FEDRIGONI

Politica per la Sicurezza delle Informazioni

Ver.	Data	Descrizione Aggiornamento	Autore
1.0	15.10.2021	Prima versione	Group IT Security Manager

Emesso da	Verificato da	Approvato da
Group IT Security Manager	Group Chief Information Officer, Group Compliance Officer & Chief Internal Auditor	Group Board of Directors

FEDRIGONI
Group

Sede legale
Via Enrico Fermi 13/f
37135 Verona (VR), Italy
T +39 045 8087888
F +39 045 8009015

Sede operativa
Piazzale Lodi 3
20137 Milano, Italy
T +39 02 467101

fedrigoni.com

FEDRIGONI

Indice

1. Overview della Politica ... 3
   1.1. Introduzione ... 3
   1.2. Obiettivo ... 3
   1.3. Riferimenti ... 4
   1.4. Termini e definizioni ... 4
2. Politiche per la sicurezza delle informazioni ... 5
   2.1. Controlli organizzativi ... 6
      2.1.1. Ruoli e Responsabilità nella sicurezza delle informazioni ... 6
      2.1.2. Group Information Security Committee ... 7
      2.1.3. Gestione degli asset ... 8
      2.1.4. Classificazione delle informazioni ... 9
      2.1.5. Controllo degli accessi ... 9
      2.1.6. Sicurezza delle informazioni nelle terze parti ... 9
      2.1.7. Compliance ... 10
   2.2. Controlli sul personale ... 10
      2.2.1. Sicurezza delle Risorse Umane ... 10
   2.3. Controlli fisici ... 11
      2.3.1. Sicurezza fisica ... 11
      2.3.2. Sicurezza ambientale ... 11
   2.4. Controlli tecnologici ... 11
      2.4.1. Sicurezza delle operazioni ... 11
      2.4.2. Sicurezza delle comunicazioni ... 12
      2.4.3. Acquisizione, sviluppo, mantenimento e dismissione dei sistemi informativi ... 12
      2.4.4. Gestione degli incidenti relativi alla sicurezza delle informazioni ... 12
      2.4.5. Gestione della Business Continuity e Disaster Recovery ... 13
3. Eccezioni ... 13
4. Adeguamenti ... 13

1. Overview della Politica

1.1. Introduzione

Le informazioni sono risorse che, al pari degli altri elementi aziendali, sono essenziali per l'attività delle organizzazioni e di conseguenza devono essere adeguatamente protette. Tale aspetto risulta di particolare importanza specialmente per la crescente interconnessione degli ambienti aziendali. Il risultato di questa crescente interconnessione è che le informazioni sono ora esposte ad un crescente numero e una più ampia varietà di minacce e vulnerabilità.
La presente Politica indirizza la gestione della sicurezza delle informazioni all'interno del Gruppo Fedrigoni per assicurare adeguati livelli di sicurezza per le informazioni conservate e trasmesse attraverso tecnologie informatiche (dati personali, dati finanziari, ecc.), tenendo in considerazione i requisiti legali e un'efficace gestione del rischio.
La Politica è strutturata in quattro capitoli:

- Il presente capitolo ("Overview della Politica") definisce obiettivo, riferimenti interni ed esterni applicabili, termini e definizioni;
- Il Capitolo 2 ("Politica di Sicurezza delle Informazioni") descrive gli ambiti di sicurezza delle informazioni da presidiare con opportune politiche di sicurezza;
- Il Capitolo 3 ("Eccezioni") esplicita le eccezioni a quanto definito nella presente Politica;
- Il Capitolo 4 ("Adeguamenti") delinea le modalità di aggiornamento della Politica di Sicurezza delle Informazioni.

1.2. Obiettivo

Lo scopo del presente documento è quello di fornire una descrizione delle politiche di sicurezza da adottare all'interno del Gruppo Fedrigoni per garantire un adeguato livello di protezione delle informazioni in termini di:

- Riservatezza, assicurando che le informazioni siano accessibili solo agli utenti autorizzati;
- Integrità, salvaguardando completezza, accuratezza e conformità delle informazioni durante le attività di acquisizione, conservazione, elaborazione e condivisione;
- Disponibilità, assicurando che agli utenti autorizzati siano disponibili le informazioni di cui hanno bisogno per svolgere le proprie attività.

Le politiche di sicurezza delle informazioni sono state definite in conformità agli standard internazionali (es. ISO/IEC 27001) e alle norme relative alle pratiche di gestione della sicurezza delle informazioni, agli aspetti di rischio che caratterizzano il Gruppo e ai relativi requisiti di business. La presente Politica si applica a tutte le Legal Entity del Gruppo Fedrigoni.

1.3. Riferimenti

Riferimenti esterni:

- Tecnologia dell'informazione - Tecniche di sicurezza - Sistemi di gestione della sicurezza delle informazioni [ISO/IEC 27001]
- Sicurezza delle informazioni, cyber security e protezione della privacy - Controlli di sicurezza delle informazioni [ISO/IEC 27002]
- Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati [Regolamento generale sulla protezione dei dati o GDPR]

1.4. Termini e definizioni

Per gli obiettivi di questo documento, di seguito sono riportati termini e definizioni.

Termini	Definizioni
Controllo degli accessi	Strumenti che permettono di impostare l'accesso fisico e logico agli asset aziendali in modo che sia autorizzato e limitato in base ai requisiti di business e di sicurezza
Asset	Qualsiasi bene che abbia valore per l'organizzazione
Attacco	Tentativo non autorizzato di distruggere, esporre, alterare o qualsiasi tentativo di disattivare, rubare, accedere o fare un uso non autorizzato di un bene aziendale
Autenticazione	Processo che assicura la verifica dell'identità di un utente o un'entità
Utente autorizzato	Soggetto che possiede una formale autorizzazione ad accedere alle informazioni
Business Unit	Parte di una Legal Entity che opera come un'entità separata dall'intera azienda
Controllo	Misura a presidio di uno specifico rischio
Disaster Recovery	L'insieme delle misure tecnologiche e organizzative progettate per ripristinare sistemi, dati e infrastrutture dopo il verificarsi di un evento che interrompe i processi aziendali
Informazioni	Insieme di dati correlati che hanno valore per l'organizzazione
Evento relativo alla sicurezza delle informazioni	Occorrenza che indica una possibile violazione della sicurezza delle informazioni o un fallimento delle misure adottate
Incidente relativo alla sicurezza delle informazioni	Uno o più eventi di sicurezza delle informazioni correlati e identificati che possono danneggiare le risorse dell'organizzazione o compromettere le sue operazioni

Termini	Definizioni
Gestione degli incidenti relativi alla sicurezza delle informazioni	Insieme delle attività per la gestione coerente ed efficace degli incidenti di sicurezza delle informazioni
Sistema Informativo	Insieme di applicazioni, servizi, risorse informatiche o altri componenti di gestione delle informazioni
Legal Entity	Organizzazione che possiede diritti e responsabilità legali
Dati Personali	Qualsiasi informazione che (a) può essere usata per stabilire un collegamento tra l'informazione e la persona fisica a cui tale informazione si riferisce, o (b) è o può essere direttamente o indirettamente collegata a una persona fisica
Politica	Intenzioni e direzione di un'organizzazione, come formalmente espressa dal suo top management
Procedura	Modo specifico di svolgere un'attività o un processo
Processo	Insieme di attività interconnesse o interagenti che trasformano gli input in output
Regola	Principio accettato o istruzione che dichiara le aspettative dell'organizzazione su cosa deve essere fatto, cosa è permesso o non permesso
Minaccia	Potenziale causa di un incidente che può provocare danni a un sistema o a un'organizzazione
Utente	Soggetto con accesso ai sistemi informativi dell'organizzazione

2. Politiche per la sicurezza delle informazioni

Il Gruppo Fedrigoni ha definito i domini di sicurezza da presidiare con apposite politiche di sicurezza informatica di Gruppo che tutte le Legal Entity devono implementare e seguire.
I domini di sicurezza delle informazioni sono suddivisi in quattro aree (Controlli organizzativi, Controlli sul personale, Controlli fisici e Controlli tecnologici) e sono descritti nei paragrafi seguenti.

- Controlli organizzativi
  - Ruoli e Responsabilità nella sicurezza delle informazioni
  - Gestione degli asset
  - Classificazione delle informazioni
  - Controllo degli accessi
  - Sicurezza delle informazioni nelle terze parti
  - Compliance
- Controlli sul personale
  - Sicurezza delle Risorse Umane
- Controlli fisici

- Sicurezza fisica
- Sicurezza ambientale

- Controlli tecnologici
  - Sicurezza delle operazioni
  - Sicurezza delle comunicazioni
  - Acquisizione, sviluppo, mantenimento e dismissione dei sistemi informativi
  - Gestione degli incidenti relativi alla sicurezza delle informazioni
  - Gestione della Business Continuity e Disaster Recovery.

2.1. Controlli organizzativi

2.1.1. Ruoli e Responsabilità nella sicurezza delle informazioni

A livello di Gruppo, i ruoli e le responsabilità riguardanti la sicurezza delle informazioni e la gestione dei rischi correlati sono i seguenti.

- Group IT Security Manager:
  - Gestisce il rischio di sicurezza delle informazioni durante l'intero ciclo di vita dei dati, per tutto il Gruppo Fedrigoni, assicurando l'esecuzione di valutazioni periodiche del rischio per identificare le priorità per la gestione dei rischi di sicurezza delle informazioni e per l'attuazione di controlli per ridurre tali rischi;
  - Informa sullo stato e sui rischi di cyber security, assumendo anche il ruolo di referente per la strategia globale e il budget necessario;
  - Gestisce/sovrintende il team che si occupa delle tematiche relative alla sicurezza delle informazioni;
  - Si coordina con il Compliance Office per identificare i requisiti normativi di Gruppo;
  - Stabilisce le politiche di sicurezza delle informazioni a livello di Gruppo (focus strategico, politiche di Gruppo e linee guida normative);
  - Mantiene aggiornate le procedure di sicurezza delle informazioni di Gruppo;
  - Supporta il team di Internal Audit nell'esecuzione degli audit di sicurezza delle informazioni;
  - Agisce come Demand nei confronti dei referenti di Business per definire/valutare i requisiti di sicurezza delle informazioni in caso di nuove implementazioni o di revisione di quelle esistenti;
  - Assicura, attraverso valutazioni periodiche, l'efficacia delle misure di sicurezza delle informazioni al fine di proteggere il patrimonio aziendale e garantire il rispetto delle norme relative alle pratiche di gestione della sicurezza delle informazioni e dei requisiti aziendali;
  - Esegue attività di controllo della sicurezza delle informazioni sulla catena di fornitura e su altre terze parti rilevanti;
  - Supporta le attività di controllo della sicurezza delle informazioni richieste da terze parti;
  - Gestisce la progettazione di soluzioni appropriate per la sicurezza delle informazioni;

- Gestisce le attività di rilevamento e risposta agli incidenti di sicurezza delle informazioni.

- Group Head of IT Infrastructure, Group Head of Business Intelligence & Digital IT, IT Director BU Self-Adhesives, IT Director BU Paper:
  - Allinea le tecnologie dell'informazione alla strategia di sicurezza dell'informazione del Gruppo;
  - Implementa le soluzioni di sicurezza delle informazioni progettate dal Group IT Security Manager;
  - Fornisce supporto nella attività di valutazione periodica in ambito sicurezza delle informazioni;
  - Implementa le iniziative di rimedio identificate a valle delle attività di valutazione periodica in ambito sicurezza delle informazioni;
  - Fornisce supporto nelle attività di rilevamento e risposta agli incidenti di sicurezza delle informazioni;
  - Gestisce le attività di recupero degli incidenti di sicurezza delle informazioni;
  - Esegue le attività tecniche per mantenere aggiornate le risorse tecniche IT.

- Group Compliance Officer & Chief Internal Auditor:
  - Assicura il necessario supporto interpretativo, per gli ambiti di competenza, sugli aspetti normativi e legali in ambito sicurezza delle informazioni;
  - Fornisce indicazioni e partecipa alle attività di revisione delle politiche e dei regolamenti di sicurezza IT;
  - Definisce le attività di audit da svolgere per verificare la conformità delle modalità di gestione della sicurezza delle informazioni rispetto alle politiche e alle procedure di Gruppo;
  - Assicura che i rapporti di audit e i problemi relativi alla sicurezza delle informazioni siano condivisi e riportati al Group IT Security Manager.

2.1.2. Group Information Security Committee

La presente Politica istituisce il Group Information Security Committee. L'obiettivo del Committee è quello di guidare e sviluppare iniziative di sicurezza informatica a livello di Gruppo. Il Committee, per adempiere alla sua responsabilità:

- Definisce e sviluppa progetti per migliorare la sicurezza delle informazioni in tutto il Gruppo;
- Rivede e approva la strategia di sicurezza delle informazioni di Gruppo e le responsabilità generali;
- Definisce ruoli e responsabilità specifiche per la sicurezza delle informazioni in tutto il Gruppo;
- Stabilisce metodologie e processi per la valutazione del rischio e la protezione delle informazioni del Gruppo Fedrigoni;

- Assicura che gli aspetti di sicurezza siano presi in considerazione nelle attività di pianificazione ed esecuzione dei processi IT.

Il Committee è composto dai seguenti partecipanti:

- Group Chief Information Officer,
- Group IT Security Manager,
- Group Compliance Officer & Chief Internal Auditor,
- Group Human Resources Officer rappresentato dal Group Head of Talent Acquisition & Development,
- Group Chief Financial Officer rappresentato dal Group Treasury and Risk Director.

Il Committee deve riunirsi almeno trimestralmente.

Ogni Business Unit/Legal Entity, se necessario, deve definire e dettagliare i ruoli e le responsabilità interne per gestire adeguatamente i temi della sicurezza delle informazioni in coordinamento con i relativi ruoli di Gruppo. Ciò è particolarmente significativo per le Business Unit/Legal Entity in cui i processi IT hanno un impatto rilevante sui principali processi aziendali.

2.1.3. Gestione degli asset

Tutti gli asset tecnologici (hardware[1], software[2] e risorse di rete[3]) associati alle informazioni del Gruppo Fedrigoni devono essere identificati e registrati in un inventario mantenuto aggiornato.
L'inventario degli asset deve riportare almeno:

- L'owner responsabile dell'inventario, della classificazione e della protezione dell'asset;
- La classificazione delle informazioni associate all'asset.

Le regole per l'uso accettabile degli asset devono essere identificate e documentate al fine di garantirne il corretto e sicuro funzionamento e per ridurre e prevenire i rischi (inclusi attacchi di virus, compromissione di sistemi e servizi di rete, questioni legali) legati ad un uso inappropriato (ad esempio, errori umani, furti, frodi o usi impropri).
I dipendenti e gli utenti esterni che utilizzano o hanno accesso agli asset del Gruppo Fedrigoni devono essere resi consapevoli dei requisiti di sicurezza definiti dal Gruppo e devono essere resi responsabili di ogni utilizzo delle risorse informatiche aziendali.
Tutti i dipendenti e gli utenti esterni devono restituire tutti i beni aziendali loro concessi al termine del rapporto di lavoro, del contratto o dell'accordo di collaborazione.

[1] Strumenti di elaborazione dati, apparecchiature trasportabili, apparecchiature fisse, periferiche di elaborazione, supporti dati, supporti elettronici, altri supporti.
[2] Sistema operativo, software di servizio, software di manutenzione, software di amministrazione, software di pacchetto, software standard, applicazione commerciale.
[3] Mezzi e attrezzature di comunicazione e telecomunicazione, dispositivi di rete, interfacce di comunicazione.

2.1.4. Classificazione delle informazioni

Le informazioni del Gruppo Fedrigoni devono essere classificate ed etichettate in termini di valore, requisiti legali, sensibilità e criticità. Oltre ai dati di tipo comune (dati personali identificativi, dati finanziari, ecc.) devono essere valutati i dati peculiari di settore (es. rete di vendita, gestione della catena di fornitura, concessioni e acquisizioni). Tutti i dati devono avere un owner responsabile della loro classificazione.
Le procedure per il trattamento degli asset devono essere sviluppate e implementate in accordo con lo schema di classificazione delle informazioni adottato dal Gruppo Fedrigoni.

2.1.5. Controllo degli accessi

Le informazioni devono essere protette dall'accesso non autorizzato per garantirne la riservatezza, l'integrità e la disponibilità.
L'intero ciclo di vita delle utenze (creazione dell'account utente, cambiamento dell'account utente e rimozione dell'account utente) deve essere definito per ridurre il rischio di accesso non autorizzato alle informazioni. Inoltre, devono essere definiti requisiti specifici sulla robustezza della password e le altre tecniche di autenticazione.
L'accesso remoto deve essere limitato al personale autorizzato ed eseguito attraverso canali criptati utilizzando un appropriato processo MFA (Multi-Factor Authentication).
I profili di accesso devono essere coerenti con le attività che devono essere svolte (principio del need-to-know) e devono seguire un processo di approvazione documentato. L'assegnazione di diritti di accesso privilegiati (ad esempio, da Amministratore di Sistema) deve essere controllata attraverso un processo di autorizzazione formale in conformità con la politica di controllo degli accessi definita.
Le attività di revisione periodica dei privilegi di accesso degli utenti devono essere eseguite per tutti i sistemi informativi al fine di garantire che siano assegnati sulla base del principio del "need-to-know". Le autorizzazioni per i diritti di accesso privilegiati devono essere riviste a intervalli più frequenti, in relazione alla criticità dei sistemi a cui si accede.
I criteri di segregazione dei compiti devono essere definiti per ogni processo in cui si trattano dati (ad esempio dati finanziari, dati aziendali, informazioni di identificazione personale, ecc.).

2.1.6. Sicurezza delle informazioni nelle terze parti

In caso di accesso di terze parti alle informazioni del Gruppo Fedrigoni, devono essere stabilite adeguate misure di sicurezza per garantire la riservatezza, l'integrità e la disponibilità delle informazioni.
Deve essere definito un processo di gestione del rischio delle terze parti al fine di attribuire un profilo di rischio agli accessi effettuati dai terzi e individuare le relative misure di sicurezza da contrattualizzare con essi.

Gli accordi con le terze parti devono includere requisiti relativi alla protezione dei dati del Gruppo Fedrigoni. In particolare, le terze parti dovranno essere disponibili a condividere, su richiesta, i loro piani di sicurezza e le misure di sicurezza implementate e consentire verifiche di sicurezza da parte del Gruppo Fedrigoni.
I Service Level Agreement (SLA) devono essere inclusi nei contratti con le terze parti per definire puntualmente i livelli di servizio. I servizi forniti dalle terze parti devono essere monitorati periodicamente.

2.1.7. Compliance

La gestione dei sistemi informativi adottati nel Gruppo Fedrigoni deve essere conforme alle leggi (es. GDPR), agli standard e alle politiche di Gruppo per prevenire i rischi di non conformità e le relative conseguenze (es. sanzioni, danni di reputazione, penali contrattuali, ecc.).
Poiché i requisiti legislativi potrebbero variare da nazione a nazione, è necessario implementare un processo di gestione della conformità al fine di essere in grado di dimostrare la conformità alla legislazione vigente applicabile e di essere pronti a identificare tempestivamente i requisiti locali per mantenere lo stato di conformità.
Ogni Legal Entity deve identificare un owner per il processo di gestione della conformità responsabile di affrontare, in coordinamento con il Group IT Security Manager e in coordinamento con il Group Compliance Officer & Chief Internal Auditor, le attività relative ai requisiti di sicurezza delle informazioni applicabili localmente

2.2. Controlli sul personale

2.2.1. Sicurezza delle Risorse Umane

Durante il processo di assunzione di personale, le attività di verifica effettuate dal dipartimento Human Resources sui candidati devono essere proporzionate ai requisiti aziendali, alla classificazione delle informazioni a cui tali candidati potranno/dovranno accedere e ai relativi rischi associati.
Gli accordi contrattuali con i dipendenti e i collaboratori devono specificare le loro responsabilità in tema di sicurezza delle informazioni.
Il Management delle Legal Entity deve richiedere a tutti i dipendenti e collaboratori di applicare le misure di sicurezza in conformità con le politiche e le procedure definite dal Gruppo Fedrigoni. I dipendenti e i collaboratori devono essere consapevoli delle minacce e istruiti sul corretto utilizzo dei sistemi informativi e dei dispositivi di proprietà del Gruppo Fedrigoni (attività di sensibilizzazione e formazione).
I dipendenti e i collaboratori devono essere consapevoli che le loro responsabilità e i loro doveri in materia di sicurezza delle informazioni rimangono validi anche dopo la cessazione o la modifica del rapporto di lavoro o di collaborazione.

I diritti di accesso attribuiti ai dipendenti e collaboratori in relazione alle informazioni e alle strutture di elaborazione delle informazioni devono essere rimossi al momento della cessazione del rapporto di lavoro o di collaborazione o aggiornati in seguito a cambiamenti intercorsi.

2.3. Controlli fisici

2.3.1. Sicurezza fisica

Le misure di controllo inerenti gli accessi fisici devono essere definite per assicurare che solo il personale autorizzato possa accedere alle aree aziendali. In particolare, le misure di sicurezza fisica devono essere applicate dove sono conservati gli asset che contengono informazioni aziendali sensibili o critiche. L'implementazione delle misure di sicurezza fisica deve tenere in considerazione i livelli fisici specifici definiti dal Gruppo Fedrigoni.
Le misure di controllo inerenti gli accessi fisici devono essere regolarmente monitorate per garantire la loro efficacia nella protezione contro gli accessi non autorizzati.

2.3.2. Sicurezza ambientale

Le attrezzature devono essere protette anche dalle minacce ambientali (ad esempio incendio, inondazione, interferenze elettriche, ecc.). Gli ambienti di lavoro devono rispettare le politiche di Gruppo in materia di salute e sicurezza.

2.4. Controlli tecnologici

2.4.1. Sicurezza delle operazioni

Le modifiche all'organizzazione, ai processi aziendali, alle strutture di elaborazione delle informazioni e ai sistemi che influiscono sulla sicurezza delle informazioni devono essere controllate e documentate (Change Management)
L'uso delle risorse deve essere monitorato e devono essere effettuate proiezioni sui requisiti futuri in termini di capacità per garantire il mantenimento del livello delle prestazioni dei servizi IT (Capacity Management), tenendo conto della criticità del business dei sistemi interessati.
Il back-up delle informazioni del Gruppo Fedrigoni deve essere effettuato e testato regolarmente per mantenere la disponibilità dei dati in linea con i rischi associati. Inoltre, il software e le strutture di elaborazione delle informazioni devono essere protetti da codici malevoli per garantire l'integrità del software e delle informazioni.
I log degli eventi che tengono traccia delle attività degli utenti, degli amministratori e degli operatori di sistema, delle eccezioni, dei guasti e degli eventi relativi alla sicurezza delle informazioni, devono

essere prodotti, conservati e rivisti regolarmente. Le attività di registrazione devono essere eseguite in conformità alla legislazione vigente.
Le informazioni sulle vulnerabilità tecniche dei sistemi informativi utilizzati devono essere ottenute in modo tempestivo, l'esposizione a tali vulnerabilità deve essere oggetto di valutazione e devono essere adottate misure appropriate per affrontare il rischio associato.
Ciascuna Legal Entity, prendendo in considerazione il proprio contesto aziendale e i relativi rischi, valuta l'implementazione di procedure di mascheramento dei dati (ad esempio per proteggere i dati personali) e sistemi o tecniche di prevenzione della perdita di dati al fine di identificare, monitorare e proteggere le informazioni da accessi non autorizzati.

2.4.2. Sicurezza delle comunicazioni

I dispositivi di comunicazione e di rete devono essere protetti per garantire l'integrità, la riservatezza e la disponibilità dei dati. La sicurezza dei dispositivi di rete deve essere configurata correttamente, per assicurare la corretta segregazione tra i diversi ambienti di utilizzo. La sicurezza relativa allo scambio di dati tra luoghi fisici distinti (stabilimenti, sedi centrali e magazzini) e con le terze parti deve essere affrontata anche per mezzo di specifiche misure di sicurezza (ad esempio implementando la crittografia dei dati).

2.4.3. Acquisizione, sviluppo, mantenimento e dismissione dei sistemi informativi

Il ciclo di vita di sviluppo del sistema e le sue fasi (installazione, configurazione, manutenzione e dismissione) devono essere chiaramente definiti per prevenire la perdita di dati o la modifica non autorizzata. Gli ambienti di sviluppo, test e produzione devono essere segregati e l'accesso al codice sorgente del programma deve essere limitato.
Devono essere definite politiche di Gruppo per valutare le misure di sicurezza relative all'adozione di servizi Cloud e dispositivi di Mobile Computing.
Al fine di identificare i requisiti di sicurezza prima dello sviluppo e/o dell'implementazione dei sistemi informativi, deve essere definito e implementato a livello di Gruppo un processo di Security by Design.

2.4.4. Gestione degli incidenti relativi alla sicurezza delle informazioni

Gli eventi di sicurezza e le vulnerabilità associate ai sistemi informativi devono essere comunicate tempestivamente per intraprendere le appropriate azioni correttive.
Devono essere messe in atto procedure di segnalazione e di escalation degli eventi. Tutti i dipendenti e i collaboratori devono essere informati su come poter segnalare le diverse tipologie di eventi che potrebbero avere un impatto sulla sicurezza degli asset informatici del Gruppo Fedrigoni.

Le attività di gestione degli incidenti di sicurezza delle informazioni devono essere allineate al processo definito a livello di Gruppo. In caso di violazione di dati personali, le attività di gestione devono essere conformi ai requisiti normativi vigenti (es. GDPR).

2.4.5. Gestione della Business Continuity e Disaster Recovery

Un sistema di gestione della Business Continuity è un insieme di processi, procedure e sistemi tecnologici finalizzati a garantire la continuità delle attività aziendali, in caso di eventi/disastri significativi, minimizzando i relativi impatti (es. perdita di ricavi, perdita di efficienza operativa, perdita di immagine e reputazione, ecc.). Per definire un sistema di gestione della Business Continuity deve essere analizzato il contesto di business del Gruppo Fedrigoni, definite le relative strategie di continuità operativa (Piano di Business Continuity) e le misure tecnologiche ed organizzative per ripristinare sistemi, dati ed infrastrutture dopo il verificarsi di un evento che interrompa i processi aziendali (Piano di Disaster Recovery).
Il piano di Business Continuity e il piano di Disaster Recovery devono essere regolarmente testati al fine di verificarne l'efficacia e l'efficienza e rivisti e aggiornati periodicamente in caso di cambiamenti significativi del contesto del Gruppo.

3. Eccezioni

Le Legal Entity o le Business Unit possono decidere di adottare requisiti più restrittivi rispetto quelli delineati dalla presente Politica. Tali situazioni non sono considerate eccezioni alla Politica e pertanto devono solo essere notificate al Group IT Security Manager.
Le eccezioni a questa Politica devono essere formalmente approvate dal Group IT Security Manager in accordo con i principi guida del Gruppo Fedrigoni.

4. Adeguamenti

La presente Politica deve essere rivista formalmente almeno una volta ogni tre anni.
In caso sia necessario implementare cambiamenti prima della scadenza triennale fissata per l’aggiornamento della Politica, gli stessi devono essere condiviso con il Group Compliance Officer & Chief Internal Auditor.