bureau Plattner

INFORMATION SECURITY POLICY AND CONTROL

Rev.	Date	Changes	Prepared by	Verified by	Classification
0	03.02.2025	First issuance	Carlo Gurioli	Hugo Perathoner	Public

1. PURPOSE AND SCOPE OF APPLICATION

The purpose of this document is to outline the general principles of information security defined by Bureau Plattner, with the aim of developing an efficient and secure Information Security Management System (ISMS).

2. REGULATORY REFERENCES

- ISO/IEC 27001:2022 - Information security, cybersecurity and privacy protection - Information security management systems - Requirements
- Legislative Decree of 30 June 2003, No. 196, as amended by Legislative Decree 101/2018 - Provisions of the Data Protection Authority and EU Regulation 679/2016 (GDPR) on the protection of personal data.

3. DESCRIPTION

For Bureau Plattner, the primary objective of information security is to protect data and information, as well as the associated technological, physical, logical, and organizational infrastructure, and their management. This entails the implementation and maintenance of a secure information management system, based on compliance with the following principles:

1. **Confidentiality:** ensuring that information is accessible only to duly authorized individuals and/or processes;
2. **Integrity:** safeguarding the consistency and accuracy of information from unauthorized modifications;
3. **Availability:** ensuring that authorized users have access to information and related architectural components when required;
4. **Control:** guaranteeing that data management is always carried out using secure and validated processes and tools;
5. **Authenticity:** ensuring the trustworthy origin of information;
6. **Privacy:** ensuring the protection and control of personal data.

Within the framework of services provided, compliance with the established security levels aims to ensure:

- the guarantee of having entrusted the processing of one’s informational assets to a reliable partner;
- a strong and reputable corporate image;
- full compliance with the Service Level Agreements (SLA) agreed with clients;
- client satisfaction;
- adherence to applicable legal requirements and international security standards.

For this reason, Bureau Plattner has developed an Information Security Management System in accordance with the requirements of ISO/IEC 27001:2022 and applicable legal provisions, as a means to manage information security within the scope of its business activities.

4. SCOPE OF APPLICATION

The information security policy of Bureau Plattner applies to all internal personnel and third parties involved in information management, as well as to all processes and resources used in the design, implementation, deployment, and continuous delivery of its IT services.

5. DESCRIPTION OF THE POLICY

The Information Security Policy of Bureau Plattner reflects the organization's commitment to its clients and third parties to ensure the protection of information and of the physical, logical, and organizational tools used in information processing across all activities.

Bureau Plattner's Information Security Policy is inspired by the following principles:

1. to ensure that the organization maintains full awareness of the information it processes and evaluates its criticality, in order to facilitate the implementation of appropriate protection levels;
2. to ensure secure access to information, in order to prevent unauthorized processing or processing carried out without the necessary rights;
3. to ensure that both the organization and third parties involved in information processing adopt procedures designed to uphold adequate levels of security;
4. to ensure that anomalies and incidents affecting the information system and the organization's security levels are promptly identified and properly managed, through effective prevention, communication, and response systems, in order to minimize business impact;
5. to ensure that access to corporate premises and individual rooms is granted exclusively to authorized personnel, thereby safeguarding the security of facilities and assets;
6. to ensure compliance with legal requirements and with the security commitments established in contracts with third parties;
7. to ensure the detection of abnormal events, incidents, and system vulnerabilities, in order to preserve the security and availability of services and information;
8. to ensure business continuity and disaster recovery, through the application of established security procedures.

Bureau Plattner defines and documents its policies, objectives, and commitments with regard to information security, also taking into account the expectations of all stakeholders, potential risks and opportunities, and the need to ensure compliance with mandatory and client-specific requirements.

To implement these policies, Management identifies and determines how to achieve defined objectives, making them quantifiable and measurable.

The information security policy is continuously updated to ensure ongoing improvement and is shared with the organization, third parties, and clients through the internal documentation system and specific communication channels.

6. RESPONSIBILITIES AND UPDATES

The Management of Bureau Plattner is responsible for the Information Security Management System, ensuring its alignment with the evolving corporate and market context, and assessing any actions to be taken in response to events such as:

- significant developments in business activities;
- emergence of new threats not previously considered in the risk assessment process;
- major security incidents;
- changes in the regulatory or legislative framework relating to the secure processing of information.