POLITICA PER LA SICUREZZA DELLE INFORMAZIONI

BONDIOLI & PAVESI S.P.A. HP HYDRAULIC S.P.A. SIBONI S.P.A. DINOIL S.P.A. FIRA S.P.A.

In conformità al D.L. n. 138 del 04/09/2024 e s.m.i. che recepisce la Direttiva (UE) 2022/2555 NIS2

L'Azienda riconosce che la sicurezza informatica e la continuità operativa dei propri servizi digitali rivestono un ruolo essenziale per la tutela dei dati, delle informazioni e degli interessi dei propri stakeholder. A tal fine, la Direzione definisce la presente Politica per la Gestione del Rischio di Cybersecurity, che stabilisce i principi generali per l'adozione di misure organizzative e tecniche conformi alla Direttiva UE 2022/2555 (*NIS2*) e alla normativa nazionale di recepimento.

L'Azienda si impegna a:

- definire e formalizzare ruoli, responsabilità e poteri in materia di cybersecurity, promuovendo la responsabilizzazione (accountability) e l'efficacia dei processi decisionali;
- istituire e mantenere un'organizzazione per la sicurezza informatica approvata dagli organi direttivi, garantendone la diffusione e la comprensione all'interno delle articolazioni competenti;
- mantenere un elenco aggiornato del personale che ricopre specifici ruoli e responsabilità in ambito cybersecurity, rendendolo disponibile agli attori interni interessati;
- stabilire una Politica per la Gestione del Rischio di Cybersecurity basata sul contesto operativo, sulle priorità aziendali e sulla strategia di protezione digitale;
- adottare politiche documentate per i seguenti ambiti di sicurezza:
  a) gestione del rischio;
  b) ruoli e responsabilità;
  c) affidabilità delle risorse umane;
  d) conformità e audit di sicurezza;
  e) gestione dei rischi della supply chain;
  f) gestione degli asset;
  g) gestione delle vulnerabilità;
  h) continuità operativa e disaster recovery;
  i) gestione delle identità digitali, autenticazione e controllo accessi;
  j) sicurezza fisica;
  k) formazione e consapevolezza del personale;
  l) sicurezza dei dati;
  m) ciclo di vita dei sistemi informativi e di rete;
  n) protezione delle reti e delle comunicazioni;
  o) monitoraggio degli eventi di sicurezza;
  p) risposta agli incidenti e ripristino.

La presente Politica viene comunicata al personale e alle parti interessate ed è soggetta a riesame periodico almeno annuale, nonché in occasione di incidenti significativi, variazioni organizzative o mutamenti dell'esposizione alle minacce e ai relativi rischi.

La Direzione si impegna a fornire le risorse necessarie per garantire l'attuazione effettiva dei principi qui stabiliti e a promuovere un processo di miglioramento continuo della postura di sicurezza dell'Azienda.

Presidente del Consiglio di Amministrazione

POLITICA PER LA SICUREZZA DELLE INFORMAZIONI – FINSUGE S.P.A.

La Politica per la Sicurezza delle Informazioni di FINSUGE S.P.A. riflette l'impegno della Direzione e di tutta l'organizzazione nel garantire la protezione delle informazioni da ogni minaccia, interna o esterna, deliberata o accidentale.
Il Consiglio di amministrazione definisce e attua questa Politica e ne affida l'attuazione alla Direzione dei Sistemi Informativi di Gruppo, assicurandone la diffusione, la comprensione e l'applicazione a ogni livello aziendale.
La gestione della sicurezza delle informazioni si fonda sul presidio dei tre principi fondamentali:

- Riservatezza: assicurare che le informazioni siano accessibili esclusivamente alle persone debitamente autorizzate.
- Integrità: preservare l'esattezza e la completezza delle informazioni e dei metodi di elaborazione.
- Disponibilità: garantire che le informazioni e i sistemi che le trattano siano accessibili e utilizzabili tempestivamente su richiesta degli utenti autorizzati.

Per presidiare tali principi, FINSUGE S.P.A. ha implementato un Sistema di Gestione per la Sicurezza delle Informazioni conforme alla norma internazionale ISO/IEC 27001, basato sui seguenti impegni strategici:

- Tutela delle informazioni: adottare misure organizzative e tecniche idonee a proteggere i dati propri, dei clienti, dei fornitori e delle parti interessate, durante tutto il loro ciclo di vita.
- Formazione, consapevolezza e responsabilizzazione: promuovere la cultura della sicurezza attraverso programmi strutturati di formazione e sensibilizzazione per tutto il personale.
- segnalazione e gestione degli incidenti di sicurezza, predisponendo piani di continuità operativa e disaster recovery per limitare gli impatti, garantire la resilienza dei servizi e favorire il miglioramento continuo.
- Selezione e controllo dei fornitori: qualificare i fornitori sulla base di criteri stringenti di sicurezza delle informazioni, stipulando accordi contrattuali specifici e realizzando monitoraggi e verifiche periodiche.
- Controllo degli accessi: applicare criteri rigorosi di gestione degli accessi fisici e logici alle informazioni, assicurando che le autorizzazioni siano assegnate, revocate o modificate tempestivamente in funzione dei ruoli aziendali.
- Miglioramento continuo ed etica organizzativa: garantire il costante miglioramento del Sistema di Gestione per la Sicurezza delle Informazioni attraverso audit, analisi e riesami, operando nel rispetto dei principi di correttezza, trasparenza e responsabilità verso tutti gli stakeholder.

In conformità al D.L. n. 138/2024, di recepimento della Direttiva (UE) 2022/2555 (NIS2), l'Azienda integra nella presente Politica i principi essenziali della normativa europea, impegnandosi a:

- garantire una chiara definizione di ruoli e responsabilità in ambito cybersecurity;
- mantenere un'organizzazione dedicata alla sicurezza informatica approvata dalla Direzione;
- adottare misure tecniche e organizzative adeguate alla gestione del rischio cyber, la sicurezza degli asset, la gestione delle vulnerabilità, la continuità operativa e la risposta agli incidenti;
- assicurare la diffusione, la consapevolezza e il rispetto delle prescrizioni NIS2 all'interno dell'organizzazione.

La Politica viene riesaminata in occasione di mutamenti rilevanti nel contesto normativo, organizzativo o tecnologico, per assicurarne la continua adeguatezza, coerenza con la strategia aziendale e l'allineamento alle migliori pratiche internazionali.

Presidente del Consiglio di Amministrazione