



Version 5.0

Information and Cyber Security Policy

What we do to protect the confidentiality, integrity, and availability of all information entrusted to our organization.

Created on February 22, 2026

Public

Executive Summary and approval

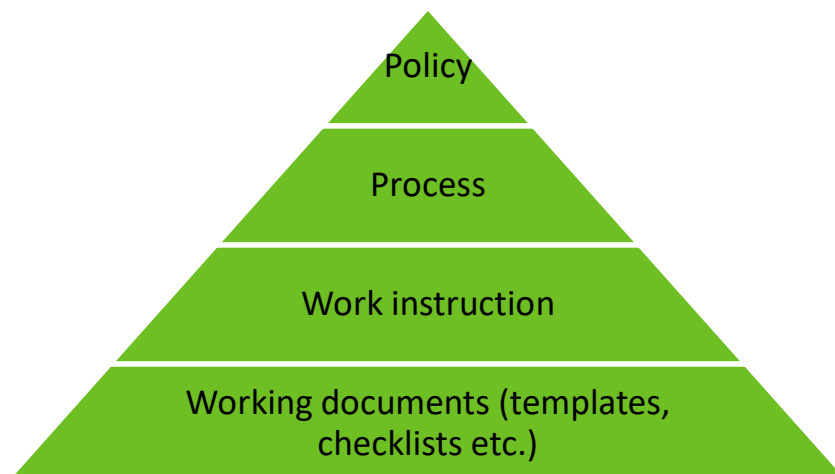
At VAT, we change the world with vacuum solutions – that is our purpose as the world’s leading developer and manufacturer of leading-edge vacuum valves. We are committed to conducting business with the highest standards of confidentiality, integrity and availability for information.

Our company's internal assets, such as expertise, plans, product documentation, and strategic projects, are crucial to VAT's success. We must prevent these assets from being always disclosed to unauthorized individuals.

To do this, we need to conscientiously safeguard these assets. This includes not only technical security measures but also the responsibility of every employee and contractor to adhere to related policies and work instructions. This collective effort helps ensure the strongest protection of our valuable information.

For our security measures to be effective, it's essential that all staff, whether internal or external, understand what's required of them. They should set an example whenever possible and continuously seek ways to enhance our security processes. This proactive approach helps protect our assets and close any potential security gaps.

The Information Security Policy is part of VAT’s Process Hierarchy. It complements and is supported by other internal policies and work instructions, notably the Data Privacy Policy and the Employee Manual, along with all its appendices.



The information & cyber security policy (PIT_PO_014) has been approved by the GEC on February 1st, 2026, and replaces all previous versions.

Group Executive Committee

March 1, 2026

General

This policy shall improve the awareness of our employees for the threats of cybercrime and help them contributing to minimize VATs risks arising from any acts of cybercrime.

Target and Motivation

In every aspect of VAT's operations, information processing and technology are crucial for task completion. All vital strategic and operational functions are significantly supported by Information and Communication Technology. Without secure and efficient information processing, VAT's operations would be impossible.

During business transactions, various types of information may emerge or be provided by third parties (customers, suppliers, etc.) that are deemed confidential. Unauthorized disclosure or publication of this information could harm VAT or third parties.

This information can take many forms, such as documents, printouts, emails, passwords, development, and CAD data, among others.

Information is one of VAT's most valuable assets (akin to capital, value, strength, investment) and must be protected as any other critical business component. This is increasingly important in our interconnected world, where information faces more threats and vulnerabilities.

Beyond ensuring the utmost protection of data, it's also crucial to provide access to data based on each user's specific access rights.

Group IT is tasked with the operation and maintenance of IT systems.

The aim of this policy is to offer guidance and support from the Group Executive Committee (GEC) on information security. This aligns business needs and relevant laws and regulations to safeguard company data in terms of availability, confidentiality, and integrity.

The Group Executive Committee (GEC) provides clear guidance on principles that align with our business objectives. The GEC supports and is committed to information and cyber security through the organization-wide publication and maintenance of this policy and supporting work instructions. To mitigate risks resulting from insufficient IT security, we maintain clear and comprehensible information-security requirements aligned with VAT's Enterprise Risk Management. These requirements aim to reduce the likelihood and impact of, among other things:

- data protection breaches
- confidentiality breaches
- legal non-compliance
- copyright violations
- adverse internal or external influences
- operational disruption and inability to perform required tasks
- production outages
- financial damage

This Information Security Policy is based on the ISO/IEC 27001: 2022 standard. This framework contains general principles for initiating, maintaining and continually improving appropriate security management.

Scope

The Information Security Policy applies to all VAT employees and contracted parties working on behalf of VAT with access to information. All must comply with these guiding principles and apply to all legal units which are fully consolidated.

The policy concerns both digital information - and thus also the electronic devices suitable for processing and transport - as well as analog information and media (e.g. paper), which contain information that is considered worth protecting.

When working with third parties, it is important to ensure that this policy including associated policies and work instructions are applied.

Summarized:

- All employees must handle the VAT's information assets responsibly
- The responsibility for information security lies with the respective superiors of an organizational unit and with the process owners
- Group IT supports both the Heads- of and the employees in complying with information security requirements

This document applies in the currently published form and replaces the version from January 2025.

Organization and responsibilities

The Information & Cyber Security Office manages, coordinates and is responsible for Information Security Management within VAT and is supported locally by the respective defined contact persons. If no contact person is defined locally, the respective local managing director is the first point of contact for the Information & Cyber Security Office.

The Information & Cyber Security Office supports the Head of IT, the Head of Legal & Compliance and, if necessary, the Data Protection Officer in all matters relevant to information security.

Tasks of the Information & Cyber Security Office see Appendix A

Regulations

Security Objectives

VAT Group is ISO / IEC27001:2022 certified and pursues the following security objectives within the framework of information security and in coordination with ISO / IEC2700x.

- The availability of information and systems is secured in such a way that the expected downtime is minimized and can be tolerated. Downtimes that can lead to major work delays or missed deadlines should be avoided by taking appropriate measures.
- The requirements for integrity and confidentiality are based on both legal compliance and the internal requirements on the confidentiality of any information.
- The dual-use requirements must be emphasized - this requires appropriate security and confidentiality measures.
- The requirements of data protection must be fully met when processing personal data. The measures must be in an economically justifiable ratio to the value of the information to be protected. Damages with a high financial or immaterial impact must be prevented.
- Access to information is limited by the need-to-know principle. In new systems, this authorization option "by design" must already be provided. In addition to protecting the IT infrastructure - networks, servers, personal computers, software - buildings and premises must also be adequately protected.
- VAT's reputation in public depends crucially on high reliability. Information & Cyber Security measures must be taken to counteract a loss of trust.

Strategic Direction

To achieve the set security objectives and continuously improve the security level of VAT, a documented information security management system (ISMS) is defined, implemented, monitored, checked, maintained, and improved.

The scope of the Information Security Management System (ISMS) encompasses the entire VAT group, its products and services, and all associated employees, processes, and contracted parties. This includes all information and data that is collected, processed, or utilized.

Based on the results of the Information & IT Risk Analysis, appropriate measures and precautions must be taken to avoid fines, penalties and recourse claims as well as to avert material and immaterial damage from VAT and thus to reduce risks.

The security awareness of VAT employees is continuously maintained and developed through appropriate training and awareness-raising measures on topics relating to information and cyber security as well as corresponding guidelines, work instructions and other regulations. Information and cyber security are a holistic and strategic task that requires responsible and committed action from all employees. This applies in particular to the reporting and handling of information security incidents.

This information and cybersecurity policy is supported by further policies and operationalized by concrete process descriptions and work instructions.

The measures to achieve the security goals are managed in the ISMS and include the following categories:



Personal Responsibility

All employees and contracted parties are required to protect information assets and ensure a level of information and cybersecurity appropriate to the required level of protection by complying with all applicable information security policies, procedures, and work instructions.

Responsibility for information and cybersecurity is shared across the organization and applies to all employees, regardless of role, function, or position. Each individual is accountable for maintaining information security within their area of work and influence.

Employees and contracted parties are required to promptly identify, report, and respond to information security incidents, weaknesses, or nonconformities in accordance with established procedures and escalation processes.

To maintain and improve safety awareness and the corresponding qualifications, employees and contractors must participate in all cyber security training to which they have been invited.

All employees shall identify and report risks within their area of responsibility and, where applicable, participate in risk treatment activities and propose appropriate improvement measures.

Heads of business units and assigned Process and Data Owners are responsible for enforcing and monitoring compliance with the defined requirements among all employees and external contractors under their responsibility.

.

Data Handling

The secure handling of sensitive business information and personal data by VAT is ensured by the following measures:

- The requirements mentioned under “Personal responsibility” are fulfilled.
- The processing of personal data is carried out in accordance with the internal data protection policy (MRC_PO_019)
- Contracts with all suppliers, customers and other partners include a corresponding obligation to protect confidential information (MRC_TL_003, MRC_TL_004)
- All business processes are strictly organized according to our PMS in accordance with ISO 9001
- Information must be declared, labelled, and treated according to the Policy Classification of Documents (MRC_PO_022)

These measures help to ensure a high level of security and confidentiality when handling important information and to protect the integrity of data within VAT.

Measures in the event of violation

Actions that are violations of the requirements of this policy and corresponding policies, work instructions and other regulations are:

- Actions that compromise the security objectives related to information about employees, customers, contractual partners, or the facilities and systems of VAT.
- Actions that cause actual or potential material or non-material damage to VAT by breaching security.
- Actions that allow unauthorized access to information or enable their disclosure or unauthorized alteration.
- Actions that result in compromising the reputation of VAT.

Non-compliance with internal policies and applicable regulations may lead to substantial adverse consequences for VAT. Violations may result in disciplinary and labor law measures in cases of willful misconduct or gross negligence, and may also give rise to civil or criminal liability.

These principles shall be established and documented as part of a defined disciplinary process.

Implementation controlling

Control of Implementation aims to achieve standards and transparency in IT security as uniformly as possible. The implementation status of IT security measures is documented by the Information Security Office and is regularly presented to the Head of Legal & Compliance, the Head of IT, the Data Protection Officer, and to the GEC.

The effectiveness of the policy, as well as the organizational and technical measures, are periodically reviewed (at least annually) and adjusted as necessary and sensible.