



# Information Security Policy

## 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 summarize and present the basic principles and objectives for an effective information security management.

This policy is an abstract of Information Security Statement 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.

## 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

## 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.

DOCUMENT NAME	INFORMATION SECURITY POLICY ABSTRACT	1
DOCUMENT TYPE	POLICY	
CLASSIFICATION	C1 PUBLIC	