Politica per la Sicurezza delle Informazioni

POLIFIN

Cronologia:

Edizione	Data	Motivo revisione/ commenti
01	03 marzo 2026	Prima emissione

Approvazione:

	Funzione
Redatto da:	QHSE & Sustainability Function
	Security & Compliance Function
Controllato da:	QHSE & Sustainability Director
	Corporate Chief Information & Digital Officer
Approvato da:	Consiglio di Amministrazione

INDICE

1. PREMESSA

Il Gruppo Polifin (di seguito, “il Gruppo” oppure “Polifin”) opera nel rispetto dei principi di etica del lavoro, competenza tecnica e miglioramento continuo, promuovendo una cultura orientata all’innovazione e all’eccellenza operativa. Tali valori costituiscono il fondamento del posizionamento del Gruppo nei propri settori di riferimento.

Sulla base dei principi di sostenibilità, dei valori aziendali, nonché delle dimensioni del Gruppo e del contesto organizzativo, è stata definita la presente Politica per la Sicurezza delle Informazioni.

La Politica ha lo scopo di stabilire i principi fondamentali e di fornire al personale linee guida, volte a garantire la protezione dei sistemi informativi, dei dati aziendali e delle informazioni del Gruppo Polifin.

La presente Politica per la Sicurezza delle Informazioni definisce i principi fondamentali e le linee guida attraverso cui il Gruppo Polifin intende assicurare la **riservatezza**, l’**integrità** e la **disponibilità** delle informazioni, proteggendo l’organizzazione dalle minacce informatiche in continua evoluzione.

L’obiettivo della Politica è fornire un quadro di riferimento per la definizione degli obiettivi di sicurezza delle informazioni e sostenere il miglioramento continuo, in coerenza con le esigenze operative e con il contesto di rischio del Gruppo.

La Policy si applica a tutte le società del Gruppo Polifin e riguarda dipendenti, collaboratori esterni, fornitori e qualsiasi soggetto che abbia accesso o gestisca informazioni aziendali. Tutti i destinatari della presente Politica sono tenuti ad operare in conformità ai principi e alle disposizioni in essa contenuti. La Politica è resa disponibile agli stakeholder ed è adeguatamente comunicata all’interno dell’organizzazione e resa disponibile all’esterno.

Il presente documento è approvato dal Consiglio di Amministrazione del Gruppo Polifin. Il Consiglio di Amministrazione ne assicura inoltre il riesame periodico, al fine di valutarne l’adeguatezza e individuare eventuali azioni di miglioramento.

In tale contesto, tutte le società del Gruppo adottano i contenuti della Politica attraverso le proprie strutture organizzative, impegnandosi a:

- garantire la conformità alle normative applicabili;
- fornire ai dipendenti un chiaro quadro di riferimento e orientamento;
- contribuire all’individuazione e al perseguimento degli obiettivi e dei traguardi del Gruppo.

2. APPROCCIO ALLA SICUREZZA DELLE INFORMAZIONI

Il Gruppo Polifin affronta la sicurezza delle informazioni adottando un **approccio sistematico** e **basato sull'analisi del rischio**. Tale metodologia prevede che le misure di sicurezza siano calibrate in funzione della criticità degli asset informativi da proteggere, assicurando così una protezione adeguata e proporzionata rispetto ai rischi identificati.

Per garantire una gestione efficace e coerente della sicurezza delle informazioni, il Gruppo si impegna a rispettare i seguenti principi fondamentali:

- **Proteggere la riservatezza, l'integrità e la disponibilità delle informazioni trattate**: incluse quelle dei clienti, dei dipendenti e dei partners commerciali;
- **Continuità operativa e resilienza**: vengono adottate misure volte ad assicurare che i processi aziendali possano proseguire anche in presenza di eventi avversi, minimizzando l'impatto di eventuali interruzioni e favorendo il rapido ripristino delle attività;
- **Prevenire accessi non autorizzati, alterazioni non consentite e indisponibilità delle informazioni**, riducendo al minimo i rischi attraverso un'efficace gestione del cambiamento e dei processi IT;
- **Gestione tempestiva degli incidenti di sicurezza**: il Gruppo Polifin si prefigge di rilevare, gestire e risolvere con prontezza eventuali incidenti legati alla sicurezza delle informazioni, limitando i potenziali danni e prevenendo il ripetersi di situazioni analoghe;
- **Tutela della reputazione aziendale**: la protezione delle informazioni è essenziale per preservare la credibilità e l'immagine del Gruppo presso clienti, partner e mercato di riferimento;
- **Mantenimento del rapporto di fiducia con clienti e stakeholder**: le azioni adottate mirano a soddisfare le aspettative e le necessità di tutte le parti interessate, consolidando la fiducia nei confronti dell'organizzazione;
- **Conformità normativa e contrattuale**: vengono rispettate tutte le normative vigenti in materia di sicurezza delle informazioni, nonché i requisiti specifici previsti nei contratti stipulati con clienti e fornitori;
- **Promozione della cultura della cybersecurity**: il Gruppo Polifin promuove la consapevolezza e la responsabilità in materia di sicurezza informatica all'interno dell'azienda, incoraggiando una cultura diffusa della sicurezza a tutti i livelli organizzativi.

3. APPROFONDIMENTO SULLE MISURE PER LE SOCIETÀ INCLUSE NELL'AMBITO DELLA DIRETTIVA NIS2

I paragrafi seguenti si applicano esclusivamente alle Società del Gruppo Polifin che rientrano nel campo di applicazione della Direttiva Europea Network Information Security 2 (anche detta, NIS2) (2022/2555).

Queste società devono adottare misure specifiche per la sicurezza delle informazioni e la cybersecurity, così da garantire una protezione elevata e uniforme. Questa policy indica le aree chiave e le misure necessarie per rispettare la Direttiva NIS2.

A livello di Gruppo, la funzione Security & Compliance ha il compito di coordinare le attività di sicurezza, mantenere un livello adeguato in materia di information security, garantire la coerenza nell'applicazione della presente Policy tra le varie Società.

Gli impegni e la responsabilità assunti dal top management relativamente alla sicurezza delle informazioni si concretizzano attraverso le seguenti azioni:

- promuovere l'importanza dell'efficacia delle attività relative alla sicurezza informatica, in conformità ai requisiti e l'importanza del raggiungimento degli obiettivi prefissati;
- stabilire e diffondere la politica per la sicurezza delle informazioni, comprensiva di principi e obiettivi;
- agevolare l'integrazione della sicurezza delle informazioni nei processi aziendali;
- assicurare la disponibilità di risorse adeguate in funzione delle necessità;
- vigilare su incidenti di sicurezza e sulla gestione del rischio.

3.1 GESTIONE DEL RISCHIO INFORMATICO

La gestione del rischio è un processo fondamentale per la protezione delle informazioni delle Società del Gruppo Polifin. La funzione Security & Compliance si impegna a identificare, valutare e trattare i rischi informatici in modo strutturato e associandoli alle vulnerabilità e alle minacce sugli asset.

Sono mappati gli asset critici e, attraverso l'analisi del rischio residuo, è possibile definire le priorità di intervento e le contromisure più adeguate, adeguatamente registrate, monitorate e rendicontante.

3.2 PROTEZIONE DEGLI ASSET E CONFIGURAZIONE

Ogni asset informatico, sia esso hardware o software, è identificato e gestito tramite un inventario che le società hanno il compito di popolare, mantenere e aggiornare. Per quanto riguarda i dati aziendali, questi sono classificati in base alla criticità e a ciascuna categoria sono applicate specifiche misure di sicurezza. In relazione alle configurazioni dei dispositivi, queste saranno gestite in maniera centralizzata, con particolare attenzione agli aggiornamenti, alle configurazioni sicure e alla protezione degli endpoint.

3.3 SICUREZZA DELLA SUPPLY CHAIN

La sicurezza della catena di fornitura rappresenta un elemento strategico del Gruppo. I fornitori ritenuti critici sono sottoposti a una valutazione preventiva dei rischi e i rapporti con gli stessi sono gestiti attraverso specifiche clausole relative alla sicurezza delle informazioni e monitorati nel tempo.

3.4 SICUREZZA FISICA E LOGICA

La protezione degli ambienti fisici e logici che ospitano dati e sistemi è parte integrante della strategia di sicurezza. L'accesso ai data center e alle aree riservate è regolamentato da procedure rigorose, e in base al rischio identificato, possono essere adottate misure fisiche come il controllo degli accessi e la videosorveglianza. Parallelamente, i sistemi informatici sono protetti con misure logiche efficaci, inclusi, a titolo di esempio, segmentazione della rete, antivirus e backup sicuri.

3.5 GESTIONE DEGLI INCIDENTI INFORMATICI

Ogni società del Gruppo in scope NIS2 adotta, in linea con la presente policy, una strategia chiara per la gestione degli incidenti informatici. A livello di Gruppo, è istituito il **Computer Security Incident Response Team** (CSIRT) incaricato di rilevare, classificare e rispondere tempestivamente agli eventi. Ogni incidente è documentato e analizzato per identificare le cause scatenanti, definire misure correttive e preventive.

In caso di incidente, le autorità competenti sono informate secondo quanto previsto dalla normativa vigente.

La comunicazione con gli stakeholder è gestita in modo coordinato con le funzioni coinvolte per ridurre l'impatto reputazionale.

3.6 BUSINESS CONTINUITY IT E DISASTER RECOVERY

La continuità dei processi aziendali in caso di interruzioni causate da incidenti informatici o da disastri naturali è essenziale ed è assicurata attraverso piani specifici di business continuity IT e disaster recovery. I piani e gli scenari sono testati regolarmente per verificarne l'efficacia e aggiornati in base all'evoluzione del contesto tecnologico e dei rischi. Inoltre, sono definite chiare procedure di escalation e responsabilità durante le situazioni di crisi.

Gli obiettivi della gestione della business continuity IT sono:

- assicurare la continuità delle operazioni IT nel rispetto delle priorità individuate;
- ridurre al minimo tempi e costi di ripristino delle attività IT interrotte;
- operare in relazione alla valutazione del rischio IT;
- definire ruoli, responsabilità e modalità operative delle risorse umane interne ed esterne (inclusi fornitori esterni) coinvolte.

La funzione di Security & Compliance assicura che i piani di continuità siano conformi ai requisiti normativi, con i livelli di rischio identificati, coerentemente con quanto definito dalla presente Policy.

3.7 SICUREZZA DELLE INFORMAZIONI NEL RAPPORTO DI LAVORO

Il Gruppo tutela la sicurezza delle informazioni aziendali adottando controlli e misure adeguate lungo l'intero ciclo di vita del rapporto di lavoro del dipendente, garantendo che in ogni sua fase – dall'on boarding all'off boarding – la tutela delle informazioni sia gestita in modo sicuro e coerente con le politiche aziendali.

A tal fine, l'organizzazione applica anche rigorosi criteri di segregazione dei compiti, garantendo che attività critiche non siano concentrate in capo a un unico soggetto.

3.8 FORMAZIONE E CONSAPEVOLEZZA

La consapevolezza e l'adeguato livello di conoscenza dei dipendenti e del top management riguardo a tematiche di sicurezza informatica sono cruciali per la protezione efficace degli asset del Gruppo. Ogni dipendente riceve un'adeguata formazione sulle politiche, sulle procedure e sui processi in relazione al ruolo che svolge. Particolare attenzione è riservata ai ruoli più esposti e alle funzioni critiche.

3.9 MONITORAGGIO

L'efficacia delle misure di sicurezza è oggetto di controlli periodici attraverso audit interni e/o esterni. Il monitoraggio continuo dei sistemi permette di individuare comportamenti anomali e violazioni, agendo tempestivamente per correggerli. Report sintetici dei risultati del monitoraggio sono condivisi con la direzione e i Consigli di Amministrazione delle società del Gruppo in scope NIS2 per garantire una supervisione adeguata.

POLIFIN

POLIFIN S.p.A.
Viale Vittorio Emanuele II, 10/M - 24121 - Bergamo BG - Italy
Tel. e Fax +39 035 235 236
C.F./P.IVA 03440020166