INFORMATION SECURITY POLICY

INDUSTRIA DE DISEÑO TEXTIL, S.A.
(INDITEX, S.A.)

APPROVED BY THE BOARD OF DIRECTORS

ON 10 DECEMBER 2019

Reference	
Name of the Standard	Information Security Policy
Scope	Global
Type	Policy
Supervisor	Information Security
Date of approval	10/12/2019[1]
Version	2.0

[1] Date format: DD/MM/YYYY

TABLE OF CONTENTS

1. Purpose

The Information Security Policy (the "**Policy**"), was approved by the Board of Directors on 10 December 2019, following a favourable report of the Audit and Compliance Committee, on the proposal of the Information Security Committee (the "**ISC**"). This Policy sets forth the principles and guidelines whereby Inditex (the "**Company")** will protect its information, pursuant to applicable regulations and its ethical values defined in the Code of Conduct and Responsible Practices (the "**Code of Conduct**"), as well as the provisions of the Regulations of the Information Security Committee (the "**ISC Regulations**") and of any other applicable regulations.

Inditex shall ensure that its information (the "**Information**") is protected, regardless of the manner it is transmitted, shared, projected or stored. Such protection affects both the existing information within the Group, and that shared with third parties.

In this regard, Information Security shall mean safeguarding and protecting (i) proprietary information of the Group, whether stored in own or third parties' information systems; and (ii) proprietary information of third parties stored in Group's information systems.

For the purposes hereof, Information Systems shall mean any technology system or technological means, whether own or third parties', which manage, store or transmit Information (including cloud technologies and the like).

2. Scope of application

This Policy shall apply to the Company and its Group. It shall be binding for the entire staff, regardless of their job and position.

For such purposes, Inditex Group shall mean any company in which Inditex owns, whether directly or indirectly, at least a 50% stake of the share capital or 50% of the voting rights.

The enforcement of this Policy, in full or in part, may extend to any natural and/or legal person associated with Inditex on any terms other than an employment relationship, where this is practicable on account of the nature of the relationship and may be appropriate to meet its purpose.

Under this Policy, Inditex may develop a number of procedures and instructions to implement and enforce the obligations undertaken, and to bring it into line with the different local laws and regulations applicable to the Group.

The application of this Policy is supplementary to other mandatory internal regulations, such as the Compliance Policy regarding Personal Data Protection and Privacy, and any others relating to Company's information.

3. Objectives

This Policy provides a framework for Inditex to define the guidelines for an effective protection of the Information managed by the Group, and has the following objectives:

- Ensuring the **confidentiality** level appropriate for each type of Information, pursuant to the classification set in the Procedure on Information Classification.

- Keeping the **integrity** of the Information, so that it remains unchanged in respect of the moment it was created by its owners or holders.
- Ensuring the **availability** of the Information in all its carriers and whenever it is necessary, ensuring business continuity and fulfilment of all the obligations applicable to the Company.

4. Overarching principles

The achievement of the objectives described in section 3 above revolves around the following overarching principles:

- Classification of Information. Information shall be classified in accordance with its value, relevance and criticality for the business, so that protective measures are aligned with the level of classification of each information asset. Likewise, Information assets shall be classified taking into account the legal and operational requirements, and best practices and standards in this regard.
- Use of Information Systems. Use of Information Systems shall be limited to lawful and exclusively professional purposes, to carry out job-related tasks. Consequently, a personal use of such resources and/or systems is not permitted, nor can they be used for any unlawful purpose.
- Segregation of duties. Concentrations of risks stemming from the absence of a segregation of duties and the key-person dependency in critical business functions must be avoided.

  In this regard, formal procedures shall be set to monitor assignment of privileges to Information Systems, in such a way that users can only have access to such resources and Information necessary for the performance of their duties.
- Information retention. Where necessary or convenient, retention periods will be set by Information category, considering the operational or regulatory compliance requirements as well as the relevant procedures for Information disposal.
- Access to Information by third parties. Monitoring procedures shall be developed to control how Information of Inditex or of third parties related to the Group is made available or accessed by any other third parties.
- Security in Information Systems. Development and production environments shall be kept in independent Systems. Likewise, development and maintenance of Information Systems shall include the necessary controls and records to ensure the appropriate implementation of security specifications.
- Continuity. A process for continuity management shall be set to ensure recovery of critical Information for the Group in the event of disaster, reducing downtime to acceptable levels.
- Compliance. The Information Systems and communications of the Group shall be permanently aligned with the requirements of current laws and regulations applicable in all jurisdictions where it operates, as well as with the applicable internal applicable regulations.

5. Responsibilities

Protection of the Information and the Systems which process, store or transmit it, is incumbent on employees at all organizational and working levels of the Company, to the extent required from them, as detailed below:

5.1 Responsibilities of employees

- All Group employees must be familiar with, understand and comply with the Policy and with the applicable internal regulations governing security and use of Information Systems, being compelled to keep professional secrecy and confidentiality in respect of the Information handled in their working environment, and to report as a matter of urgency, and in accordance with the procedures set, any potential incident or security breach detected.
- Employees who hire services from third parties entailing the use or access by these latter to the Information, shall understand the risks arising from the outsourcing process, and ensure an effective management thereof.
- The use of the Information Systems or of digital services by the employees, expressly including e-mail and instant messaging services, shall be limited to lawful and exclusively professional purposes, in order to perform job-related tasks. Consequently, a personal use of such resources and/or systems is not permitted, nor can they used for any unlawful purpose.

5.2 Responsibilities regarding suppliers and other third parties

- In addition to the provisions of section 5.1 above, any agreement with third parties which entails the use or access by these latter to the Information, including agreements for the provision of services, or outsourcing services agreements, shall include the specific security requirements relating to the technology and the activities conducted by those who render such services.
- In this regard, provisions should be included in such agreements to ensure that suppliers, sub-contracted staff or any external facilitator which uses or has access, whether potential or real, to the Information (through the Information Systems by any other means, as addressed in section 1 above), must be familiar with the Policy and comply with it, where applicable, being compelled to keep the professional secret and confidentiality in respect of the Information handled for the term of their relationship with the Group.

5.3 Information Security department

The Information Security department shall carry out its control duties in an independent manner, and it shall be responsible for implementing the Policy and monitoring compliance therewith, and with all requirements arising from applicable laws, regulations and best practices in the field of Information Security. Wherefore, the Information Security department shall be responsible for:

- Implementing an Information Security strategy that ensures observance of the overarching principles of the Policy, and that namely covers the following aspects:

  - Appropriate access to Information, based upon the principle of least privilege and the approval of the owner of the Information asset;
  - Appropriate segregation of roles and duties in Information Systems;
  - The right configuration, administration and operation of the infrastructure, services and/or software used in the different business processes both within and outside Group facilities, from the perspective of security;
  - The right implementation of security requirements during the life cycle of such Information Systems which support the processes of the Company.
  - An appropriate protection of Information Systems and of their against physical or environmental threats, based upon their criticality, allowing to identify, assess, prevent and respond to any risk which may compromise the security thereof.

- Setting and reviewing the appropriate controls to ensure compliance with the Policy and its regulations, including the organizational and technological mechanisms necessary to allow continuous monitoring of access to and use of Information Systems, services or Information, managed by the Group.
- Preventing, detecting and responding to any incident relating to Information Security, and acting pursuant to the provisions of "Procedure for the Information Security Incident Response Plan" of the Inditex Group.
- Driving the regulatory development of the Policy, through the necessary procedures and instructions, to define a global framework of Information Security at all levels. Likewise, it shall review, update and disclose any changes which may give rise to amendments of the Policy.
- Carrying out training and raising awareness on Information Security processes.
- Setting a continuous improvement approach.
- Ensuring compliance with the applicable laws and regulations in the scope of the duties it is entrusted under the Policy.

5.4 Information Security Committee

Inditex relies on an Information Security Committee, composed of members of management, which seeks, in furtherance of its Regulations, to ensure the effective and consistent enforcement of best practices regarding information security management across the organization.

The Security Committee shall be responsible, inter alia, for overseeing the Information Security strategy, including budget expenditure, investments and resources in security plans, and coordinating security needs of management, business units and geographies.

It shall report at least on an annual basis, through the Information Security Department, to the Executive Chairman and the Governing Bodies of the Company, on the status of security, the evolution of threats and the risk appetite, the allocation of resources for security, and any significant incident.

6. Implementation

Inditex undertakes to assign specific resources to ensure the effective implementation of the Policy.

7. Audit and Control

Inditex expressly reserves the right to take, with due proportionality, the required monitoring and control measures necessary to establish the appropriate use of the Information Systems it makes available to its employees, including verifying the contents of the communications and devices, observing at any rate the applicable laws and regulations. The communication and acceptance of the Policy shall serve the purposes of prior notice to the employee.

The Group will undergo regular reviews and controls, and will be subject to internal and external audits to assess general compliance with the Policy.

Any potential violation of the Policy shall be determined in the relevant procedure, pursuant to applicable provisions, without prejudice to any legal responsibilities, including sanctions in the work environment, which may enforced on the infringing party.

8. Communication of the Policy

This Policy will be available to all employees on INET, and to all stakeholders of the Company on the corporate website. Likewise, the Policy shall be subject to the appropriate disclosure, training and awareness-raising action, aimed at its full understanding and implementation.

9. Update and review of the Policy

The Policy will be reviewed and updated, where applicable, to bring it into line with any changes that the business model may undergo, or that may occur in the context where the Group operates, ensuring at all times the effective implementation thereof.

* * *