

SECURITY AND CYBERSECURITY POLICY FOR INFORMATION SYSTEMS



Madrid, December 19, 2022

Konecta



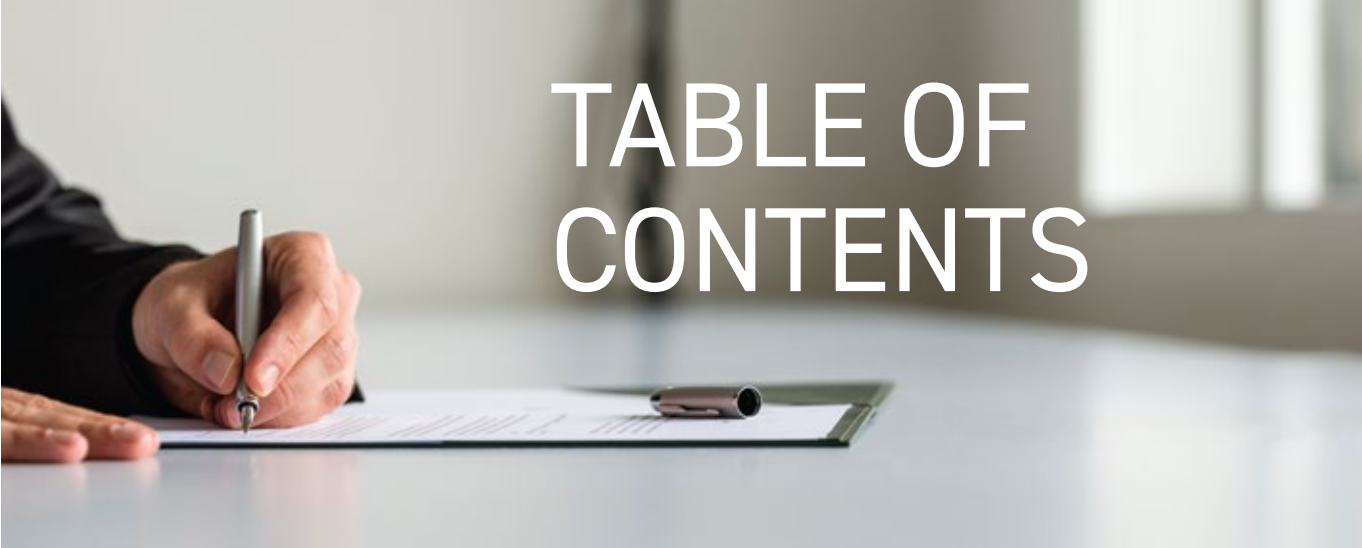


TABLE OF CONTENTS

- 1 PURPOSE
- 2 SCOPE OF APPLICATION
- 3 GENERAL PRINCIPLES OF ACTION
- 4 CURRENT REGULATION AND REVIEW

This Security and Cybersecurity Policy for Information Systems is included within the corporate strategy for the maintenance of Information Security and regulatory compliance by Konecta Group companies (hereinafter Konecta, the Company, or the Organisation), and lays the foundations and principles on the safe use of information systems and telecommunications.

1.- PURPOSE

The purpose of this Security and Cybersecurity Policy for Information Systems (hereinafter the “Policy”) is to ensure the integrity, privacy and confidentiality of information, in accordance with current legislation on the matter, weighing any potential risks and making an efficient use of the available resources, all this based on criteria of proportionality in management.

The massive use of information technology and telecommunications (ICTs) in all areas of society, has created a new space, namely, the cyberspace, where conflicts and aggressions take place, and where cyber-threats against Konecta and its various companies exist.

This Policy establishes a framework that sets out the principles to ensure the protection of Konecta information systems against unauthorised access, loss or damage while processing information, or other cyber-threats, and to secure the availability, integrity and confidentiality of the data managed by Konecta.

This policy is designed to set out the framework for Konecta stakeholders, boost confidence in the information systems of the Company, and ensure strict compliance with current legislation on the subject.

2.- SCOPE OF APPLICATION

This Policy is globally applicable to all Konecta entities and is endorsed by the General Management and the Board of Directors. Each member of the Company is responsible for promoting the principles and commitments contained herein while performing their duties.

Given that many of Konecta Group Companies have their registered office outside the EU, they shall adjust their internal regulations to the requirements and regulations of each State, respecting and safeguarding the basic principles herein outlined, with a view to continuously improve in the respect and protection of the information accessed.

3.- GENERAL PRINCIPLES OF ACTION

This policy reflects Konecta's express commitment to identify and establish appropriate guidelines and support for managing the security of the information handled, in accordance with the specific requirements and applicable laws and regulations.

Konecta seeks to guarantee “a safe use of networks and information systems through the strengthening of our prevention, defence, detection, analysis, research, recovery and response capabilities against the cyberattacks” that may occur.

Konecta advocates for promoting a safe use of information systems and telecommunications, while remaining aligned with the business strategy and goals and, in this line, has set among its following specific objectives remaining consistent with the context in which the Company activities are carried out:

- Boosting the security and resilience of the networks and information systems used.
- Creating awareness among all staff of the company on the risks arising from cyberspace.
- Training and maintaining the knowledge, skills, experience and technological capabilities necessary to support Konecta's goals with regard to cybersecurity.

In this respect, Konecta is committed to achieving the following goals:

- Considering information and the systems supporting it as strategic assets. Thus, Konecta is determined to reaching the necessary security levels to ensure the confidentiality, integrity and availability requirements of the information processed in the organisation, and of the IS resources for processing, storing or distributing said information.
- Ensuring the dissemination of the rules defined in support of this Policy, with the aim of instilling in Konecta's staff a level of awareness and training on IS, to ensure the implementation of good practices in this area, as an inherent part of their functions.
- Promoting the achievement and development of the security levels of information required, as part of a continuous improvement and progress process, based on the definition of the goals and requirements to be met, the implementation of timely processes and measures, the monitoring of effectiveness and efficiency, and the adoption of appropriate corrections and modifications.
- This Policy must be the main tool for properly ensuring Information Security, promoting and ensuring compliance thereof within different services.
- Ensuring that the necessary mechanisms to guarantee the continuity of critical business activities grounded on Information Systems are in place, and allowing for the recovery of information within an acceptable time period.
- Ensuring quality in the services provided.
- Reducing or eliminating, where possible, dangers and risks in assets, processes and services provided by Konecta Group.
- Setting out essential Information Security measures to be adopted by Konecta to protect itself against threats that could affect the confidentiality, integrity and availability of information to any extent.

The goals of this Policy will be implemented under the basis of a long-term strategy. The activities to fulfil these goals must be maintained over time. With regard to security risks, action plans must be defined and adjusted every year (security checks, definition of security projects, continuous monitoring, etc.)

The transition plans necessary to reduce any impact on Konecta's activities and / or resources will be set out to also ensure:

- That staff knows and applies Konecta's internal IS procedures and protocols.
- That the staff understands that they must only process information for which they have been authorised and use Konecta assets solely for the performance of their professional duties. That the staff meets the basic standards of access to applications and / or computers with access to personal data
- That the staff is familiarised with the existing procedures in the company to know how to respond to any activity or threats that may affect Security of Information, in which case, they must inform the Technology Department and the Security Director (CISO).

4.- CURRENT REGULATION AND REVIEW

This Policy provides the basis for compliance with the following standards:

- ISO/IEC 27001:2013 Information technology--Security techniques--Information security management systems - Requirements.
- ISO/IEC 27002:2013 Information technology -- Security techniques -- Code of practice for information security controls.
- PCI/DSS.
- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, concerning the protection of natural persons with regard to the processing of personal data and the free movement of such data and repealing Directive 95/46 /EC (General Data Protection Regulation) (Text with EEA relevance).
- Organic Law 3/2018, of 5 December on the Protection of Personal Data and guarantee of digital rights.

This Security and Cybersecurity Policy for Information Systems shall be reviewed and updated, where necessary, to adjust to the changes experienced by Konecta's business model, or to those resulting from the adoption of rules of direct application, while ensuring its effectiveness and compliance.

NOTE: This Security and Cybersecurity Policy was revised and approved on 19 December 2022 by the Konectanet Group's governing body, S.L.U.