# POLITICA DELLA CYBERSICUREZZA

La Politica Aziendale di Cybersicurezza è adottata in conformità ai requisiti della Direttiva NIS 2 (Direttiva UE 2022/2555) e del D. Lgs. 4 settembre 2024, n. 138 di recepimento. La presente Politica definisce l'approccio strategico dell'organizzazione alla gestione dei rischi di cybersicurezza per garantire la resilienza delle reti e dei sistemi informativi.

## SCOPO E OBIETTIVI

La Direzione di IG3 S.R.L. ha definito, approvato e si impegna a mantenere attiva a tutti i livelli dell'organizzazione la presente Politica di Cybersicurezza.

Lo scopo della presente Politica è garantire un livello elevato di Cybersicurezza attraverso:

- La protezione delle reti e dei sistemi informativi da minacce cyber, incidenti e attacchi informatici;
- La gestione integrata dei rischi di cybersicurezza secondo un approccio basato sul rischio;
- La resilienza operativa e la continuità dei servizi;
- Il rispetto degli obblighi di notifica degli incidenti significativi alle Autorità competenti (ACN e CSIRT Italia);
- L'implementazione delle misure tecniche e organizzative previste dalla Direttiva NIS 2;
- La promozione di una cultura della cybersicurezza a tutti i livelli aziendali.

Gli obiettivi strategici che si pone l'Organizzazione sono di seguito riportati:

- Raggiungere e mantenere un livello adeguato di cybersicurezza proporzionato ai rischi identificati;
- Garantire la sicurezza della catena di approvvigionamento;
- Assicurare la conformità normativa con la Direttiva NIS 2 e le nome attuative;
- Minimizzare l'impatto degli incidenti di cybersicurezza su servizi, utenti e altre organizzazioni.

## CAMPO DI APPLICAZIONE

La presente Politica si applica:

- A tutti gli organi di governance dell'organizzazione, inclusi i membri dell'organo di gestione;
- A tutto il personale (dipendenti, collaboratori, consulenti), a qualsiasi livello;
- A tutti i fornitori e partner della catena di approvvigionamento che trattano dati o gestiscono servizi critici per l'organizzazione;
- A tutte le reti, sistemi informativi e servizi utilizzati per l'erogazione dei servizi.

L'attuazione della presente politica è obbligatoria e vincolante. Ogni accordo con soggetti terzi deve includere clausole contrattuali che garantiscano il rispetto dei requisiti di cybersicurezza qui definiti.

## GOVERNANCE DELLA CYBERSICUREZZA

In conformità all'Art. 20 della Direttiva NIS 2, l'organo di gestione (la Direzione) assume la responsabilità diretta in materia di cybersicurezza. Tale responsabilità si concretizza nell'approvazione e supervisione dell'attuazione della presente Politica, nella valutazione e approvazione delle misure di gestione dei rischi cyber adottate dall'organizzazione e nella supervisione dell'implementazione delle misure tecniche, operative e organizzative necessarie.

L'organo di gestione partecipa a programmi di formazione specifici sulla cybersicurezza per mantenere una conoscenza adeguata delle minacce e delle strategie di protezione e garantisce l'allocazione di risorse adeguate, umane, tecniche e finanziarie, per assicurare un livello di sicurezza appropriato.

L'organo di gestione risponde direttamente della violazione degli obblighi in materia di cybersicurezza.

## POLICY SICUREZZA DELLE INFORMAZIONI

Il patrimonio informativo da tutelare è costituito dall'insieme delle informazioni trattate e gestite attraverso i servizi forniti dall'Azienda e localizzate in tutte le infrastrutture e gli ambienti (inclusi sistemi cloud e data center).
In conformità a quanto previsto dalla Direttiva (UE) 2022/2555 e dal D.lgs. 138/2024, l'Azienda adotta un approccio di gestione del rischio cyber volto a garantire la sicurezza delle reti e dei sistemi informativi, nonché la continuità dei servizi da essa forniti.

È necessario assicurare, in ogni fase del trattamento e della gestione delle informazioni:

- La **confidenzialità**: le informazioni devono essere accessibili solo a persone, sistemi o entità autorizzate, in base a diritti di accesso definiti e periodicamente revisionati;
- L'**integrità**: deve essere preservata la correttezza, la completezza e la tracciabilità delle informazioni e dei processi, prevenendo possibili modifiche non autorizzate o accidentali;
- La **disponibilità**: i sistemi e le informazioni devono essere accessibili e utilizzabili dagli utenti autorizzati nei tempi e nei modi richiesti per l'erogazione dei servizi.

La carenza di adeguate misure di sicurezza può comportare impatti negativi significativi, tra cui danni reputazionali e perdita di fiducia da parte di clienti e stakeholder, interruzioni operative, violazioni normative e perdite economico-finanziarie.
Un livello di sicurezza adeguato è condizione essenziale per la resilienza operativa dell'Azienda e per la condivisione sicura delle informazioni.

## RESPONSABILITÀ PER L'OSSERVANZA E L'ATTUAZIONE DELLA POLICY DI CYBERSICUREZZA

L'osservanza e l'attuazione della presente policy è responsabilità di:

1. **Tutto il personale interno**
   Tutti i dipendenti e collaboratori, a qualsiasi titolo coinvolti nei processi aziendali che prevedono il trattamento o la gestione di dati, informazioni e sistemi informatici rientranti nel perimetro della Direttiva NIS 2, sono tenuti a:
   - Rispettare le procedure operative aziendali;

- Adottare comportamenti conformi ai principi di sicurezza informatica e di protezione dei dati;
- Segnalare tempestivamente eventuali anomalie, incidenti, vulnerabilità o violazioni di sicurezza di cui vengono a conoscenza, in linea con i requisiti di reporting degli incidenti previsti dalla Direttiva NIS 2.

**2. Soggetti esterni e fornitori**

Tutti i soggetti esterni (fornitori, partner, consulenti e terze parti) che intrattengono rapporti con l'Azienda e che, a qualsiasi titolo, trattano o hanno accesso a dati, sistemi o infrastrutture aziendali, devono garantire il rispetto dei requisiti di sicurezza definiti nella presente Policy e nelle clausole contrattuali applicabili, in conformità ai principi di sicurezza della supply chain previsti dalla Direttiva NIS 2.

Chiunque – dipendente, consulente o collaboratore esterno – in modo intenzionale o per negligenza, violi le regole di sicurezza stabilite dalla presente Policy, causando danni all'Azienda o ai suoi clienti, potrà essere perseguito nelle opportune sedi e nel pieno rispetto dei vincoli di legge e contrattuali.

## RIESAME

La Direzione verificherà periodicamente e regolarmente, o in concomitanza di cambiamenti significativi, l'efficacia e l'efficienza delle procedure aziendali inerenti la cybersicurezza, in modo da assicurare un supporto adeguato all'introduzione di tutte le migliorie necessarie e in modo da favorire l'attivazione di un processo continuo, con cui viene mantenuto il controllo e l'adeguamento della Policy in risposta ai cambiamenti dell'ambiente aziendale e delle condizioni normative.

Durante questa fase dovranno essere tenuti in considerazione tutti i cambiamenti che possono influenzare l'approccio dell'Azienda alla gestione della Cybersicurezza, includendo i cambiamenti organizzativi, l'ambiente tecnico, la disponibilità di risorse e le condizioni normative o contrattuali.

## IMPEGNO DELLA DIREZIONE

La Direzione Aziendale sostiene attivamente la Cybersicurezza attraverso un chiaro indirizzo strategico, un impegno concreto, l'assegnazione di incarichi e il riconoscimento formale delle responsabilità in materia di Sicurezza.

In conformità ai principi della Direttiva NIS2, la Direzione assume la piena responsabilità della supervisione e della gestione del rischio informatico, garantendo che la sicurezza delle informazioni sia un obiettivo integrato nella governance e nella strategia aziendale.

Quinto di Treviso, lì 13/11/2025

La Direzione

IG3 SRL
Vicolo Zagaria, 4
31055 Quinto di Treviso (TV)
Cod. Fisc. e Part.IVA 04045190263
Tel. 0422/97097