Information Security Statement

	Function	Name	Signature
Author	ISMS Manager	Maurizio Di Donato	Maurizio DI DONATO Maurizio DI DONATO (09/giu/2025 10:29 GMT+2)
Review	CIO	Stefano Boscolo	Stefano Boscolo Bozza (09/giu/2025 05:32 ADT)
Approval	CEO	Pietro Gorlier	Pietro GORLIER (09/giu/2025 09:58 EDT)

Document Name	G_PL_01 Information Security Statement.docx		
Approval Date	09/06/2025	Version	1.5
Document Classification	C2 Internal	Pages	8

Document Version History

Version No.	Version Date	Summary of Changes
1.0	21/12/2020	First version of the document (derived from the old POL-01)
1.1	24/01/2022	Annual revision and some editorial changes
1.2	22/09/2022	Change of approver due to change of CEO
1.3	10/03/2023	Annual revision and some editorial changes
1.4	31/01/2024	Annual revision and some editorial changes
1.5	09/06/2025	Annual revision and some editorial changes

Terms and Definitions

For the purposes of this document, the Acronyms and Definitions are given in the *G_STD_00 "Acronyms and Definitions".*

References

Document Code	Title
G_PR_01	ISMS Document Management

Document Distribution and Classification

This document is intended for internal use only and the information it contains are classified to be "**C2 Internal**" (please refer to the document *G_PR_01 "ISMS Document Management"*).

Basing on that classification, the document is available for the usage inside the Company and can be shared outside the Company under authorization of the ISMS Manager.

Summary

1 Purpose

Comau considers the information assets protection a primary aspect for the safeguard and the continuity of its business and of its customers business.
The purpose of this document is to define the general criteria, roles and responsibilities for an effective information security management.
This statement has been approved by CEO and represents Comau commitment on Information Security.
Information Security Statement and Policies are valid for all Comau within the Information Security Management System scope: compliance with them is considered mandatory.

2 Basic Principles

Comau attributes primary importance to information security in consideration of:

- the increasing vulnerability determined by the increased dependence on information systems and services.
- the increase of difficulties in achieving effective control of access to information, caused by the interconnection of private and public networks, as well as by the sharing of information resources.
- the increased use of distributed architectures
- the awareness of the limited effectiveness of "security", if pursued exclusively with technical measures but not supported by policies, organizational and operational practices

The purpose of Information Security for Comau is to preserve:

- information assets, functional for providing services to its relevant interested parties.
- information entrusted to Comau by its relevant interested parties, from all threats, whether internal or external, deliberate or accidental

2.1 Objectives

Comau Information Security System is designed to achieve the following objectives:

- protect the interest of stakeholders, employees and third-party.
- ensure compliance with applicable laws and regulations.
- ensure a standard model for corporate information protection and the management of related risks.
- guarantee a proper corporate information protection and the continuity of business processes, based on the level of confidentiality, integrity and availability requested.
- minimize the business risk by preventing and minimizing the impact of information security incidents.
- retain documentation of the designed and implemented systems.
- retain evidence of the authorization processes and of the performed activities as required by business functions.

Those objectives are pursued through:

- the application to systems designs and implementation of the best standard currently available to protect information assets to ensure compliance to relevant legislation on information processing and the required level of:
  - Confidentiality (information is accessible only to authorized individuals or systems)
  - Integrity (information and processing methods have to be accurate and complete)
  - Availability (information must be available and usable as required by business processes)
- The establishment, implementation, operation, monitoring, review, maintenance and improvement of an effective Information Security Management System (ISMS) for the specific scope of certification.
- In addition to the objectives described in this policy, those defined annually in the management review are integrated, measured by the ISMS Manager, and evaluated by the Management.

3 Roles and Responsibilities for Information Security

3.1 Comau

- Defines the reference model and behavioral rules for the Information Security to which all Comau Legal Entity must adhere.
- Defines and communicates the Information Security policies and the minimum protection standards to be adopted at subsidiaries companies.
- Defines general criteria for roles and responsibilities for information security management at Comau Legal Entity.
- Promotes assessment and audit activities to verify the proper information security Annex and guidelines application and the effectiveness of the security measures implemented.
- Considers the risks of climate change for information security and the effects of business on the environment.

3.2 Chief Executive Officer (CEO)

Chief Executive Officer promotes the definition and the implementation of an adequate system of information protection and management. CEO delegates the definition, implementation and monitoring of the information security system to CISO, Managers and Users based on their roles.

3.3 Chief Information Officer (CIO)

Chief Information Officer is accountable for providing the overall strategic direction and leadership for the ICT department. This includes developing strategic ICT plans that align with overall company strategy to reduce overall costs and promote business development; collaboration, communication, and relationship management with a range of relevant interested parties; and oversight of all ICT operations and initiatives.

3.4 Chief Information Security Officer (CISO)

The Chief Information Security Officer performs two core functions for the enterprise. The first is safeguarding information system assets by identifying and solving potential and actual security problems and overseeing the operations of the enterprise's security solutions. The second is establishing an enterprise security stance through policy, architecture and training processes. Secondary tasks will include the selection of appropriate security solutions, and oversight of any vulnerability audits and assessments. Chief Information Security Officer reports to Chief Information Officer.

3.5 Information Security Management System Manager (ISMS Manager)

ISMS Manager has the following responsibilities:

- defining and updating of the Information Security Annex and guidelines.
- designing the information security system and preparing plans for its implementation.
- coordinating the information security system implementation.
- monitoring the implementation of information security systems and of protection measures on information system assets.
- promoting training, awareness and communication initiatives and programs on Information Security.
- promoting audit and assessment activities for the continuous monitoring of the adequacy and effectiveness of the information protection system.
- reporting to Management the status of information security system, plans, actions and issues.

The ISMS Manager operates in collaboration with Human Resources and Legal departments.

The ISMS Manager is also responsible for:

- designing the ISMS and preparing plans for its implementation.
- coordinating the ISMS implementation.
- maintaining and monitoring the ISMS.

Information Security Management System Manager reports to Chief Information Officer.

3.6 ISMS Team

The ISMS Team, reporting functionally to ISMS Manager, have the following responsibilities:

- supports the ISMS Manager in maintaining and improving the ISMS.
- support the business owners and business departments, on information classification and information security issues.
- support the end users for topics included in the ISMS scope and perimeter.

3.7 ISMS Focal Point

The ISMS Focal Point is the person appointed from Direct Manager, with approval of the ISMS Manager, that is responsible for managing the various ISMS scope and/or perimeter sections; the ISMS Focal Point responsibility could be intended, depending on ISMS scope and perimeter:

- geographically at a country level.
- logically at a process level.

The ISMS Focal Point is the unique contact point between ISMS Manager and the process or country he represents; he collects all the ISMS issues related to his context and if feasible, treat them autonomously; otherwise, he informs ISMS Manager in order to build a shared action plan; in any case the ISMS Focal Point informs periodically the ISMS Manager about ISMS activities related to his context.

The ISMS Focal Point works jointly with the ISMS Manager for the following ISMS Activities:

- Country - Specific or Process - Specific documentation issuing.
- Risk Analysis.
- Internal Audit.
- Certification Audit.

3.8 Functional manager

Comau functional managers are required, according to their own responsibilities, to apply and monitor the implementation of all the rules regarding information security and to report to the ISMS Manager any issue on information security status (e.g.: security breaches, violation of policies or procedures, progress of compliance with security measures, …).

They are also required to inform suppliers and consultants, which perform activities on behalf of Comau, of the protection guidelines and procedures that need to be respected for information processing.

3.9 Users

Users process the information based on specific authorization profiles and privileges. Users are responsible for adopting behavioral measures defined by the Company through the Information Security policies.

4 Information Security Management

The effectiveness of the information security management is based upon:

- the definition of a set of policies, that are the guidelines relevant to managing risk and improving the information security.
- the implementation and operation of controls and actions to ensure information assets protection according to security requirements.
- a periodic process for managing and reporting information security risks.
- periodic audit activities performed to review the adequacy of the controls and effectiveness of the information security system to ensure its continual maintenance and improvement.

4.1 Policy

Information Security policies set the guidelines that govern Comau Information Security and to which all employees and third parties must comply to ensure protection of Comau information assets. CEO is responsible for ISMS Information Security policies approval.

4.2 Risk Management

Comau defined a systematic approach to risk management in order to identify, analyze, evaluate and manage risks related to the Confidentiality, Integrity and Availability of protected information. ISMS Manager is responsible to drive the periodic risk management process.

4.3 Reporting

ISMS Manager, in the ISMS Management Review process, reports to CEO, CIO and CISO on the adequacy of the protection system and, on the progress of implementation plans. ISMS Manager also reports information security audit results.

5 Audit

Periodic audit activities are planned and performed on information security and Information Security Management System to:

- review the adequacy of controls and the effectiveness of the information security management system identifying possible improvements.
- check the adequate implementation of policies and rules, identifying possible critical situations.
- report to CEO, CIO and CISO of Comau relevant information security issues.
- verify the effectiveness of information protection systems.

Information Security Audit activities are coordinated by ISMS Manager.