

Introduction

Comer Industries Corporation (hereinafter *the Company*) considers information security and the protection of information to be fundamental principles for achieving business objectives. Therefore, the Company is committed to ensuring that data, information, and the associated data systems, especially those with strategic value for the business, are protected with security mechanisms commensurate with their value and the risks to which they are subjected.

This Policy is applicable to all Group companies and subsidiaries and extends to third parties and suppliers acting on behalf of the Company.

Policy objectives

The Company strives to protect information from any possible threat, internal or external, deliberate or accidental, and puts in place strategies, processes, roles, and responsibilities to ensure the security of the strategic and personal data of all those involved: employees, customers, suppliers, and partners. Specifically, the Company has defined and approved a cybersecurity governance model, including roles and responsibilities for internal reporting and supervision, as well as external regulatory reporting. The application of this Policy is part of the broader framework of corporate strategy and allows the Company to align business processes and procedures with information security standards and all applicable legal and regulatory requirements. This Policy is to be reviewed annually and whenever necessitated by significant security events or changes to Company objectives.

Policy measures

With the aim of achieving these objectives, the Company voluntarily adopts and continuously evaluates the effectiveness of an Information Security Management System (hereinafter *ISMS*) based on ISO/IEC 27001 standards aimed at achieving the following objectives:

- identification of risk areas and adoption of appropriate treatments;
- compliance with regulatory requirements regarding data protection and information security in the countries where it operates (i.e. GDPR and NIS2);
- compliance with applicable contractual requirements;
- widespread awareness of the strategic value of security and information protection systems.

Best practices derived from ISO/IEC 27001 and the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF) are leveraged for the protection of information by applying the security methods deemed most appropriate to ensure the confidentiality, integrity, and availability of business information and systems (hereinafter, *assets* or *information assets*), ensuring an adequate level of protection when risks cannot be avoided. Assets include both traditional IT systems and Operational Technology (*OT*), i.e., production and manufacturing machinery with connectivity and/or information processing capacity. The ISMS is based on a set of procedures, tools, and practices for the protection of information security assets.

All employees are responsible for complying with and supporting the ISMS in their specific capacities, and violations are subject to disciplinary action, as defined in Company policies.

The Company's Board of Directors is the ultimate owner of information security risks and is accountable for compliance with regulations – as such, administration and management bodies are actively involved in the governance of information security risks and is regularly updated during management reviews on the state of information security.

To verify the effective implementation of this Policy, information security is included in the Company's internal audit program and is regularly assessed. The results of audits and assessments are reported to Company's Board of Directors and used to define corrective and improvement actions.

Policy Requirements

The following section lays out the requirements that must be respected to achieve the objectives defined above.

Asset Management: the Company must identify and maintain visibility over all information assets to protect their confidentiality, integrity, and availability. Therefore, every employee is responsible for adhering to procedures that accurately assess new assets for information security, ensuring these assets are properly inventoried and managed throughout their entire life cycle:

- All information assets, including those provided or managed by third parties, are identified, properly installed according to Company procedures and recorded in an inventory;
- Assets are managed throughout their entire lifecycle, from creation or acquisition to use, maintenance, update, physical transfer, and eventual disposal. All related activities are documented and subject to approval.

Data Protection & Management: Company data must be protected. All users are responsible for categorizing the information they produce and handling information according to its classification:

- All data and information are classified based on their sensitivity and handled and protected according to Company procedures;
- Sensitive data that is transferred or stored on a device or media must be adequately protected and encrypted according to Company procedures;
- The Company protects data through regular backups; all employees must ensure that they use appropriate company technology that is included in such backups;
- Data is destroyed securely when no longer needed, according to Company procedures.

Identity Management, Authentication & Access Control: ensuring that only authorized users can access information assets is one of the fundamental ways the Company protects these assets:

- Mechanisms to identify users (e.g., username) and ensure authenticity (e.g., password), which must be strictly protected, are utilized to protect access to all Comer Industries information assets.
- Usernames must be nominal, i.e., associated with a physical person, unless in exceptional cases for which specific approval and additional controls must be implemented;
- The Company must ensure the proper assignment of privileges and grant users the minimum rights required to perform their activities (principle of least privilege). Privileged access (e.g. system

administers and other users with special privileges) must be especially strictly controlled and monitored;

- Additional authentication factors (multi-factor authentication) are implemented to protect high-risk company information assets;
- All users must ensure that access is removed when no longer needed, especially in the case of departing employees, temporary contractors, employees who change departments, etc.

Incident Management, Operational Continuity, Disaster Recovery, Crisis Management: the Company must be properly prepared to respond and recover in the most effective way possible:

- An information security incident management plan is defined, implemented, approved by the management, tested, and periodically reviewed;
- All employees, contractors, and third-party users must promptly report any observed or suspected information security incidents;
- Each security incident is analyzed to identify lessons learned and define and implement the necessary improvement actions;
- Timely reporting is done to the competent supervisory authorities by designated individuals, in accordance with applicable legal and regulatory requirements and timelines.
- Information security events are included in the Company's emergency and crisis management process. Backup, business continuity, and disaster recovery plans are defined, tested, and updated;
- The Company monitors relevant third-party and regulatory communication channels.

Information Risk Management: to meet business objectives, the Company follows a risk-based approach to managing information security:

- A risk management plan is defined and implemented, providing a documented cyber risk assessment of individual systems performed at least every two years, which considers internal and external threats, vulnerabilities, likelihood, potential impacts, and dependencies on third-party suppliers and partners.
- Risk treatment actions are defined and documented within a dedicated risk treatment plan.

Human Resources Security: selecting the correct people for key roles and building information security awareness are vital to ensure employees have the tools necessary to support the protection of Company information assets:

- New hires must formally acknowledge and review the present document - the Integrated Information Security Policy - as part of their onboarding process;
- All Company personnel must possess essential information security competencies. The Company develops these by designing and conducting awareness and training activities according to the approved plans;
- Personnel employed in IT-related roles, particularly those with administrative access to systems as well as business applications, are identified following an assessment of their experience, skills, and reliability.

Physical and Environmental Security: physical security procedures are defined for all Comer Group locations to ensure that Company-wide practices are adopted to physically protect information assets. All employees must follow physical security guidelines, which include:

- Perimeter access (external doors and access points) is controlled by preventing unauthorized access, and each entry should be verified, monitored, and logged;
- Sensitive information on hard copies should be locked away and destroyed securely;
- Desks must be free of sensitive information, and computer screens must be locked when unattended;
- All information systems and equipment must be physically protected proportionally to their value to the Company.

Supply Chain Security: ensuring the security of the supply chain is fundamental to ensuring that Comer Industries systems, data, and business processes function as expected. All employees must support the Company in ensuring that information security aspects of the supply chain are managed, from onboarding and service delivery to renewal or eventual termination of activities:

- An inventory of suppliers is established and maintained, containing the information necessary to identify those relevant for information security purposes;
- Information security risks associated with suppliers and supplied services are periodically assessed, starting from the supplier identification phase;
- Information security requirements applicable to suppliers are defined in a manner proportionate to the identified risks, to guide supplier selection and ensure compliance with Company and regulatory requirements (vendor qualification);
- Supplier agreements include obligations to promptly notify the Company of information security incidents that may affect the confidentiality, integrity, availability, or resilience of the services or information assets provided
- Contractual clauses are included in supplier agreements, requiring suppliers to comply with the defined information security requirements.

Technical Measures for Protecting Systems and Networks: systems require security measures commensurate with the value of the assets. The introduction of systems and assets requires collaboration with the IT and cybersecurity organizations to determine technical configuration and controls:

- New technologies, including IT applications and manufacturing systems with data processing capabilities, interfaces, or network connectivity, must be evaluated for security and privacy by design and configured according to Company procedures and secure development standards. Information and systems outside the standard package of approved software must be installed and configured in conjunction with Company IT personnel;
- Assets are monitored for vulnerabilities, i.e. known software deficiencies or misconfigurations, which must be properly identified and mitigated according to a risk-based approach;
- Protection measures are put in place to ensure the proper functioning of information systems, including removing unnecessary functionalities, protection of endpoints, lifecycle management of hardware and software, backups, and logging;

- The Company must ensure that its networks are designed to limit the potential impact of security incidents through segregation and segmentation, implement up-to-date network security systems such as firewalls that control network traffic, and maintain inventories of networking devices and systems;
- Remote access to networks must be protected, for example via logging and multi-factor authentication. Any Company employees or third parties who access systems remotely must do so via secure channels and strong authentication, such as a second factor;
- Event logging and monitoring: systems are continuously monitored to detect anomalies, which are analyzed to identify potential security events according to Company procedures.

The Company undertakes to spread the principles of this Policy by using internal and external communication channels.

Approval of Policy

PRESIDENT and CEO: Matteo Storchi

Date:

August 2026

Signature:

