Corporate Information Security Policy

Chief Executive Officer
24 November 2025

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
V4	28/03/2025	Adaptation to ENS RD 311/2022
V5	24/11/2025	Includes comments in the field of OT

CONTENTS

1. Purpose

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

URBASER reaffirms its position as a sustainability-oriented Company through its mission to contribute to the proper development of cities and territories through efficient services and innovative technology. It therefore plays an important role in protecting technological, industrial and commercial activity in the development and operation of critical infrastructures that provide essential services to society and to public entities and government institutions.

URBASER must be fully prepared to intervene, react and protect its information assets in the event 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 approving this Policy, URBASER expresses its determination and commitment to achieving a level of information security appropriate to the needs of the business that guarantees the protection of assets in a consistent manner throughout the Group.

2. Scope of Application

This Policy applies to all affiliated entities (companies, joint ventures, or any other type of association) in which URBASER, S.A.U. is the majority shareholder or has control (hereinafter, "URBASER") and is mandatory 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 and members of governing bodies.

In those investee companies where this Policy does not apply, the alignment of their own policies with those of this Policy will be promoted through their representatives on the administrative bodies.

3. Content

Information security, one of the fundamental pillars on which URBASER is built, must be understood as a comprehensive 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, availability, authenticity and traceability of customer and other stakeholder data.

In this regard, URBASER has set itself 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 requirements (applicable legislation in force in each country, contractual requirements and stakeholder needs).
- Provide the resources necessary to achieve the established objectives.
- Identify and, where appropriate, assess and categorise the risks and opportunities inherent in activities, processes and services, planning the necessary actions to address them, preventing undesirable effects and enhancing their favourable effects.
- Ensure the supply chain from an information security perspective.
- Ensure that all personnel, including external collaborators with access to the organisation's information systems,

have the appropriate culture, training, awareness and skills to carry out their activities safely for themselves and others, guaranteeing information security at all times.

- Implement the necessary security measures to ensure the confidentiality, integrity, availability, authenticity and traceability of information security throughout its life cycle.
- Manage information security incidents to minimise their impact and likelihood of occurrence.
- Align the information security management strategy with the IT and OT business continuity strategy.
- Continuously improve the information security management system, encouraging the active participation of the entire organisation to promote and adopt measures that create more secure and optimised processes.

In order to prevent existing threats at URBASER from materialising or, if they do materialise, to prevent them from seriously affecting the information it handles or the services it provides, URBASER's security activities will be guided by the following principles:

- **Efficiency:** priority will be given to understanding potential threats and the risks arising from them, with the aim of anticipating their action and evolution and protecting the Company from their potential harmful effects, mitigating them to a level acceptable to the business.
- **Responsibility:** users must preserve the security of the assets that URBASER makes available to them, in accordance with the defined security criteria, requirements, procedures and technologies.
- **Legality:** the necessary compliance with the laws and regulations on security in force at all times in all the territories in which URBASER operates shall be observed at all times.
- **Cooperation and coordination:** cooperation and coordination between all business units and staff will be prioritised in order to generate the appropriate synergies and strengthen joint capabilities.
- **Prevention:** in order to prevent and avoid information or services being compromised 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 controls identified through a threat and risk assessment.
- **Detection:** the operation of systems and services will be monitored continuously to detect anomalies in service levels and act accordingly.
- **Response:** mechanisms will be established to respond effectively to information security incidents.
- **Recovery:** Continuity plans will be developed for Information and Communication Technology (ICT) systems and Operational Technology (OT) systems.

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

4. Training

The necessary training and awareness-raising activities will be promoted to ensure knowledge, implementation and monitoring of this Policy on information security.

5. Queries, communications or complaints

Any queries regarding this Policy should be addressed to URBASER's Corporate Cybersecurity Department.

Any incident relating to 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 relevant regulatory compliance body through the Ethics

Channel on the Group's website (https://www.urbaser.com/canal-etico/).

6. Breaches

This Policy is considered a mandatory rule, and therefore any violation thereof will constitute a breach of this Policy and the Company will take the appropriate disciplinary, contractual or legal measures, as applicable, without prejudice to any other liabilities that the offender may have incurred. Similarly, URBASER reserves the right to take any measures it deems appropriate against business partners who breach this Policy. 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 this Policy 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 Management Body any modifications and updates that contribute to its development and continuous improvement.

www.urbaser.com