Information Security Policy

Drafted by	**Reviewed by**	**Approved by**
Teldat	Head of Information Security	Information Security Committee

CHANGES WITH RESPECT TO THE PREVIOUS VERSION

Edition	**Date**	**Modified sections**
1	24.05.2022	First edition

Table of content

1. Introduction

Teldat needs to be able to guarantee the security of information to offer a high-quality service to its customers and, simultaneously, preserve its business processes. Information Security consists of protecting this data against a wide range of threats to ensure business continuity, minimize risks and maximize business opportunities and the return on investments.

2. Scope of application

This policy is aligned with **Teldat's** global safety guidelines and is applicable to all information (whatever its format, location, means of communication, dissemination, or storage).

3. Goals

a) Guarantee **Teldat's** basic Information Security requirements are met (i.e., completeness, confidentiality, and availability).

b) Provide a framework to manage **Teldat's** Information Security by setting up a standardized risk management process.

c) Ensure **Teldat's** business continuity.

d) Make sure Information Security requirements are particularly complied with in research, development, and product manufacturing processes, as well as in marketing ones.

e) Build trust among **Teldat** customers.

f) Guarantee Information Security without failing to protect other goods and assets belonging to the Company, always in compliance with the applicable legislation and technical and organizational framework.

g) Create and maintain an Information Security Management System that includes the necessary policies, standards, procedures, and guidelines to implement all security requirements in the different corporate areas. This way, Information Security can be continuously assessed.

h) Establish a regulatory framework for the classification, labelling and dissemination of information.

i) Promote the continuous improvement of the information security management system.

4. Principles

The following basic principles apply to **Teldat**'s Security policy:

a) Comply with all legal and contractual requirements that apply to business operations. For the purposes of this policy, this specifically applies to matters related to personal data protection, corporate information, and on-going business processes.

b) Restrict the use made of the information itself (as well as of corporate processing means) to tasks where it's needed for employees to carry out their jobs. No assets can be used for personal benefit.

c) Keep corporate information secret and never disclose it to third parties (unless it is mandatory for business purposes, and always in accordance with the security measures in force).

d) Draft periodic reports on Information Security.

e) All Teldat employees and external partners are responsible for upkeeping information security. Thus, all of them must have received adequate training and be aware of the role they must perform.

5. Responsibilities

Teldat's Management undertakes to adopt all necessary measures to implement, maintain and continuously improve the Information Security Management System, and to meet the requirements applicable to information security. To do so, this Security Policy is made public and internally disseminated within the organization, ensuring all interested parties have access to it. In addition, a person responsible for managing Teldat's Information Security will be appointed.

Moreover, each manager is responsible for guaranteeing the people working for him/her protect the information in accordance with the rules set by **Teldat**.

Information Security protection is a global corporate goal that must be enforced by all company members. As such, employees and external partners must be aware of the security policy in place and follow its procedures, standards, guidelines, and recommendations for all matters that could have an impact on their job or **Teldat**.

If the security policy, guidelines, or applicable legislation (where applicable) is breached, the disciplinary measures or actions defined by **Teldat** will be adopted.

6. Related policies

This Information Security policy is supplemented with several specific guidelines that provide details on the principles that govern particular aspects of information security.

Signed by: Information Security Committee

In Tres Cantos, on 24 May 2022