

Information Security Policy

Abstract

Code:	PO-001
Version:	02
Validity date:	25.02.2025
Classification:	Public
Type:	ISO 27001

	<i>Issuance</i>	<i>Validation</i>	<i>Approval</i>
Role	RSGIS	Risk Management Team	Board of Directors
Name	Uboldi	Lombardini	Bernardini
Signature	<i>(signed in original)</i>	<i>(signed in original)</i>	<i>(signed in original)</i>

1 Scope

Tecniplast SPA (hereinafter -the organization-) is pursuing the target of implementing an Information Security Management System (ISMS) in compliance with the requirements of the UNI CEI EN ISO/IEC 27001:2022 standard (hereinafter also ISO 27001), to guarantee the Confidentiality, Integrity and Availability of the information processed within the identified perimeter of certification. This policy is intended being a tool aimed to:

- enable all the personnel involved to understand, implement and support the principles, commitments and objectives established through the security policy;
- spread knowledge of the organizational methods and behaviors adopted to guarantee the achievement of information security objectives, within the identified perimeter.

2 Main Principles

- **People centrality** - decisive for the effectiveness of business processes and value creation, training, and updating of personnel in a manner relevant to their work activities, defining the skills required to manage the relevant processes, and promoting personnel awareness regarding the specific objectives for information security.
- **Information Management, Security, and Classification** - ensure that assets and related information are properly tracked and classified to facilitate proper use and thus, implementation of appropriate protection measures (e.g., how Confidential or Strictly Confidential Information is shared).
- **IT infrastructure management** - adoption of the technical and procedural best practices to ensure IT security with a view to continuous improvement for the protection of information.
- **Business continuity management** – implementation of a Business Continuity system, with the aim of providing guidelines for managing the company's business continuity, through the analysis and treatment of risks, as well as a Disaster Recovery Plan, designed to allow, in the event of a disastrous event, the timely restoration, or in any case in the shortest time possible, of the functionality of the services provided.
- **Physical security management** - ensuring protection against threats from natural, intentional, and accidental events that can cause harm to people and company's property.
- **Promotion of Security information attitude** - among employees and collaborators thought contractual provisions, sealing relevant responsibilities (e.g. personal data processing authorizations, as well as confidentiality commitments); implementing awareness program for information security, and defining the rules for the correct use of the devices.
- **Management of information security with suppliers** - mitigation of risks associated with third-party access to company's assets by implementing security requirements that must be met.
- **Logical access security** - implementation of a user authentication system, which must include appropriate user profiling and technological and organizational controls.
- **Incident Management** - implementation of an effective system for managing incidents impacting on information and personal data (e.g. appointment of a dedicated team, readiness for action, impact analysis, and remediation) to preserve company's business continuity.

END OF THE DOCUMENT / FINE DEL DOCUMENTO

(This page intentionally left blank) / (pagina intenzionalmente vuota)