# Corporate Information Security Policy

## Purpose

This Corporate Information Security Policy establishes and regulates the general provisions and the guiding principles of the information security issues that are applicable to the Company.

URBASER, reaffirms its position as a sustainability-oriented Company, carrying out its mission of contributing to the proper development of cities and territories through efficient services and innovative technology. Therefore, URBASER 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 the society, government entities and public institutions.

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

By approving this Policy, URBASER states its commitment and determination to achieve an appropriate level of information security, matching the needs of the business that homogeneously guarantee the protection of assets throughout the Group.

Additionally, the information security measures applicable to URBASER assets will include the personnel of its collaborating entities (suppliers, subcontractors, etc.) when their activities involve managing corporate information.

## Scope

This Policy is applicable to all employees, managers and members of the governing bodies of URBASER S.A.U., its subsidiaries and investee companies/joint ventures in which URBASER is the majority shareholder/partner or where control is held by URBASER's management ("URBASER" or "the Company"). It is the responsibility of all URBASER employees to act professionally and protect the Company's reputation.

## Contents

Information security is one of the most important principles on which URBASER is built, and it must be understood as a comprehensive concept that aims to preserve assets and protect the interests and strategic objectives of the Company. Likewise, the information security must contribute to preserve confidentiality, integrity and availability of its customers and stakeholder's data.

In this context, URBASER is committed to:

- Set information security objectives, aligned with line of business needs, implement and monitor them using metrics to assess their level of compliance.
- Provide the resources that are necessary to achieve the objectives defined.
- Identify and, when applicable, assess and categorize the inherent risks and opportunities in the activities, processes and services, planning the necessary actions for their treatment, preventing unwanted effects and enhancing their beneficial effects.
- Understand and meet the information security needs and expectations of its customers and other stakeholders, setting the appropriate measures to comply them.
- Continuously improve the information security management system, encouraging active participation of the entire organization to promote and adopt measures creating safer and more enhanced processes.

- Ensure that all staff, including the external collaborators, who have access to the information systems in the Company, have the appropriate training and information to safely develop their activities, ensuring at all times information security.
- Understand, disclose and ensure compliance with the legal and regulatory requirements applicable to the activities carried out, following the reference standards and each country's applicable legislation related to information security.

In order to prevent, that the existing threats in URBASER materialize or, in the event they do materialize, that they do not affect severely neither the information nor the provided services it handles, URBASER's security activities will be guided according the following principles:

- **Efficiency**: knowledge of the potential threats and the risks derived from them will be prioritized, with the objective of anticipating their action, evolution and protecting the Company from its potential harmful effects, mitigating them to an acceptable level for the business.
- **Responsibility:** the users must preserve the security of the assets that URBASER makes available to them, in accordance with the criteria, requirements, procedures and security technologies defined.
- **Legality:** the necessary compliance with laws and regulations on security matters will be observed at all times, being in force at any time in all the territories where URBASER operates.
- **Cooperation and Coordination:** cooperation and coordination between all business units and employees will be encouraged, in order to generate adequate synergies and strengthen joint capacities.
- **Prevention:** to prevent information or services from being harmed by security incidents, URBASER will implement the security measures required by current security regulations needed in each country, as well as any other additional control identified through the risk assessment process.
- **Detection:** the activity of systems and services will be continuously monitored to detect discrepancies in the service levels and to react accordingly.
- **Response:** mechanisms will be set in place to respond effectively to information security incidents.
- **Recovery:** developing continuity plans related to Information and Communication Technologies (ICT), as a part of the business continuity plan and recovery activities.

This Policy is of mandatory compliance, therefore its violation will infringe it and the Company will adopt the appropriate disciplinary measures, in accordance with the applicable labour legislation for each case.

**José María López Piñol**
**Chief Executive Officer**

Madrid, 31st July 2020