konvecta

Information systems security and cybersecurity policy

Corporate Policies 2025

Table of contents

01 Purpose

The objective of this Information Systems Security and Cybersecurity Policy (hereinafter, the “Policy”), is to establish and disseminate the basic and general rules of Konecta, a multinational group of companies specialising in the provision of digital customer management services and solutions (hereinafter, Konecta, the Company or the Firm), to guarantee the integrity, privacy and confidentiality of information, in accordance with current legislation on the matter, weighing up the risks and making efficient use of resources, all based on criteria of proportionality in management.

The widespread use of information and communication technologies (ICT) in all areas of society has created a new space, cyberspace, where conflicts and attacks can occur, and cyber threats exist that could harm Konecta and its various companies.

This Policy establishes a framework that sets out the principles for ensuring the protection of Konecta's information systems against unauthorised access, loss or damage during information processing or other types of cyber threats, guaranteeing the availability, integrity and confidentiality of the information in the data managed by Konecta.

This Policy is designed to establish the framework for Konecta's internal stakeholders (employees, shareholders, investors, executives) and external stakeholders (customers, suppliers, auditors, governments, regulatory bodies, the media, competitors and financial institutions), enhancing confidence in the company's information systems and ensuring scrupulous compliance with current regulations in each country, internal requirements and international standards.

This Policy will be available on the corporate website (Konecta.com) to ensure that it can be consulted by all interested parties.

02

Scope of application

This Policy falls within the scope of the Compliance Framework Policy and extends to all Konecta entities, backed by the company's senior management.

Consequently, its content is mandatory for all Konecta employees, regardless of their position or role within the organisation or their geographical location.

Notwithstanding the foregoing, its scope of application may be extended, when necessary and possible due to the nature of the relationship, to all individuals and/or legal entities linked to Konecta on a business or professional basis, through a relationship other than employment: suppliers, contractors and workers in the supply chain, and business partners.

Given that many of Konecta's companies have their registered office outside the European Union, internal regulations will be adapted to the regulations of each State where necessary, respecting and ensuring compliance with the basic principles set out herein.

03

General principles of action

The Information Systems Security and Cybersecurity Policy reflects the Company's express commitment to determining and establishing guidelines and adequate support for the administration of the security of the information it handles, in accordance with its own requirements and with current laws and regulations.

Konecta strives to ensure “the secure use of networks and information systems by strengthening our capabilities for prevention, defence, detection, analysis, investigation, recovery and response to cyberattacks” that may occur.

Konecta advocates promoting the secure use of information systems and telecommunications, always in line with the business strategy and objectives. In this regard, it has set the following specific objectives, which are consistent with the context in which the company's activities are carried out:

- Promoting the security and resilience of the networks and information systems used.
- Raising awareness among all company personnel of the risks arising from cyberspace.
- Training and maintaining the knowledge, skills, experience and technological capabilities to support Konecta's cybersecurity objectives.

In this regard, Konecta undertakes to achieve the following objectives:

- Consider information and the systems that support it as strategic assets. Konecta therefore expresses its determination to achieve the necessary security levels to guarantee the confidentiality, integrity and availability of the information processed within the organisation and of the information system resources that process, store or distribute it.

- Ensure the dissemination of the regulations defined in support of this Policy, with the aim of instilling in Konecta's staff a level of awareness and training in information security that guarantees the application of appropriate practices in this area, as an inherent part of the performance of their duties.

- Promote the achievement of the required levels of information security as a continuous process of improvement and constant progress, based on the definition of the objectives and requirements to be met, the implementation of the appropriate processes and measures, the verification of their effectiveness, efficiency and efficacy, and the adoption of the appropriate corrections and modifications.

- This Policy should be the main tool for adequately guaranteeing Information Security, promoting and ensuring compliance within the different services.

- Ensure the existence of the necessary mechanisms to guarantee the continuity of the company's critical activities that are supported by information systems, allowing for their recovery within an acceptable period of time.

- Maximise the quality of services provided.

- Reduce or eliminate, as far as possible, the dangers and risks in the assets, processes and services provided by Konecta.

- Determine essential information security measures that Konecta must adopt to protect itself appropriately against threats that could affect the confidentiality, integrity and availability of information in any way.

The objectives of this Policy will be implemented based on a long-term strategy. Activities to achieve the objectives must be maintained over time.

In line with security risks, action plans must be defined and adjusted each year (security controls, definition of security projects, continuous monitoring, etc.).

The necessary transition plans will be established to reduce any impact on Konecta's activities and/or resources, and Konecta will also ensure that employees:

- … are familiar with and apply Konecta's internal procedures and protocols regarding information security.
- … have tools that allow them to easily access internal operating procedures (Intranet). In addition, alternative communication channels will be used to communicate certain processes, special measures or procedural updates.
- … are aware that they must only process the information for which they have been authorised and use Konecta's assets solely for the performance of their professional duties. Employees must comply with the basic rules for accessing applications and/or equipment with access to personal data.
- … are familiar with the company's existing procedures so that they know how to act in the event of any activity or threat that may affect information security, and must inform the Technology Department and the Chief Information Security Officer (CISO).

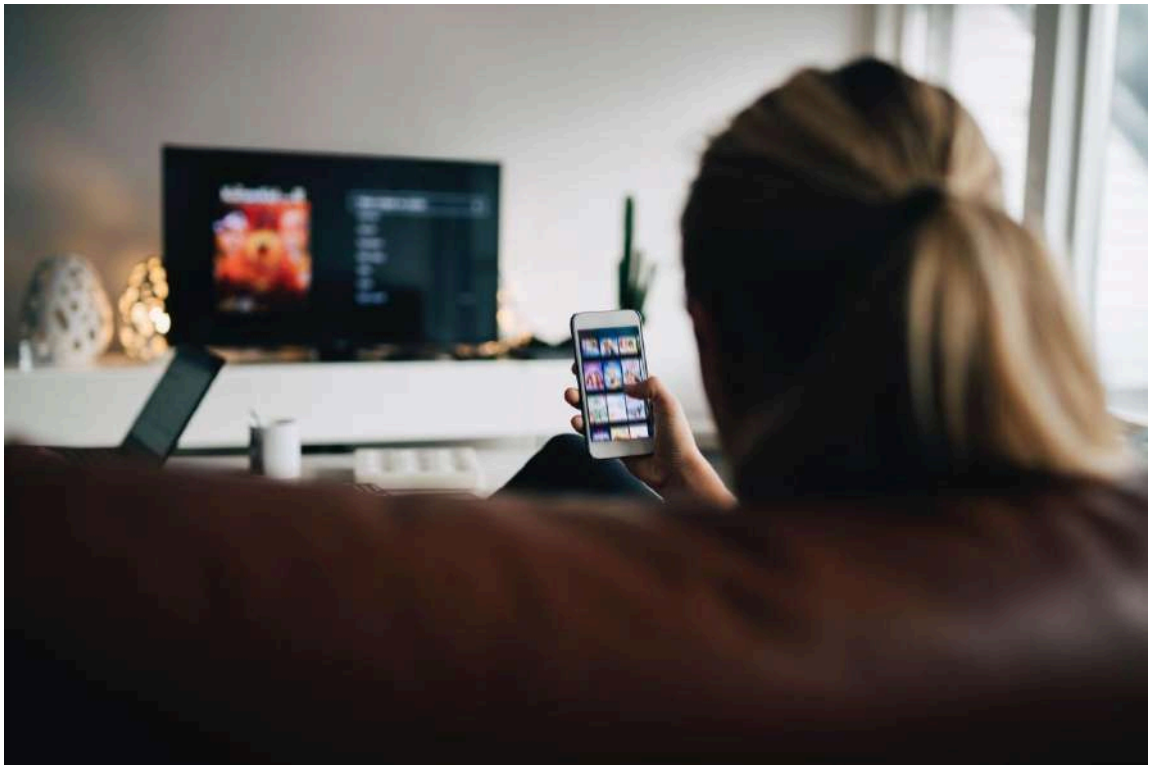
Aware that each of the countries in which the company operates has a different social context and different needs, this Privacy and Confidentiality Policy is articulated through plans and actions related to the principles set out therein, adapted to the reality of each of its local operations.

These principles of action respond to the impacts, risks and opportunities (IROs) arising from the applicable material issues: information security, digital transformation, compliance and corporate ethics, and suppliers' management.

Both employees and any third parties who suspect the existence of any potential breach related to this Policy or to the Code of Ethics, may submit their information, questions or concerns on this matter, confidentially and without fear of reprisals, through the Information Channels available on Konecta's corporate website (https://Konecta.integrityline.com), depending on the nature of the situation, in accordance with procedure PG COR 26 Information Channels, available on the same website, which specifies the different channels available and the nature of the communication that can be made through them.

This channel is available 24 hours a day, 7 days a week. No reprisals will be tolerated against anyone who, in good faith, reports facts that could constitute a breach of this policy, and the guarantees and protections established by the applicable regulations and legislation will apply to those who report.

Failure to comply with this policy will be subject to the corresponding disciplinary measures in accordance with internal rules and procedures, without prejudice to any administrative or criminal penalties that may also result from this and which may be imposed by the competent authority.



04

Updating and revision

This Policy lays the foundations for compliance with the following standards:

- ISO/IEC 27001:2022 Information technology -Security Techniques-Information security management systems - Requirements.
- ISO/IEC 27701- Extension of ISO 27001 for privacy management.
- ISO/IEC 27002:2022 Information technology - Security techniques - Code of practice for information security controls.
- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance).
- Personal Data Protection Laws applicable in each country.

The Information Systems Security and Cybersecurity Policy will be reviewed periodically or when necessary to bring it into line with changes in the business model, the approval of new regulations or international best practices, ensuring its effectiveness and ongoing compliance.

NOTE: This Policy has been approved on December 16, 2025, by the highest governing body and replaces any previous version of it, with only this document being valid from this date onwards.

Version Control

Version	Review date	Reviewed	Validated	Approved	Reason for change
2	06/22/2021	IT_Information Security Organization & Procedure	Legal Affairs	Board of Directors	General Policy Review
3	12/19/2022	IT_Information Security Organization & Procedure	Legal Affairs	Board of Directors	General Policy Review
4	12/16/2025	IT_Information Securityn Organization & Procedure	Legal Affairs	Board of Directors	Alignment with legal requirements Alignment with the new format and branding