

Information Security Policy

COPA-DATA Group

Public | Version 1.0 | October 2026

Guiding principle and significance of information security

About COPA-DATA

COPA-DATA is an independent, family-owned software vendor headquartered in Salzburg, Austria. Since our founding in 1987, we have been dedicated to making life easier for people working in industrial and infrastructure environments. Our industrial software products - including the zenon software platform and the STRATON runtime system - enable automation, digitalization, and sustainable operations for our customers worldwide, including global leaders in the energy as well as in various manufacturing industries.

As a trusted technology partner, we understand that our customers rely on us to protect not only our own critical data and processes but also the sensitive information they entrust to us. Information security is therefore not just an operational necessity - it is fundamental to maintaining the trust that our customers, partners, and stakeholders place in us.

COPA-DATA operates as an international Group with its headquarters in Salzburg, Austria, and subsidiaries across Europe, North America, the Middle East, and Asia-Pacific. Product development is centralized at the headquarters, while the subsidiaries focus on sales, customer services, and local market development. Straton Automation SA, based in Échirolles, France, additionally develops the STRATON soft-PLC runtime. All Group companies operate under a unified Information Security Management System, as defined in the ISMS Policy Scope Document.

Our Vision for Information Security

Business-aligned information security - enabling innovation, usability, and trust.

COPA-DATA's mission is to make life easier for people working in industrial and infrastructure environments. Our information security vision supports this mission: we maintain a business-aligned level of protection that safeguards our business operations, intellectual property, and customer data - while preserving the usability and innovation that define our products and services. By integrating security into our business processes and software development, we protect the trust that customers, partners, and stakeholders place in us and ensure the long-term resilience and competitiveness of our company.

Strategic Objectives

To achieve our vision, COPA-DATA pursues the following strategic information security objectives:

- Establishment of a uniform COPA-DATA Group Information Security Management System (ISMS)
- ISO 27001 certification for all companies and locations within the COPA-DATA Group
- TISAX label for defined locations with customers within the automotive industry
- Continuous improvement of our security culture

Core Principles

The ideas, expertise, and intellectual property of our employees are the foundation of our success. The availability and reliability of our software solutions, IT infrastructure, and digital services - as well as our responsiveness as a partner - reflects our commitment to customers and business partners and contributes significantly to the reputation of COPA-DATA. To protect these values, we maintain a worldwide, business-aligned level of protection for the confidentiality, integrity, and availability of our processes, information, and systems.

The declared corporate goal of effectively protecting central business processes, including our software development environments, customer data, source code, and IT systems, is met by creating globally valid security standards and integrating information security into internal processes. The defined information security objectives contribute directly to the achievement of the company's goals.

Information security is a shared responsibility - every employee is expected to act in a security-conscious manner and to report potential vulnerabilities or incidents without delay.

Our expertise, our advantage

Care and accuracy in handling information

Need-to-know principle

COPA-DATA fosters an open and collaborative communication culture. Every employee is responsible for handling information in accordance with its classification level and ensuring that access - whether physical, digital, or through IT system authorizations - is granted and maintained appropriately.

Correct handling of information

The secure handling of business and customer data is a core responsibility of every employee. Information must be treated in accordance with its classification level throughout its entire lifecycle - from creation to disposal.

Technical security

COPA-DATA invests in the secure design and continuous improvement of its IT infrastructure, software development environments, and premises. Technical measures are a key element of our security strategy, with a particular focus on protecting our most critical systems and data assets.

Own responsibility

Information security is a shared responsibility at all levels of the organization. Every employee is expected to comply with applicable security policies and to report vulnerabilities, suspicious situations, or incidents without delay. Managers are responsible for ensuring awareness and compliance within their teams. The effectiveness of implemented measures is regularly reviewed based on audit results, management assessments, and operational experience.

Implementation

The company uses an Information Security Management System (ISMS) based on the international standard ISO/IEC 27001 to ensure the implementation of information security requirements. The ISMS follows the recommended continuous improvement process based on the PDCA model (Plan, Do, Check, Act). The aim is to verifiably and regularly ensure the adequacy, completeness, sustainability, effectiveness and efficiency of the implemented information security processes and protective measures.

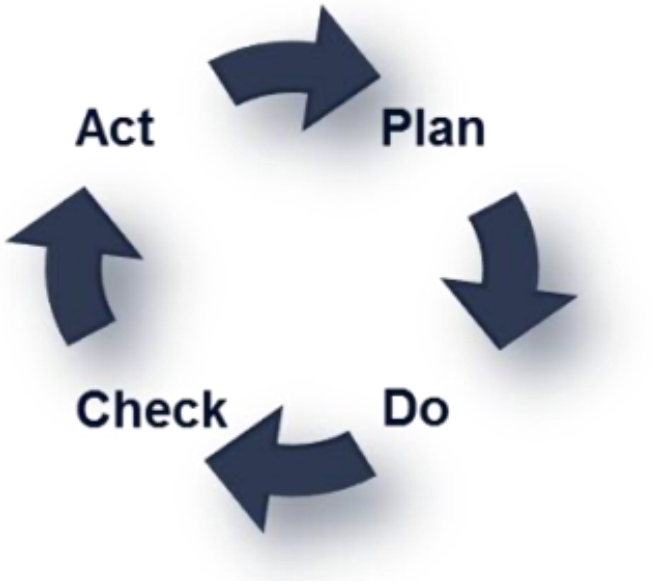


Figure 1: PDCA-Model

PLAN - Determining the ISMS

The strategies, goals, processes, regulations, procedures, methods, tools, and responsibilities of the ISMS are determined.

DO - Implementation and execution of the ISMS

The defined processes, regulations, and procedures are implemented according to the objectives of the ISMS. Selected measures are implemented.

CHECK - Monitoring and reviewing the ISMS

Based on practical experience, the results of audits and management assessments, the processes, effectiveness and efficiency of the selected approaches and measures are measured and reviewed. It is identified whether there is a need for action and where there is room for improvement.

ACT - Maintaining and improving the ISMS

Based on the results of the phase check and other feedback (e.g. current risk situation / threat situation / further developments / requirements), corrective and preventive measures are taken, which lead to a continuous improvement of the ISMS and the security level. The handling of security incidents is another task of this phase.

Management commitment and support

Management endorses and actively supports information security as a strategic objective for the COPA-DATA Group. Together with the Information Security Management Team, management drives the establishment, maintenance, and continuous improvement of a business-aligned level of information security and ensures that adequate human, organizational, and financial resources are provided.

COPA-DATA is committed to satisfying applicable legal, statutory, regulatory, and contractual requirements related to information security.

Final provisions and scope

This policy applies to the entire COPA-DATA Group, including all subsidiaries and offices worldwide. It is binding for all employees, contractors, and third parties who have access to COPA-DATA information or systems. This policy is communicated to all employees and is part of the mandatory onboarding process for new employees.

This policy is supported by detailed internal policies, processes and guidelines covering areas such as risk management, incident response, IT emergency management, audit management, and employee awareness. These internal documents provide specific operational guidance and are regularly reviewed and updated.

Unless otherwise indicated, all supporting guidelines have the same scope as this policy and are valid from the date of their publication. Country-specific or site-specific legal and organizational requirements are addressed in supplementary local regulations where necessary.

The scope of application of the underlying ISMS is centrally defined and documented separately.

Violations of this policy may result in disciplinary action up to and including termination of employment.

This policy is reviewed at least every year or when significant changes occur and updated as necessary.

This Information Security Policy has been reviewed and formally approved by the COPA-DATA Executive Management and is published on their behalf, reflecting management's full commitment to information security across the COPA-DATA Group.

© Ing. Punzenberger COPA-DATA GmbH