

## INFORMATION SECURITY POLICY

### CONTENTS

CONTEXT .....	2
PURPOSE AND SCOPE .....	2
PRINCIPLES AND ACTIONS DERIVING FROM THIS POLICY.....	2
PRINCIPLES.....	2
ACTIONS.....	2
APPLICATION AND RESPONSIBILITIES .....	3
APPROVAL, PUBLICATION AND REVIEW.....	3

## CONTEXT

The Puig Ethical Code establishes that data and information assets are assets whose gathering and treatment must be limited to that which is strictly necessary for carrying out the company's legitimate activities, and promotes a proactive framework for their protection.

## PURPOSE AND SCOPE

This Policy develops the commitments established in the Puig Ethical Code and defines the principles and actions that constitute the framework for the treatment, management, and security of data or information assets. Data or information assets are any type of resource that contains information necessary for the activity of the business, regardless of the platform, channel, or way in which it is communicated, transmitted, shared, projected, or stored, whether internal or external, or whether owned by Puig or by third parties.

The purpose of this policy is to provide Puig with a framework for the protection of data and information assets to preserve their confidentiality, integrity, and availability, and guarantee compliance with applicable regulations relating to information security.

This Policy has been approved by the Board of Directors of Puig Brands, S.A. and applies to all Puig<sup>1</sup> companies and activities.

This Policy is the generic framework which defines the principles and actions to be implemented by those responsible for the data and information assets in each functional area.

Specific Puig divisions and business units may develop this Policy through other divisional or local regulations that comply with the provisions of this Policy.

## PRINCIPLES AND ACTIONS DERIVING FROM THIS POLICY

### PRINCIPLES

This Policy is based on the following principles:

- **Protection of the business**, prioritizing the protection of information that directly affects business operations, innovation, and the continuous improvement of our activities.
- **Management of risk**, adopting measures to identify existing risks in the management of information and avoid those that are unnecessary or excessive.

### ACTIONS

To comply with the objectives and principles established, the following actions are required:

- **Classification of information:** All information assets must be identified and classified in terms of value, legal requirements, confidentiality, sensitivity, and importance to the organization. The owners of the assets are responsible for ensuring that they are properly classified and protected according to the following classification based on the law and good practice, their potential impact on the business and its image, and on partners or others linked to Puig:
  - Secret information: information of strategic importance that can cause severe or irreparable impact and whose access is limited to a very small group of people.

---

<sup>1</sup> "Puig" refers to the Puig Brands, S.A. company and its subsidiaries and other entities that may be incorporated in the future in which Puig Brands, S.A. holds or may hold direct or indirect control, according to article 42 of the Spanish Commercial Code.

- Restricted information: sensitive information belonging to a business area or department that may give rise to moderate economic losses, breaches of applicable regulations, or damage to the reputation of Puig, among other potential consequences. It is only accessible to a specific group of people expressly authorized by the owner of the information.
- Confidential information: information that can cause serious impact and whose access is limited to a specific group of people, specific areas, or parts of areas.
- Internal information: information that can cause limited impact and is generally available to all or most people, although it cannot be disclosed publicly.
- Public information: information that is in the public domain or that is made available for public distribution through a Puig channel and that can be freely consulted.
- **Information security management:** a level of protection, control, and adequate management of Puig information assets is guaranteed.
- **Incident management:** procedures are established for the management of information security incidents that include notification, response, and recovery.
- **Identity control:** the life cycle of identities and the accounts associated with each of them must be controlled and managed appropriately.
- **Access control:** access to information must be controlled and restricted to authorized persons, and access rights must be reviewed regularly to ensure they are adequate.
- **Business continuity:** in the event of possible interruptions or failures of business operations, plans are developed in advance to guarantee its ability to continue, whilst protecting, maintaining, and recovering information.
- **Training and awareness:** training and awareness actions are implemented that guarantee the security of information for users.
- **Compliance:** compliance with applicable information security regulations is guaranteed.
- **Review and continuous improvement:** Regular audits and review activities will be carried out to evaluate the effectiveness of the Information Security Policy and information security practices.

Puig guarantees the principles, actions and methodology included in this Policy by providing the necessary material, technological, financial, and human resources.

## APPLICATION AND RESPONSIBILITIES

This Policy is mandatory for any person or legal entity who has access to the data or information assets of Puig, and all interested parties must promote compliance with this Policy.

Failure to comply with this Policy may incur disciplinary measures and other consequences as provided for by law.

## APPROVAL, PUBLICATION AND REVIEW

This Policy has been approved by the Board of Directors of Puig Brands, S.A. on April 5, 2024, and came into force at that time.

Responsibility for the publication, communication, and review of this Policy is assigned to the Information and Cybersecurity Area in coordination with the Legal Area.