konvecta

Politica per la sicurezza e la cybersicurezza dei sistemi informatici

Politiche Aziendali 2025

Indice

01

Finalità

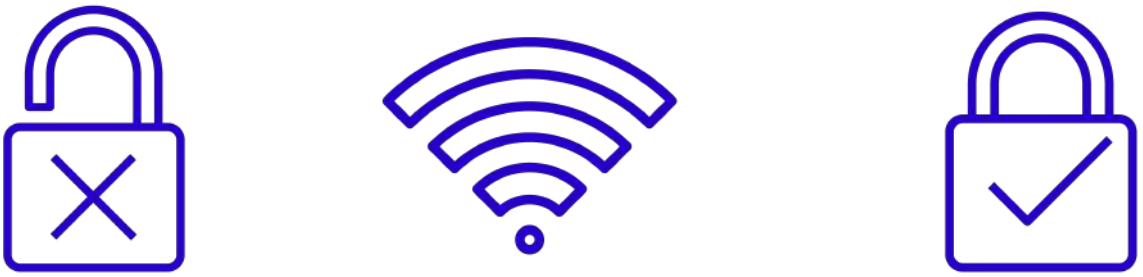
L'obiettivo della presente Politica per la sicurezza e la cybersicurezza dei sistemi informatici (di seguito, la "Politica"), che fa parte della Politica quadro di conformità, è quello di stabilire e diffondere le norme di base e generali di Konecta, gruppo multinazionale di società specializzate nella fornitura di servizi e soluzioni digitali di customer management (di seguito Konecta, l'Azienda, la Società o la Compagnia), per garantire l'integrità, la privacy e la riservatezza delle informazioni, in conformità con la legislazione vigente in materia, valutando i rischi e realizzando un uso efficiente delle risorse, il tutto sulla base di criteri di proporzionalità nella gestione.

L'uso massiccio delle tecnologie dell'informazione e delle telecomunicazioni (TIC) in tutti i settori della società ha creato un nuovo spazio, il cyberspazio, in cui possono verificarsi conflitti e aggressioni, nonché minacce informatiche che mettono a rischio Konecta e le sue diverse società.

La presente Politica stabilisce un quadro di riferimento che definisce i principi necessari per garantire la protezione dei sistemi informativi di Konecta da accessi non autorizzati, perdita o danni durante il trattamento delle informazioni, nonché da altri tipi di minacce informatiche, assicurando la disponibilità, l'integrità e la riservatezza delle informazioni dei dati gestiti da Konecta.

La presente Politica è stata concepita per stabilire il quadro di riferimento per i gruppi di interesse interni a Konecta (collaboratori, azionisti, investitori, dirigenti) ed esterni (clienti, fornitori, revisori, governi, enti regolatori, mezzi di comunicazione, concorrenti ed enti finanziari), rafforzando la fiducia nei sistemi informativi dell'azienda, garantendo il rigoroso rispetto della normativa vigente in materia in ciascun paese, dei propri requisiti e degli standard internazionali.

La presente Politica sarà disponibile sul sito web aziendale (Konecta.com) per garantirne la consultazione da parte di tutte le parti interessate.



02

Ambito di applicazione

La presente Politica rientra nell'ambito di applicazione della Politica quadro di conformità e si estende a tutte le entità di Konecta, con il sostegno della Direzione generale dell'azienda.

Di conseguenza, il suo contenuto costituisce un obbligo di osservanza per tutti i lavoratori di Konecta, indipendentemente dalla posizione o dalla funzione che ricoprono all'interno dell'organizzazione, nonché dalla loro ubicazione geografica.

Fatto salvo quanto sopra, il suo ambito di applicazione potrà essere esteso, quando necessario e possibile in base alla natura del rapporto, a tutte le persone fisiche e/o giuridiche legate a Konecta a livello aziendale o professionale, per un rapporto diverso da quello lavorativo: fornitori, appaltatori, lavoratrici e lavoratori della catena di approvvigionamento e partner commerciali.

Poiché molte delle società di Konecta hanno sede legale al di fuori dell'Unione europea, la normativa interna sarà, se necessario, adattata a quella propria di ciascun Stato, nel rispetto e nella tutela dei principi fondamentali qui enunciati.

03

Principi generali di attuazione

La Politica per la sicurezza e la cybersicurezza dei sistemi informatici riflette l'impegno esplicito dell'azienda a definire e stabilire le linee guida e il supporto adeguato alla gestione della sicurezza delle informazioni che gestisce, in conformità ai propri requisiti e alle leggi e ai regolamenti vigenti.

Konecta si impegna a garantire "un uso sicuro delle reti e dei sistemi informativi attraverso il rafforzamento delle nostre capacità di prevenzione, difesa, rilevamento, analisi, ricerca, recupero e risposta agli attacchi informatici" che potrebbero verificarsi.

Konecta promuove un uso sicuro dei sistemi informatici e delle telecomunicazioni, rimanendo sempre in linea con la strategia e gli obiettivi aziendali e, in questo senso, ha fissato tra i suoi obiettivi specifici i seguenti, coerenti con il contesto in cui si svolgono le attività dell'azienda:

- Promuovere la sicurezza e la resilienza delle reti e dei sistemi informativi utilizzati.
- Sensibilizzare l'intero personale aziendale sui rischi derivanti dal cyberspazio.
- Formare e mantenere le conoscenze, le competenze, l'esperienza e le capacità tecnologiche necessarie per sostenere gli obiettivi di Konecta in materia di sicurezza informatica.

In questo senso, Konecta si impegna a raggiungere i seguenti obiettivi:

- Considerare le informazioni e i sistemi che le supportano come risorse strategiche. Pertanto, Konecta manifesta la propria determinazione a raggiungere i livelli di sicurezza necessari a garantire i requisiti di riservatezza, integrità e disponibilità delle informazioni elaborate nell'organizzazione e delle risorse dei sistemi informatici che le elaborano, archiviano o distribuiscono.
- Garantire la diffusione delle norme definite a sostegno della presente Politica, con l'obiettivo di infondere nel personale di Konecta un livello di consapevolezza e formazione in materia di sicurezza delle informazioni, in modo da garantire l'applicazione di pratiche adeguate in questo campo, come elemento inerente allo svolgimento delle loro funzioni.
- Promuovere il raggiungimento dei necessari livelli di sicurezza delle informazioni come un processo continuo di miglioramento e progresso costante, basato sulla definizione degli obiettivi e dei requisiti da soddisfare, sull'implementazione dei processi e delle misure appropriate, sulla verifica della loro funzionalità, efficacia ed efficienza e sull'adozione delle correzioni e delle modifiche ritenute opportune.
- La presente Politica deve essere lo strumento principale da utilizzare per garantire adeguatamente la sicurezza delle informazioni, promuovendone e assicurandone il rispetto all'interno dei diversi servizi.
- Garantire l'esistenza dei meccanismi necessari ad assicurare la continuità delle attività critiche dell'azienda basate sui sistemi informatici, consentendo il loro ripristino in un lasso di tempo accettabile.
- Massimizzare la qualità dei servizi forniti.
- Ridurre o eliminare, per quanto possibile, i pericoli e i rischi relativi alle risorse, ai processi e ai servizi forniti da Konecta.
- Determinare le misure essenziali di sicurezza delle informazioni che Konecta deve adottare per proteggersi adeguatamente dalle minacce che potrebbero in

qualche modo compromettere la riservatezza, l'integrità e la disponibilità delle informazioni.

Gli obiettivi della presente Politica saranno implementati sulla base di una strategia a lungo termine. Le attività volte al raggiungimento degli obiettivi devono essere mantenute nel tempo.

In linea con i rischi per la sicurezza, i piani d'azione devono essere definiti e adeguati ogni anno (controlli di sicurezza, definizione di progetti di sicurezza, monitoraggio continuo, ecc.).

Saranno stabiliti i piani di transizione necessari per ridurre qualsiasi impatto sulle attività e/o sulle risorse di Konecta, che provvederà inoltre a garantire che le lavoratrici e i lavoratori:

- ... conoscano e applichino le procedure interne e i protocolli in materia di sicurezza delle informazioni di Konecta;
- ... dispongano di strumenti che consentano loro di accedere facilmente alle procedure operative interne (Intranet); inoltre, saranno utilizzati canali di comunicazione alternativi per la comunicazione di determinati processi, di misure speciali o di aggiornamenti delle procedure;
- ... siano consapevoli che devono trattare solo le informazioni per le quali sono stati autorizzati e utilizzare le risorse di Konecta esclusivamente per lo svolgimento delle loro funzioni professionali. I lavoratori e le lavoratrici devono rispettare le norme di base per l'accesso alle applicazioni e/o alle apparecchiature con accesso a dati di carattere personale;
- ...conoscano le procedure aziendali esistenti per sapere come agire di fronte a qualsiasi attività o minaccia che possa compromettere la sicurezza delle informazioni, informando il Reparto tecnologico e il Direttore della sicurezza (CISO).

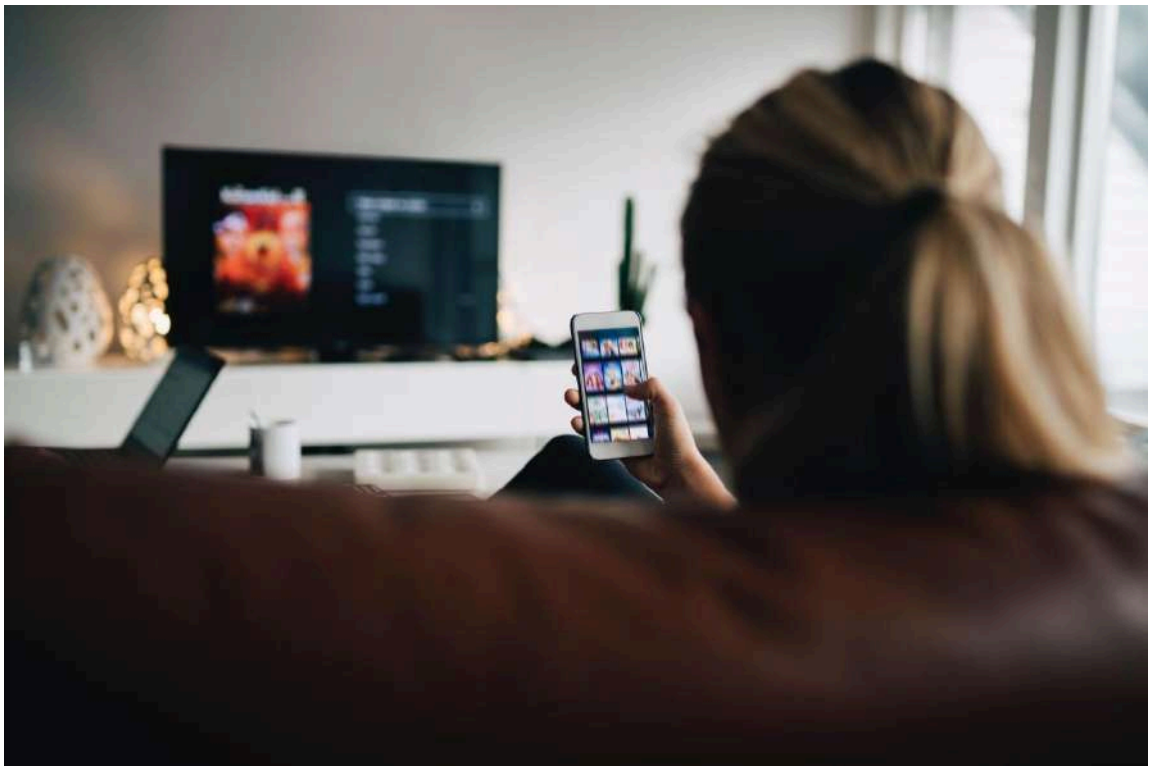
Essendo noi consapevoli del fatto che ciascuno dei paesi in cui l'azienda opera ha un proprio contesto sociale ed esigenze diverse, la presente Politica si articola in piani e azioni, relativi ai principi in essa contemplati, adattati alla realtà di ciascuno dei suoi stabilimenti locali.

Questi principi di azione rispondono agli impatti, ai rischi e alle opportunità (IRO) derivanti dalle questioni materiali applicabili: sicurezza delle informazioni, trasformazione digitale, conformità ed etica aziendale e gestione dei fornitori.

Tanto le lavoratrici e i lavoratori quanto qualsiasi terza parte che presuma l'esistenza di una potenziale violazione legata alla presente Politica o al Codice etico, potranno trasmettere le loro informazioni, dubbi o preoccupazioni in materia, in modo confidenziale e senza timore di ritorsioni, attraverso i Canali di Informazione disponibili sul sito web aziendale di Konecta (https://Konecta.integrityline.com), a seconda della natura della situazione, in conformità con la procedura PG COR 26 Canali di informazione, disponibile nello stesso spazio web, in cui sono specificati i diversi canali disponibili e la natura della comunicazione che può essere effettuata attraverso di essi.

Questo canale è disponibile 24 ore su 24, 7 giorni su 7. Non saranno tollerate ritorsioni contro chi, in buona fede, comunichi fatti che potrebbero costituire una violazione della presente Politica e ai comunicanti saranno applicate le garanzie e le tutele previste dalla normativa e dalla legislazione applicabile.

La violazione della presente Politica sarà soggetta alle misure disciplinari corrispondenti, in conformità con le norme e le procedure interne, fatte salve le sanzioni amministrative o penali che, se del caso, potrebbero derivarne e che saranno imposte dall'autorità competente.



04

Aggiornamento e revisione

La presente Politica costituisce la base per il rispetto delle seguenti normative:

- ISO/IEC 27001:2022 Tecnologia dell'informazione - Tecniche di sicurezza - Sistemi di gestione della sicurezza dell'informazione - Requisiti.
- ISO/IEC 27701 - Estensione della norma ISO 27001 per la gestione della privacy.
- ISO/IEC 27002:2022 Tecnologia dell'informazione - Tecniche di sicurezza - Codice di condotta per i controlli di sicurezza dell'informazione.
- 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 e che abroga la direttiva 95/46/CE (Regolamento generale sulla protezione dei dati) (Testo rilevante ai fini del SEE).
- Leggi in materia di protezione dei dati personali applicabili in ciascun paese.

La Politica per la sicurezza e la cybersicurezza dei sistemi informativi sarà rivista periodicamente o quando necessario, per adeguarla ai cambiamenti nel modello di business, all'approvazione di nuove normative o alle migliori pratiche internazionali, garantendone l'efficacia e il continuo rispetto.

NOTA: La presente Politica è stata riveduta e approvata il 16 dicembre 2025 dal massimo organo di governance e sostituisce qualsiasi versione precedente; a partire dalla data odierna sarà ritenuto valido esclusivamente il presente documento.

Controllo delle revisioni

Edizione	Data di revisione	Revisionato	Validato	Approvato	Motivo della modifica
2	22/06/2022	IT_Sicurezza delle Informazioni Organizzazione e Procedure	Consulenza Legale	Consiglio di Amministrazione	Generale Revisione delle Politiche
3	19/12/2022	IT_Sicurezza delle Informazioni Organizzazione e Procedure	Consulenza Legale	Consiglio di Amministrazione	Generale Revisione delle Politiche
4	16/12/2025	IT_Sicurezza delle Informazioni Organizzazione e Procedure	Consulenza Legale	Consiglio di Amministrazione	Adeguamento ai requisiti di legge Adeguamento al nuovo formato e al marchio