Corporate Information Security Policy

Chief Executive Officer

17 April 2024

VERSION CONTROL

Version	Date	Changes
V1	31/07/2020	New Creation
V2	28/04/2023	Adaptation to ISO/IEC 27001:2013
V3	17/04/2024	Adaptation to ISO/IEC 27001:2022

CONTENTS

1. Subject matter

The Corporate Information Security Policy aims to establish and regulate the general provisions and guiding principles for information security issues concerning the Company.

URBASER reaffirms its position as a sustainability-oriented company through its mission to contribute to the appropriate development of cities and territories through efficient services and innovative technology. For this reason, it plays a relevant role in the protection of technological, industrial and commercial activity in the development and operation of critical infrastructures that provide essential services to society and governmental public entities and institutions.

URBASER must be perfectly prepared to intervene, react and protect its information assets in case of security incidents that may affect it, as well as to ensure that all its activities and services are aligned with the most demanding local and international information security guidelines.

By means of the approval of this Policy, URBASER manifests its determination and commitment to reach a level of information security adequate to the needs of the business that guarantees the protection of the assets in a homogeneous way in all the Group.

2. Scope of application

This Policy is applicable to all the participated entities (companies, UTEs, Joint Ventures or any other associative formula) in which URBASER, S.A.U. is the majority shareholder or has control (hereinafter, "URBASER") and **of** obligatory compliance for all users who participate in the management, use or exploitation of URBASER's Information, including, but not limited to directors, executives, employees, collaborators, managers, members of the governing bodies.

In those investees in which this Policy does not apply, the alignment of their own policies with those of this Policy will be promoted through their representatives in the governing bodies.

3. Content

Information security, one of the fundamental pillars on which URBASER is built, must be understood as an integral concept that aims to preserve the assets and protect the interests and strategic objectives of the Company. Similarly, information security must contribute to preserving the confidentiality, integrity and availability of the data of clients and other interested parties.

In this sense, URBASER, assumes the following objectives:

- Align the information security strategy with URBASER's business strategy.
- Establish good information security governance to ensure its proper management and operation in accordance with applicable information security requirements (applicable legislation in force in each country, contractual requirements and stakeholder needs).
- Provide the necessary resources to achieve the established objectives.
- Identify and, where appropriate, assess and categorise the risks and opportunities inherent to activities, processes and services, planning the necessary actions for their treatment, preventing undesired effects and enhancing their favourable effects.

- Securing the supply chain from an information security point of view.
- Ensure that all personnel, including external collaborators with access to the organisation's information systems, have the appropriate culture, education, awareness and training to carry out their activities in a secure manner for themselves and others, guaranteeing the security of information at all times.
- Implement the necessary security measures to ensure the confidentiality, integrity and availability of information security throughout its life cycle.
- Manage information security incidents to minimise the impact and likelihood of their occurrence.
- Align the information security management strategy with the IT business continuity strategy.
- Continuously improve the information security management system, encouraging the active participation of the entire organisation to promote and adopt measures that shape more secure and optimised processes.

In order that the existing threats in URBASER do not materialise or, in case of materialising, do not seriously affect neither the information that it handles nor the services provided, the security activities of URBASER will be guided by the following principles:

- **Efficiency:** priority will be given to the knowledge of potential threats and the risks derived from them, with the aim of anticipating their action, evolution and to preserve the Company from their potential harmful effects, mitigating them to an acceptable level for the business.
- **Responsibility:** users must preserve the security of the assets that URBASER places at their disposal, in accordance with the defined security criteria, requirements, procedures and technologies.
- **Legality: the** necessary compliance with the laws and regulations in security matters, in force at all times in all the territories in which URBASER operates, will be observed at all times.
- **Cooperation and Coordination:** cooperation and coordination between all business units and staff will be prioritised in order to generate appropriate synergies and strengthen joint capabilities.
- **Prevention:** in order to prevent and avoid the information or services from being damaged by security incidents, URBASER will implement the security measures determined by the security regulations currently in force in each country, as well as any other additional control identified through a threat and risk assessment.
- **Detection: the** operation of systems and services will be monitored on a continuous basis to detect anomalies in performance levels and act accordingly.
- **Response:** Mechanisms shall be put in place to respond effectively to information security incidents.
- **Recovery:** Information and Communication Technology (ICT) systems continuity plans will be developed.

In order to comply with this standard, the roles and responsibilities regarding information security are defined in the Roles and Responsibilities Regulation (NS-19-CORP), where the Information Security Committee, the governing body of this Policy, is defined.

4. Training

The necessary training and awareness-raising actions shall be promoted for the knowledge, implementation and monitoring of this Information Security Policy.

5. Doubts, communications or complaints

Any queries within the scope of this Policy should be addressed to the URBASER Corporate Information Security Area.

Any incident regarding non-compliance with the provisions of this Policy and related procedures, or its alignment with the provisions of the Group's Code of Conduct, should be addressed to the corresponding regulatory compliance body through the Ethics Channel set up on the Group's website (https://www.urbaser.com/canal-etico/).

6. Non-compliance

This Policy is considered to be a mandatory rule, and therefore its violation will constitute a breach of it and the Company will adopt the appropriate disciplinary, contractual or legal measures, where appropriate, without prejudice to any other responsibilities that the offender may have incurred. Likewise, URBASER will reserve the right to adopt the measures that it considers appropriate against the business partners that do not comply with it. Any exception or exemption, whether for organisational, legal, contractual, technological or other reasons to this Policy or to any rule, procedure or technical instruction on which it depends, will be managed in accordance with the internal documents defined for this purpose.

7. Review and update

The Information Security Committee shall review annually or whenever there is a substantial change in the context of the organisation, ensuring that it reflects international recommendations and best practices in accordance with regulatory requirements and applicable legislation. It shall also propose to the Governing Body the modifications and updates that contribute to its development and continuous improvement.

www.urbaser.com