal Titolare o dal Responsabile.
- Data Protection Officer (DPO), i cui compiti sono espressamente previsti dagli articoli 39 e ss. del GDPR e riportati nel documento: Linee di indirizzo per il Sistema di Controllo Interno, reperibile presso il sito www.esprinet.com
- **Responsabile del SGSI:** figura incaricata di coordinare l'attuazione, il mantenimento e il miglioramento continuo del Sistema di Gestione per la Sicurezza delle Informazioni, monitorandone l'efficacia e riferendo all'Alta Direzione sul suo andamento e sulle esigenze di aggiornamento.
- **Punto di contatto NIS2 :** ai fini di questo processo è la figura che, conformemente al ruolo definito dal decreto NIS, ha il compito di curare l'attuazione delle disposizioni del decreto NIS per conto del soggetto stesso, a partire dalla registrazione, e interloquisce, per conto del soggetto NIS, con l'Autorità nazionale competente NIS. Il punto di contatto NIS per il Gruppo Esprinet è svolto dal CIO.
- **Referente CSIRT:** ai fini di questo processo è la figura che, conformemente al ruolo definito dalla Determinazione ACN 33017/2025, ha il compito di interloquire con lo CSIRT Italia, di cui all'articolo 2, comma 1, lettera i) del decreto NIS, ed effettuare le notifiche di cui agli articoli 25 e 26 del medesimo decreto per conto del soggetto NIS. Il referente CSIRT per il Gruppo Esprinet è il Cybersecurity Supervisor

Nello svolgimento delle attività sopraindicate possono, inoltre, essere coinvolte, a vario titolo, Funzioni aziendali di altre Società di Esprinet.

6. DEFINIZIONI

- **Accountability:** L'assegnazione della responsabilità di un'attività o processo aziendale, con il conseguente compito di rispondere delle operazioni svolte e dei risultati conseguiti, a una determinata figura aziendale; in ambito tecnico, si intende la garanzia di poter attribuire ciascuna operazione a soggetti (utenti o applicazioni) univocamente identificabili;
- **Asset:** dati, personale, dispositivi, sistemi e strutture che consentono all'organizzazione di raggiungere gli scopi aziendali.
- **Autenticazione:** fornisce la garanzia che una caratteristica dichiarata di un'entità è corretta.

Information & Cyber Security PolicyRevisione: **01 del 22/10/2026****PAG. 7 DI 18**

- **Autorizzazione:** La procedura che verifica se un cliente o un altro soggetto interno o esterno ha il diritto di compiere una certa azione, ad es. di trasferire fondi o accedere a dati sensibili.
- **Best practice:** Raccolta organizzata di raccomandazioni derivanti dalla selezione delle pratiche migliori per l'erogazione dei servizi.
- **CISO:** il Chief Information Security Officer è il servizio di coordinamento di tutte le attività legate alla sicurezza delle informazioni.
- **Information & Cyber Security:** l'Information & Cyber Security garantisce la protezione delle informazioni archiviate, elaborate e trasmesse, in tutte le forme, preservando le seguenti caratteristiche:
- **Riservatezza:** garantire che le informazioni siano disponibili solo per gli utenti autorizzati
- **Integrità:** garantire che le informazioni siano protette da modifiche non autorizzate per garantirne l'affidabilità e la correttezza
- **Disponibilità:** garantire che le informazioni siano disponibili quando e dove sono necessarie
- **Informazione:** conoscenza o insieme di dati che hanno valore per un individuo o un'organizzazione. (ISO/IEC 27000).

Possono esistere in molte forme:

- Stampate o scritte su supporto cartaceo
- Memorizzate elettronicamente
- Trasmesse via posta o mezzi elettronici
- Registrate su video
- Trasmesse verbalmente.
- **Minacce alla sicurezza:** potenziale causa di un incidente indesiderato, che potrebbe danneggiare un sistema o un'organizzazione.
- **Minimo privilegio (Least Privilege):** il principio che stabilisce che a ciascun utente o amministratore di sistema siano assegnate le abilitazioni strettamente necessarie allo svolgimento dei compiti assegnati.
- **Misure di sicurezza:** salvaguardie o contromisure prescritte per un sistema informativo o un'organizzazione per proteggere la riservatezza, l'integrità e la disponibilità del sistema e delle sue informazioni.
- **Modifiche al sistema informativo:** l'aggiunta, la modifica o la rimozione di qualsiasi cosa che possa influenzare il sistema informativo.
- **Outsourcing:** Affidamento a società esterne della gestione di funzioni/servizi. Può riguardare i sistemi informatici (gestione sistemi elaborativi e reti, help desk, fornitura apparati), le infrastrutture (manutenzione impianti, sorveglianza), la formazione, ecc.
- **Rischio informatico:** Il rischio di incorrere in perdite economiche, di reputazione e di quote di mercato, in relazione all'utilizzo di tecnologia dell'informazione e della comunicazione (Information and Communication Technology – ICT).

- **Rischio informatico residuo:** Il rischio informatico a cui il Gruppo è esposto, una volta applicate le misure di attenuazione individuate nel processo di analisi dei rischi.
- **Risorse ICT:** tutte le risorse ICT e fattori abilitanti che supportano il sistema informativo, ad esempio sistemi informatici, di rete, di comunicazione, applicativi e di telecomunicazione, infrastruttura, hardware, software, dati, database, personale, procedure, strutture fisiche, fornitori basati su cloud, fornitori di Software as a Service (SaaS) e qualsiasi materiale e servizio correlato.
- **Security & Privacy by Design:** i principi di privacy e sicurezza sono integrati nelle attività di elaborazione e nelle pratiche commerciali, dalla fase di progettazione fino all'intero ciclo di vita (ex art. 25 GDPR).
- **Segregazione dei compiti (Segregation of Duties):** il principio che stabilisce che l'esecuzione di operazioni di particolare criticità sia svolta attraverso la cooperazione di più utenti o amministratori di sistema con responsabilità formalmente ripartite;
- **Sistema di IA:** un sistema automatizzato progettato per funzionare con livelli di autonomia variabili e che può presentare adattabilità dopo la diffusione e che, per obiettivi espliciti o impliciti, deduce dall'input che riceve come generare output quali previsioni, contenuti, raccomandazioni o decisioni che possono influenzare ambienti fisici o virtuali.
- **Sistema di Gestione della Sicurezza delle Informazioni (SGSI):** il complesso di sistemi di processo, documenti, tecnologie e persone che aiutano un'azienda a gestire, monitorare, controllare e migliorare la Sicurezza delle Informazioni.
- **Sistema informativo:** insieme di applicazioni, servizi, risorse di tecnologia dell'informazione o altri componenti per la gestione delle informazioni.
- **Strong Authentication:** autenticazione a più fattori, nella quale si combinano più elementi di autenticazione per rendere più complessa la compromissione del sistema.
- **Vulnerabilità:** una condizione che consente il verificarsi di una minaccia.

7. PRINCIPI GENERALI RELATIVI ALLA SICUREZZA DELLE INFORMAZIONI

Esprinet ha definito i seguenti principi generali di sicurezza da adottare nell'ambito di tutti i processi e delle attività svolte dal personale interno ed esterno, ispirandosi allo Standard ISO 27001. Essi costituiscono un quadro di riferimento per ottenere un adeguato livello di protezione del patrimonio informativo aziendale, mediante il continuo miglioramento dei processi organizzativi e la ricerca di soluzioni tecnologiche innovative in relazione alle evoluzioni della tecnologia, delle minacce e degli strumenti di difesa.

7.1. USO SICURO DEGLI STRUMENTI INFORMATICI

La riservatezza delle informazioni deve essere rispettata anche attraverso la scrupolosa osservanza delle disposizioni contenute nelle Politiche aziendali di Esprinet e nel Codice Etico che il Gruppo adotta per una corretta gestione degli strumenti elettronici dati in dotazione al Personale, delle banche dati organizzate da Esprinet e per tutti gli ulteriori specifici adempimenti connessi.

La diffusione di nuove tecnologie informatiche espone Esprinet e gli utenti a rischi di natura patrimoniale, oltre alle responsabilità penali conseguenti alla violazione di specifiche disposizioni di leggi, creando problemi alla sicurezza e all'immagine dell'azienda stessa. Pertanto, l'utilizzo di risorse informatiche digitali (device e software) deve ispirarsi ai principi di correttezza e diligenza. Gli strumenti informatici, in particolare, devono essere custoditi con cura, evitando ogni possibile forma di danneggiamento. [Per ulteriori dettagli, fare riferimento alle politiche aziendali relative all'utilizzo degli strumenti informatici rese disponibili all'occorrenza alla parti interessati e quelle relative alla Sicurezza delle Informazioni.](#)

7.2. SECURITY E PRIVACY BY DESIGN

Il processo di sviluppo deve considerare i requisiti relativi alla sicurezza informatica e alla protezione dei dati personali sin dalla fase iniziale di progettazione.

Un'importante, ma non esclusiva, applicazione di tale principio risiede nella pianificazione e nell'adozione di appropriate misure e soluzioni volte ad evitare o limitare potenziali danni da minacce e vulnerabilità identificate. Le misure di sicurezza e le soluzioni tecniche devono essere individuate ed implementate in funzione del valore delle informazioni e, quindi, dei rischi di sicurezza e privacy, cui sono esposti gli asset IT delle Società del Gruppo.

7.3. NEED TO KNOW

Il Gruppo definisce le logiche di accesso ai dati e alle informazioni, caratterizzanti il patrimonio informativo, nel rispetto del principio del "privilegio minimo", ovvero in relazione alla loro criticità intrinseca e in funzione della pertinenza del ruolo ricoperto dal richiedente.

7.4. SISTEMI DI INTELLIGENZA ARTIFICIALE

Nell'ambito dell'adozione di Sistemi di intelligenza artificiale il Gruppo si impegna affinché sia garantito l'uso responsabile e conforme alla normativa dell'IA, massimizzandone i benefici e proteggendo al contempo i diritti e la privacy di tutti i dipendenti delle Società del Gruppo e le informazioni riservate dell'organizzazione, dei clienti, dei fornitori e di ogni altro soggetto interessato.

[A tal proposito Esprinet si è dotata di apposite linee guida in materia di utilizzo dell'AI, istituendo anche un Team di lavoro dedicato.](#)

7.5. SEPARAZIONE DEI RUOLI

Le Società del Gruppo implementano apposite misure organizzative, procedurali e tecniche affinché le responsabilità siano definite e debitamente distribuite evitando sovrapposizioni funzionali o allocazioni operative che concentrino le attività critiche su un unico soggetto (persona fisica o giuridica, unità organizzativa, ruolo o funzione aziendale).

8. FRAMEWORK DI GESTIONE DELLA SICUREZZA DELLE INFORMAZIONI

Le Società del Gruppo definiscono le misure di sicurezza da realizzare a tutela degli asset IT caratterizzanti il proprio patrimonio informativo, tramite l'emanazione di politiche, procedure e linee guida in materia di

Sicurezza delle Informazioni. L'insieme di tutta la documentazione in ambito, sviluppata in coerenza con le regole del Sistema Normativo Interno, costituisce il Framework documentale di gestione della Sicurezza delle Informazioni del Gruppo.

Nei paragrafi che seguono viene fornita una descrizione sintetica dei principali ambiti caratterizzanti il framework di sicurezza delle Società del Gruppo, definiti in ottemperanza ai principi di sicurezza di cui al capitolo precedente.

8.1. STRATEGIE DI SICUREZZA

La strategia per la Sicurezza delle Informazioni del Gruppo si articola nei seguenti punti:

- raggiungimento degli obiettivi di sicurezza in tutti gli ambiti tramite misure ed interventi omogenei e coerenti;
- utilizzo delle valutazioni sul rischio informatico per stabilire l'intensità e l'efficacia dei controlli di sicurezza;
- attribuzione di priorità ai controlli di sicurezza che hanno come scopo la prevenzione delle minacce, rispetto a quelli con finalità di mitigazione degli impatti derivanti dagli incidenti;
- distribuzione delle misure di sicurezza su diversi livelli, così che un'eventuale falla in una linea di difesa sia coperta dalla successiva ("difesa in profondità");
- garanzia che l'implementazione di ogni controllo di sicurezza includa le modalità ed i meccanismi adeguati a verificarne l'efficacia e la corretta attuazione nel tempo.

8.2. CLASSIFICAZIONE E GESTIONE DEGLI ASSET IT

Tutte le risorse materiali e immateriali caratterizzanti il patrimonio informativo delle Società del Gruppo hanno un valore strategico e, pertanto, devono essere adeguatamente protette.

La messa in sicurezza del patrimonio informativo ha inizio con l'identificazione degli asset IT e delle informazioni che lo caratterizzano, le quali devono essere classificate secondo metriche coerenti con le politiche di classificazione delle informazioni definite delle Società del Gruppo e che ne evidenzino le criticità in termini di sicurezza per facilitare la corretta implementazione di misure di protezione adeguate.

Le principali attività da eseguire per una corretta gestione degli asset IT aziendali sono le seguenti:

- **Asset Inventory:** Costituire e mantenere aggiornato, nel corso del tempo, un inventario degli asset IT al fine di assegnare la responsabilità di tutela degli stessi e monitorarli per l'intero ciclo di vita. Affinché sia garantito un corretto livello di protezione dei dati e delle informazioni.
- **Classificazione degli asset:** L'organizzazione, con il supporto della funzione IT, deve definire una metodologia per la classificazione degli asset sulla base dei criteri di confidenzialità, integrità e disponibilità, al fine di identificare con gli owner delle informazioni il livello di criticità in termini di

sicurezza e definire adeguate misure di protezione. Tale classificazione deve essere realizzata in coerenza con la policy di classificazione delle informazioni definita dal Gruppo e deve essere periodicamente aggiornata.

8.3. GESTIONE DEL RISCHIO INFORMATICO

Il Processo di Gestione del Rischio Informatico (indicato in seguito anche come “Rischio IT”) rappresenta lo strumento mediante il quale il Gruppo assicura l'efficacia delle misure di sicurezza poste a protezione del sistema informativo. Tale processo consente inoltre la gradazione delle misure di mitigazione in funzione del profilo di rischio dell'asset IT definito dalle funzioni preposte.

Il Processo di Gestione del Rischio interessa:

- tutte le iniziative di sviluppo di nuovi progetti e di modifica rilevante del sistema informativo (Security by Design);
- le procedure in esercizio, per le quali non è stata svolta un'analisi del rischio in fase di sviluppo (ovvero realizzate antecedentemente all'entrata in vigore della presente Policy).

Esso viene eseguito con una periodicità adeguata alla tipologia degli asset IT, in presenza di situazioni che possono influenzare il complessivo livello di esposizione al rischio informatico del sistema informativo.

Tra le situazioni che possono richiedere una esecuzione straordinaria dell'analisi del rischio si evidenziano:

- il verificarsi di gravi incidenti di sicurezza informatica;
- la rilevazione di carenze nei controlli di sicurezza (vedi vulnerabilità di sicurezza gravi);
- la diffusione di notizie su nuove vulnerabilità o minacce di sicurezza informatica.

Il processo è svolto con il concorso delle funzioni aziendali responsabili dei processi di business che gli asset IT supportano, della funzione di Risk Management e della funzione IT attraverso il servizio di Sicurezza Informatica.

I risultati del processo (livelli di classificazione, rischi potenziali e residui, lista delle minacce considerate, elenco dei presidi individuati), ogni loro aggiornamento successivo, le assunzioni operate e le decisioni assunte, sono documentati e sottoposti all'approvazione dell'Alta Direzione.

8.4. FORMAZIONE E AWARENESS (PERSONALE E SICUREZZA)

Il personale, sia esso dipendente che di terze parti, rappresenta un elemento cruciale nel processo di gestione della sicurezza del sistema informativo delle Società del Gruppo.

Il Gruppo promuove con cadenza periodica e per tutti i dipendenti, adeguati programmi di formazione al fine di assicurare il rispetto del Framework di sicurezza e il rispetto dei ruoli e delle responsabilità ad essi assegnati.

In particolare, devono essere fornite a tutto il personale delle norme comportamentali sull'utilizzo dei dispositivi aziendali (es. postazioni di lavoro, dispositivi mobili, telefoni, stampanti) e sui servizi di comunicazione aziendali (es. posta elettronica, navigazione Internet, social media) al fine di garantire la Sicurezza delle Informazioni aziendali ed evitare eventuali violazioni della loro riservatezza.

Per i soggetti incaricati a svolgere funzioni ritenute critiche, deve essere attuata una formazione mirata sulle tematiche inerenti la sicurezza informatica.

Infine, il Gruppo deve realizzare programmi di sensibilizzazione sulla sicurezza, al fine di accrescere il grado di consapevolezza (awareness) dei dipendenti sui rischi relativi alla sicurezza e incentivare la segnalazione di attività insolite o eventuali incidenti.

Tali programmi di Security Awareness devono prevedere iniziative diverse che mirano a raggiungere tutti i dipendenti delle Società del Gruppo e adottare delle tecniche di misurazione (es. spear phishing) in grado di valutare il livello di consapevolezza sulla sicurezza raggiunto dal personale.

8.5. GESTIONE DELLE SECURITY OPERATIONS

Di seguito, è riportato un elenco dei principali processi e dei requisiti di sicurezza caratterizzanti la loro sicura e corretta gestione:

- **Gestione dei Cambiamenti:** è necessario tenere in considerazione tutti gli aspetti di sicurezza nell'ambito della gestione dei cambiamenti degli asset IT. In particolare, si richiede di valutare gli impatti e i rischi connessi alle richieste di cambiamento inerenti la modifica o lo sviluppo degli asset IT, identificando gli opportuni requisiti di sicurezza da adottare (Security by Design), oltre che di svolgere opportune verifiche di sicurezza prima del rilascio in produzione dei suddetti cambiamenti;
- **Sviluppo Sicuro del software:** è necessario adottare metodologie e tecniche per lo sviluppo sicuro del software che consentano di prevenire eventuali problematiche di sicurezza nel software e, nel contempo, costituiscano uno strumento utile per individuare possibili vulnerabilità presenti nel codice sorgente e le relative contromisure da applicare;
- **Capacity management:** deve essere predisposto un monitoraggio continuativo delle prestazioni e dei principali parametri degli asset IT, volto a minimizzare la perdita di dati ed informazioni dovuti a loro malfunzionamenti/interruzioni;
- **Protezione da Malware:** devono essere in uso appositi applicativi (Antivirus) finalizzati a proteggere gli asset IT aziendali. Tale protezione deve essere rafforzata dalla corretta attuazione di comportamenti adeguati da parte degli utilizzatori degli asset IT in base a specifiche disposizioni interne.
- **Patch Management:** deve essere garantito l'aggiornamento continuo degli asset IT, hardware e software, delle Società del Gruppo al fine di prevenire e correggere eventuali malfunzionamenti e di eliminare eventuali vulnerabilità di sicurezza presenti.

- **Backup:** specifiche Politiche di backup devono essere definite a livello aziendale in funzione della criticità dei dati elaborati dagli asset IT, al fine di garantire gli aspetti di disponibilità dei dati e delle informazioni delle Società del Gruppo mediante una serie di misure di salvataggio e ripristino periodico degli stessi;
- **Network security:** deve essere garantita la protezione perimetrale dei dati e delle informazioni da accessi esterni ed interni non autorizzati, mediante la definizione di opportune misure di sicurezza perimetrale (firewall, IDS, etc.) della rete aziendale. Tali misure di protezione dovranno essere periodicamente testate al fine di verificarne il corretto funzionamento ed il loro mantenimento nel tempo.

In particolare:

- l'accesso agli apparati di rete (firewall, router, ecc.) deve essere consentito solo al personale tecnico competente ed autorizzato per le necessarie attività di gestione ed amministrazione.
 - deve essere prevista la segmentazione delle reti di telecomunicazione, con controllo dei flussi scambiati;
 - devono essere previsti adeguati meccanismi per la protezione della riservatezza delle informazioni in transito sulla rete aziendale (fissa e wireless) e attraverso reti pubbliche oppure di terze parti, basati su algoritmi e protocolli sicuri (p.e. cifratura delle comunicazioni).
- **Monitoring:** devono essere predisposte adeguate misure di monitoraggio degli asset IT (produzione di log), nel rispetto delle normative sulla privacy ed il trattamento dei dati, mediante il tracciamento degli accessi e delle attività effettuate dagli utenti e di tutti gli eventi considerati significativi per il monitoraggio della sicurezza degli asset IT (es. Access log, Activity log, System log, Security log).

In aggiunta:

- Tutte le attività di IT Operations devono essere supportate da un appropriato livello di documentazione, al fine di garantire un corretto livello di competenza richiesto;
- Le responsabilità delle attività di IT Operations devono essere allocate nel rispetto dei principi del need-to-know e di separazione dei ruoli al fine di limitare il rischio di azioni non autorizzate sui dati e sugli asset IT;
- Gli ambienti di produzione e test/sviluppo devono essere separati logicamente e/o fisicamente, al fine di garantire un maggior livello di protezione per i dati e le informazioni da essi gestiti.

8.6. ASPETTI DI SICUREZZA CORRELATI AGLI ACCESSI LOGICI

L'accesso alle informazioni e agli asset IT deve essere adeguatamente gestito al fine di garantirne il rispetto della confidenzialità e dell'integrità delle informazioni da essi gestite.

La gestione sicura degli accessi logici agli asset IT componenti il sistema informativo aziendale deve essere basata sulle seguenti regole:

- deve essere formalizzato un processo di approvazione e gestione delle autorizzazioni all'accesso;
- i profili di accesso devono essere definiti in modo da permettere all'utente di accedere alle informazioni strettamente necessarie per lo svolgimento dei compiti assegnati, nel rispetto del principio del "need to know" e del privilegio minimo;
- la gestione e il controllo deve riguardare l'intero ciclo di vita dei profili di accesso degli utenti (assegnazione, creazione, aggiornamento, disattivazione e revoca);
- deve essere verificato, in modo strutturato e scadenziato, la validità delle credenziali di accesso e dei profili di accesso conformemente alle norme vigenti e in relazione al ruolo aziendale assegnato all'utente;
- devono essere definiti meccanismi di protezione adeguati all'autenticazione del personale nel caso di accesso da remoto alla rete aziendale;
- devono essere implementati dei meccanismi di controllo e tracciatura degli accessi conformemente alle norme vigenti e alle politiche aziendali.

8.7. GESTIONE DEGLI STRUMENTI CRITTOGRAFICI

I controlli crittografici sono una delle principali misure di sicurezza utilizzate per la protezione dei dati, sia "a riposo" che in transito.

Gli strumenti crittografici possono essere utilizzati per raggiungere diversi obiettivi di sicurezza quali:

- protezione della riservatezza dei dati;
- garanzia della integrità/autenticità/non ripudio delle informazioni (es. servizi di firma elettronica, sistemi di hash);
- implementazioni di sistemi di autenticazione forte (es. Certificati Digitali, [MFA](#)).

Per tale ragione, il Gruppo deve predisporre una policy che normi l'utilizzo di tali strumenti e che copra almeno i seguenti aspetti principali:

- identificazione del controllo crittografico da applicare sulla base del livello di protezione richiesto dalle informazioni e considerando la tipologia, la robustezza e la qualità dell'algoritmo di crittografia del controllo;
- applicazione del controllo crittografico nei vari ambiti in cui la informazione da proteggere risiede o è in transito;
- la gestione delle chiavi, compresi i metodi per la protezione delle chiavi crittografiche e per il ripristino di informazioni cifrate in caso di perdita, compromissione o danneggiamento delle chiavi;
- ruoli e responsabilità in ambito gestione chiavi crittografiche.

8.8. GESTIONE DELLE VULNERABILITÀ

Le Società del Gruppo devono garantire che le eventuali vulnerabilità tecniche presenti sugli asset IT devono essere opportunamente monitorate e gestite, mediante l'attuazione delle seguenti regole:

- attribuzione della specifica responsabilità di gestione e mantenimento degli asset IT in merito agli aspetti di vulnerabilità di sistema (patch management di sicurezza, hardening, ecc.);
- monitoraggio delle informazioni tecniche che periodicamente sono emesse dai soggetti preposti (vendor, centri istituzionali di sicurezza, ecc.);
- garanzia che le vulnerabilità tecniche rilevate siano analizzate e gestite, previa una loro valutazione e successiva adozione dei necessari interventi correttivi (es. opportune attività di patching);
- esecuzione di periodiche verifiche di sicurezza sugli asset IT gestiti (es. Vulnerability Assessment, Penetration Test, Security Audit) attraverso la predisposizione di un piano di verifica periodico che tenga conto della criticità degli asset IT, nonché di eventi occorsi nel periodo di riferimento (es. cambiamenti delle piattaforme tecnologiche, change rilevanti, incidenti gravi).

8.9. SICUREZZA DEI DISPOSITIVI AZIENDALI

Le Società del Gruppo devono garantire l'adozione di adeguate misure di sicurezza per prevenire problemi di protezione causati dall'errata configurazione, gestione ed utilizzo delle postazioni di lavoro e dei dispositivi mobili quali PC portatili, smartphone, tablet.

Al fine di garantire il raggiungimento di tali obiettivi, è necessario che siano definite e rispettate delle norme comportamentali per l'utilizzo dei dispositivi aziendali assegnati (vedi par. 7.1), nonché misure di sicurezza specifiche con particolare attenzione verso i dispositivi mobili (es. remote lock, remote wipe).

8.10. GESTIONE DEGLI INCIDENTI INERENTI LA SICUREZZA DELLE INFORMAZIONI

La gestione degli incidenti di sicurezza informatica ha l'obiettivo di minimizzare l'impatto di eventi avversi e di garantire il tempestivo ripristino del regolare funzionamento degli asset IT coinvolti.

Pertanto, le Società del Gruppo adottano un processo di gestione degli incidenti di sicurezza, conforme alle normative vigenti (es. GDPR) ed alle best practice di settore, volto alla mitigazione ed al contrasto tempestivo degli eventi di sicurezza informatica impattanti il sistema informativo.

Inoltre, il processo prevede l'innescio di procedure di escalation alle strutture preposte della Società di riferimento ed alle Autorità competenti, laddove si verificano gravi incidenti, con particolare riferimento ai data breach di dati personali (GDPR).

8.11. GESTIONE DEGLI ASPETTI DI BUSINESS CONTINUITY

Il Gruppo deve garantire adeguati livelli di continuità operativa, a fronte di un eventuale evento impreveduto, di qualsiasi natura, che possa comportare blocchi nell'erogazione dei servizi.

Pertanto, al fine di salvaguardare gli interessi dei suoi stakeholders, il Gruppo adotta un processo strutturato per la gestione della Business Continuity, in grado di garantire il ripristino tempestivo delle funzionalità dei servizi e di mitigare i principali rischi operativi ad essi connessi.

Il processo, in particolare, deve prevedere:

- l'elaborazione di piani di continuità operativa basati sulle reali esigenze del business aziendale nonché sull'adeguata analisi degli impatti relativi al fermo dei principali processi delle Società del Gruppo;
- la definizione e svolgimento di esercitazioni periodiche che permettano di convalidare il funzionamento delle soluzioni di Business Continuity identificate;
- la revisione periodica e l'aggiornamento tempestivo dei piani di continuità operativa in funzione delle nuove minacce alla continuità dei servizi delle Società del Gruppo;
- la richiesta di garanzie in termini di Business Continuity, all'inizio di ogni progetto e in ciascun contratto, ai "fornitori di servizi considerati critici", al fine di favorire la prevenzione sui rischi dovuti ad attività esternalizzate.

8.12. GESTIONE DELLA SICUREZZA FISICA

La protezione del patrimonio informativo del Gruppo richiede che venga posta particolare attenzione agli aspetti di sicurezza fisica, al fine di prevenire l'accesso non autorizzato ai locali aziendali ed un eventuale rischio di sottrazione, manomissione e/o danneggiamento degli asset.

Al fine di garantire la sicurezza fisica, le Società del Gruppo devono individuare adeguate misure tecniche, organizzative e procedurali da adottare relativamente alla:

- gestione delle aree fisiche (intese come sedi, aree e locali): adottare adeguate misure di sicurezza e di protezione in funzione della criticità delle risorse informative trattate e conservate;
- gestione sicura degli asset: posizionare e proteggere gli asset in funzione del livello di criticità delle informazioni;
- gestione degli accessi: garantire che l'accesso ai locali sia controllato e consentito esclusivamente al personale previamente identificato ed autorizzato.

8.13. GESTIONE DELLE TERZE PARTI

La gestione della sicurezza del sistema informativo richiede che sia garantito un adeguato livello di sicurezza delle risorse accedute e utilizzate da soggetti terzi (fornitori, consulenti, partner). Il loro accesso ai sistemi interni ed alle informazioni in essi contenute può infatti esporre le Società del Gruppo a dei rischi accidentali e/o intenzionali di distruzione, perdita, divulgazione, alterazione e accesso non autorizzato delle risorse informative.

In tale ottica, le Società del Gruppo si impegnano a:

- identificare i rischi connessi all'attività di outsourcing e a definire adeguate misure di sicurezza (Rischio delle Terze Parti);
- prevedere l'inserimento di opportuni impegni/obblighi a carico delle terze parti all'interno dei contratti di fornitura del servizio.

Il contratto stipulato con le terze parti deve prevedere che queste forniscano specifiche garanzie relative alla sicurezza informatica e report al verificarsi di eventi significativi che possano avere un impatto sulla stessa.

In generale, i principi di sicurezza definiti per il Gruppo devono essere applicati anche nei confronti dei soggetti esterni.

8.14. CONFORMITÀ

La presente Politica deve essere implementata dal Gruppo Esprinet in accordo con le normative applicabili, il quale non intende, infatti, omettere o porsi in contrasto con leggi, norme nazionali e internazionali applicabili, nonché regolamenti definiti specificatamente per l'ambito in cui esso opera.

8.15. PROTEZIONE DEI DATI PERSONALI

Il Regolamento Generale per la Protezione dei dati Personali (EU) 679/2016 (GDPR) è, dal 25 Maggio 2018, il principale testo normativo di riferimento sulla protezione dei dati personali nell'Unione Europea e rafforza le attuali disposizioni normative (sia nella sostanza che nel contesto), estendendo gli obblighi in materia di sicurezza direttamente anche ai Responsabili del trattamento.

Uno dei principali obblighi per tutte le imprese, e quindi per le Società del Gruppo Esprinet, sia che agiscano come Titolare, sia come Responsabile del trattamento, è finalizzato alla sicurezza delle operazioni di trattamento dei dati personali.

La sicurezza nel trattamento dei dati personali, disciplinata in via primaria dall'articolo 32 del GDPR, afferma che il Titolare del trattamento e il Responsabile del trattamento debbano mettere in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza proporzionato ai rischi connessi ai diritti e alle libertà delle persone fisiche, verificando nel continuo l'efficacia delle misure tecniche e organizzative, al fine di garantire la sicurezza del trattamento.

In linea con quanto stabilito dal GDPR, il Gruppo Esprinet ha come obiettivo primario la sicurezza dei dati personali gestiti, con particolare attenzione alla riservatezza, integrità e disponibilità dei dati attraverso un approccio basato sui rischi (risk-based approach) connessi ai diritti e la libertà degli interessati. Per tale ragione, il Gruppo adotta un approccio per la protezione dei dati personali che prevede la piena conformità agli adempimenti e ai principi del GDPR in ogni specifico contesto operativo e in ogni processo aziendale dove i dati personali sono trattati.

9. PROVVEDIMENTI DISCIPLINARI

Qualsiasi violazione della presente Politica, o di altre Politiche pertinenti, deve essere tempestivamente e adeguatamente segnalata a ciso@esprinet.com.

La violazione delle regole contenute in questo documento potrà comportare l'adozione di provvedimenti disciplinari secondo quanto previsto dal vigente contratto collettivo nazionale applicato dalle diverse Società del Gruppo e in relazione alla portata e alla gravità dell'infrazione commessa.

La violazione delle regole di questo documento può essere qualificata come inadempimento agli obblighi contrattuali in capo al lavoratore Dipendente. In caso di effettiva violazione degli obblighi contrattuali in capo al Dipendente, la Società del Gruppo Esprinet coinvolta chiede al lavoratore di cessare immediatamente le sue azioni e ha facoltà di intraprendere le dovute azioni disciplinari e le altre misure in conformità alle disposizioni dei regolamenti interni dell'entità, nonché alla normativa vigente.

Allo stesso modo è vietato da parte dei Dipendenti duplicare file e dati aziendali su supporto informatico in vista dell'interruzione del rapporto di lavoro con le Società del Gruppo Esprinet.

10. ARCHIVIO

La copia in originale cartacea della presente linea guida è archiviata presso l'ufficio Internal Audit, con l'evidenza delle firme di redazione, controllo ed approvazione. Una copia è archiviata all'interno del sistema documentale aziendale.