BOUTIQUE_

Your Research Partner

Information Security Policy

Reference	POL.02
Date	09/04/2026
Version	1.0
Classification	Internal Use Only

1. Introduction

Boutique considers information to be an essential strategic asset. Therefore, Boutique's Management recognizes the importance of establishing and implementing a general policy that ensures the protection of the integrity, availability and confidentiality of information. The objective is to ensure its adequate protection and contribute to the continuity and efficiency of business operations, following the guidelines of the international standard ISO/IEC 27001:2022.

1.1. Purpose

This policy aims to establish the purpose, guidance, principles and guidelines essential for the management of information security, in line with the particularities and requirements of Boutique's business and its stakeholders.

1.2. Scope

This policy applies to the entire organization, including all stakeholders and entities that have any type of commercial or contractual relationship with Boutique, such as employees, customers, suppliers and service providers. This covers everyone who has access, right to use or control over information assets belonging to Boutique and its associated resources.

All interested parties must be aware of this policy and act in accordance with it, as well as with other documents related to Information Security, as applicable and appropriate.

1.3. Responsibilities

The Information Security Policy applies to Boutique's Management and all employees, regardless of their relationship, as well as to suppliers, service providers and their employees, as well as other interested parties who have access to information under Boutique's responsibility.

Management has the following responsibilities:

- approve the Information Security Policy and other policies or procedures related to information security;
- enforce commitment to information security;
- approve the strategy for handling high and very high severity information security risks;
- ensure the necessary resources to comply with the strategy and planning, regarding information security.

Employees are responsible for:

- complying with the Information Security Policy and other policies, standards and procedures related to information security;
- communicating the security and privacy risks identified in its processes, according to the defined communication channels;
- conducting training on information security.

Thus, everyone must comply with and ensure compliance with this Policy, in addition to reporting any incident or situation that may compromise information security.

2. Information Security Principles

Boutique's Management and employees are committed to effectively managing the security of information and the assets under their responsibility, also ensuring the continuous improvement of the ISMS. This commitment is aligned with the organization's strategic objectives and based on the following security principles:

1. Ensure the protection and correct classification of information and its support assets, ensuring the three fundamental pillars of information security – confidentiality, integrity, and availability – according to its criticality to the organization and its customers.
2. Ensure that information protection is in accordance with the company's internal policies, as well as with applicable laws, regulations, customer requirements and other external standards.
3. Develop, implement and periodically review specific policies, standards, processes and controls, incorporating security and privacy measures as an

essential part of the protection of information assets against internal and external threats.

4. To carry out effective management of security incidents, through processes of prevention, detection, registration, communication, treatment and investigation of incidents and vulnerabilities that may compromise information security, data protection or business continuity.
5. Regularly conduct the assessment and monitoring of security risks, allowing the identification and mitigation of threats and ensuring that the controls implemented are aligned with the needs of the company and its customers.
6. Foster awareness, training and certification of employees in information security, encouraging the adoption of good practices and the development of an organizational culture focused on information protection.
7. Ensure that the ISMS achieves the intended results, promoting continuous improvement.

3. Information Security Policy

3.1. Information Security

Information is understood as any flow of communication or representation of knowledge as data, facts or opinions, in any medium or format (e.g. textual, numerical, graphic, cartographic, narrative, audiovisual, or conjunctions thereof).

An **Information Asset** is understood to be any asset that supports information, in any format, and that has an intrinsic value for the organization. Assets include the information entities themselves (e.g. databases, contracts, etc.), software (e.g. applications, operating systems, network platforms, etc.), hardware (e.g. computers,

communications network equipment, etc.), services (e.g. electronic communications, energy, etc.), people (e.g. qualifications, knowledge, etc.), intangibles (e.g. company reputation and image, etc.), among others.

Information Security consists of protecting information and its supporting assets in the three fundamental pillars, throughout the life cycle.

- **Confidentiality** - Ensures that information is accessed only by people who are authorized to do so, on a need-to-know basis. It prevents unauthorized access and/or disclosure of information, accidentally or intentionally.
- **Integrity** - Safeguarding the accuracy of information and processing methods, as well as the respective support assets (systems, infrastructures or others). It ensures that the information is consistent regardless of the medium where it is found. Prevents unauthorized and/or accidental modification, loss or deletion of information.
- **Availability** - Ensures access to information/services and their support assets whenever necessary and permitted, without undue delay.

The protection of information must also be in **Compliance**, both with the organization's internal policies regarding information, and with laws and regulations external to the organization. You should also consider the service requirements documented in SLAs, contracts, or operating agreements with customers.

3.2. Information Security Content

Boutique undertakes to develop specific policies and procedures that comply with the international benchmark standards, auditable, which define the requirements for the implementation of an Information Security Management System (ISMS), covering, in

particular, the areas provided for in the ISO 27001 and ISO 27002 standards, with regard to:

- Physical and environmental security: Boutique ensures the protection of its equipment and information assets against environmental risks and physical threats. All company devices and any information accessible through them must be kept in environments with appropriate physical safeguards, ensuring protection against unauthorized access, theft, or damage.
- Protection of physical and intangible assets: The protection of Boutique's assets includes both physical assets, such as equipment and infrastructure, and intangibles, such as knowledge, data, and reputation of the company. All employees must protect these assets, respecting the rules of use and avoiding any type of misuse or unauthorized sharing with third parties. Access to intangible assets, such as strategic or proprietary information, is restricted to authorized persons on a need-to-know basis.
- Use of Communications: All communications conducted, whether internally or with third parties, must comply with Boutique's ethical and security standards. Employees should avoid using language that is inappropriate, offensive or compromises the company's image. Personal communication should be limited and not interfere with professional activities, and should always be evaluated for the potential impact on information security and the organization's reputation.
- Social Media Management: Social media communication on behalf of Boutique is restricted to Management and the communications team. Employees should not post information, respond to comments, or make statements that may affect the company's image, unless authorized. The company adopts a transparent and

responsible posture in interactions with the public, always in line with legal standards and internal policies.

- Vulnerability management: Boutique conducts periodic risk assessments to identify and correct vulnerabilities in information systems. These assessments are key to ensuring that security controls are effective and to reducing the risks associated with technical failures, external vulnerabilities or internal threats. Vulnerability management must be addressed on an ongoing basis, with corrective measures implemented effectively.
- Backup: Boutique implements a backup strategy to ensure data protection and business continuity. Backups are performed regularly and stored securely, including offsite copies as needed. The backup strategy also encompasses automating processes and periodically checking to ensure that data can be recovered quickly in the event of a system failure.
- Control against malicious software: All Boutique systems are protected with antivirus software that is updated and monitored regularly. Additionally, the company adopts strict policies to prevent the spread of malware, including scanning email attachments and downloads from unverified sources. The IT team conducts frequent audits to ensure that systems are protected from external threats.
- Traceability: All critical Boutique systems generate event logs, including access attempts and actions taken by users. Record generation is critical for traceability and forensic analysis in the event of security incidents. Those records shall be kept securely and accessible only to personnel authorized for research or audits. All this infrastructure is subcontracted to specialists.
- Information Security Incident Response: Incident response is structured in clear processes, which involve identifying, containing, mitigating, and investigating security incidents. Boutique maintains an up-to-date incident response plan,

which defines the procedures to be followed in the event of incidents, ensuring that corrective actions are taken quickly.

- Risk and Impact Management: Boutique takes a proactive approach to risk management, identifying, assessing, and mitigating risks that may affect information security. Risk analysis is an ongoing process that allows you to identify threats and vulnerabilities and implement appropriate mitigation measures.
- Disaster Recovery: Boutique's Disaster Recovery Plan lays out the actions needed to restore services and operations after a disruptive event, ensuring business continuity. This plan is tested regularly to ensure that the company can react quickly to crisis situations and minimize the impact of disasters.
- Business Continuity: Boutique has a Business Continuity Plan that ensures the continuity of the company's critical operations, even in adverse situations. The plan involves preventive and corrective measures that ensure that the company can keep its essential functions up and running, even in the face of unforeseen events.

4. Version Control

Revision History

Version	Date	Author	Changes
1.0	09/04/2026	Viviana Piedade	First version

Approval

Name	Role	Version	Date
Viviana Piedade	CISO	1.0	09-04-2026