SPECIALCAVI

WE BRIDGE PEOPLE

ISO 27001

Information security policy

Information Security Policy

Contents

Introduction

Specialcavi Baldassari S.r.l. is a leading manufacturer of special cables based in Capannori, in the province of Lucca. Founded in 1990, the company has constantly innovated and expanded its production capabilities, becoming a benchmark in the sector thanks to the quality and reliability of its products.

The company offers a wide range of cables for multiple applications, including data transmission, audio-video, mobile applications, and civil and industrial uses. Specialcavi Baldassari stands out for the high quality of its products, guaranteed by the selection of the best raw materials and the continuous updating of production technologies. The cables produced undergo rigorous quality controls in accordance with Italian, EU, and international regulations.

Commitment to data security

A crucial aspect of Specialcavi Baldassari's work is its commitment to data security. The company adopts the latest technologies and protocols to ensure that customer data and internal processes are protected from any threat. This commitment is reflected in its information management practices and the certifications it has obtained, which ensure the highest level of protection and integrity of the data processed.

Ethics and Transparency

Specialcavi Baldassari operates with high ethical standards, promoting honest and transparent behavior in all its processes. This ethical approach extends to data management, ensuring that all information is treated with the utmost confidentiality and security.

Global presence and customer satisfaction

Thanks to a network of relationships based on mutual trust, the company serves thousands of companies in over 30 countries around the world. Specialcavi Baldassari aims not only to be a reliable supplier, but also an excellent partner, offering high-quality pre- and post-sales support to fully meet customer needs. Thanks to its dynamic nature, the company has always been able to offer customized solutions for the most diverse customer needs. Thanks to this characteristic, Specialcavi Baldassari has always managed to maintain a stable and high-level position in the market, even in relation to larger and more important competitors.

Specialcavi Baldassari's Information Security Management System defines a set of organizational, technical, and procedural measures to ensure compliance with the basic security requirements listed below:

- Confidentiality, i.e., the property of information to be known only to those who have privileges;
- Integrity, i.e., the property of information to be modified only and exclusively by those who have privileges;
- Availability, i.e., the property of information to be accessible and usable when requested by the processes and users who have privileges.

Strategic direction and management statement

In order to provide Specialcavi Baldassari with a general and strategic direction in the short, medium, and long term, and to ensure the protection and security of information within the scope of its activities in accordance with the guidelines of the UNI CEI ISO/IEC 27001 standard, Specialcavi Baldassari has developed the policy on the protection of company information described in this document.

In order to achieve the IT security objectives identified as necessary by the Management, an Information Security Management System must be established that is consistent with the policy that the company intends to implement. The maintenance of this system is guaranteed by implementing a continuous improvement process involving all relevant company functions:

- the **staff**, who will implement the security policies and requirements to achieve the set objectives.
- **customers**, whose security needs will be guaranteed in accordance with the commitments made by Specialcavi Baldassari
- **suppliers**, who will contribute, as partners, to the achievement of the organization's objectives and will accept the security policies and risks associated with supply.

The management is aware that the implementation of the Management System requires a significant initial effort and that maintenance and continuous improvement must be ensured by adequate organizational support.

To this end, changes will be made to the organization of Specialcavi Baldassari so that the roles and responsibilities for Information Security are defined and able to operate in the direction indicated by this policy.

Management will make available the investments necessary to meet the established policies and objectives and considers it appropriate to address the start-up phase of the System with the inclusion of external resources that are able to provide qualitative and quantitative support on all aspects related to information security.

This policy represents the general objectives and requirements issued by the management of Specialcavi Baldassari, which must be implemented by the company's departments, each within their specific area of competence, so that work activities comply with the provisions of this policy.

Risk assessment and general overview of controls

Security requirements are identified through a systematic assessment of security risks using methodologies recognized by international standards.

The results of the risk assessment will help determine the appropriate actions for managing and implementing controls to protect against these risks. They will also determine the relative priorities.

The risk assessment will be repeated periodically to address any changes that could affect the risk factor.

Based on the risk assessment, the costs of controls must be balanced against the benefits of protection against damage that the business could suffer as a result of information security breaches.

The company's information assets

Any type of data aggregation that has value for the company, regardless of the form and technology used for its processing and storage, contributes to the formation of information assets. Information must be protected in all possible formats in which it is made available:

- **paper** (documents, letters, lists, etc.)
- **electronic** (databases, disks, tapes, etc.)
- **verbal** (meetings, personal and telephone conversations, seminars, interviews, etc.)

Depending on the type and origin, the information that constitutes the company's information assets can be divided into.

- Information derived from the **customer's information assets**, represented by the set of information managed by Specialcavi Baldassari through its production processes and currently located in data centers managed directly or indirectly by the company. The security of this information must be guaranteed by contract with customers, and any security incident would have direct consequences on the company's image and business development.
- Information derived from **internal information assets**, represented by all information internal to the company and partly managed through information systems. This information influences other information and directly or indirectly affects all business activities.

The information must be evaluated to assign it the relative importance at the company business level in order to implement security countermeasures that are adequate and proportional to the different forms and methods of interaction used.

System objectives and implementation

This information security policy identifies the security aspects to be implemented within the organization in order to support Specialcavi Baldassari's mission and pursue the primary objectives listed below.

The company departments responsible for information management and security are tasked with translating the identified objectives and general information security requirements into more specific security measures and policies, with a view to achieving an adequate Information Security Management System.

The **primary objectives** to be pursued in accordance with the security policy adopted are as follows:

- Reduce serious events (ransomware, payment hijacking, serious breaches) to zero
- Set up an IT department capable of controlling logical information security: asset mapping, risk assessment, and reduction of the overall risk level by 15-20%
- Monitor the performance of the Data Security System: implement logic and tools for monitoring security performance (inventory, network monitoring, vulnerability assessment, threat protection status, incidents, monitoring of equipment, systems, and logs)
- Map physical areas that are sensitive in terms of confidentiality and ensure their physical protection
- Compliance with current voluntary (ISO 27001 in particular) and mandatory (e.g., EU GDPR in particular, Legislative Decree No. 24/2023 Whistleblowing) regulations

By achieving these objectives, management expects to safeguard the company's reputation, its physical and intangible assets, and the continuity of operations for the benefit of all stakeholders (customers, owners, employees, suppliers, and the community).

These are achieved and maintained through the collaboration of employees at all levels, who are required to:

- ensure the confidentiality, integrity, and availability of information
- assess risk levels
- monitor security levels
- formalize security requirements in relations with customers and suppliers
- ensure a corporate culture of information security and an adequate level of competence
- plan and manage business continuity

The contents of the system's guidelines and requirements apply to all internal and external personnel, partner companies, suppliers, outsourcers, and anyone who comes into contact with information owned by Specialcavi Baldassari.

All personnel who, as employees, consultants, or collaborators, work with the company in the design, development, management, and control of the services provided are responsible for complying with the requirements and guidelines of the system and are required to protect all information processed during their work activities. Staff, aware of the importance of the information processed, must act to ensure its protection and report any anomalies, even if not formally codified, of which they become aware.

In the event that the established security rules are disregarded by employees, consultants, and/or collaborators of the company, the management of Specialcavi Baldassari reserves the right to take the most appropriate measures against the offenders, in full compliance with legal and contractual constraints.
External parties who have dealings with Specialcavi Baldassari must guarantee compliance with the security requirements set out in this security policy, including by signing a "confidentiality agreement" at the time of appointment if this type of restriction is not expressly mentioned in the contract.

Conclusions

The Information Security Policy must always be consistent with the company's business objectives and, therefore, the Management reserves the right to make any changes to this document based on the results achieved by Specialcavi Baldassari, the expectations of all interested parties, and the performance of the reference market.
In accordance with the Information Security Policy and at least once a year, the Management will set security objectives, also using the results achieved during the previous year.
This policy has been approved by the Management of Specialcavi Baldassari.

The Management, Giacomo Baldassari, March 3, 2024