The Bylogix s.r.l. Information Security Policy provides a framework for the organization and its stakeholders regarding information security policy and objectives.
Our goal is to ensure maximum security of our customers' information and data.
The main focus is oriented toward safeguarding the following parameters:

- **Confidentiality**: information shall not be accessible to unauthorized parties;
- **Integrity**: information shall not be changed by unauthorized parties, shall not be corrupted, and shall be reliable;
- **Availability**: information shall be accessible to authorized parties within the stipulated time.

Compliance with current legislation and in particular with the European Data Protection Regulation (GDPR) must also be ensured.

To ensure that these objectives are fulfilled, the organization is committed to making available the resources necessary to meet the **applicable requirements** outlined in TISAX and ISO/IEC 27001, so that the operating procedures defined by the Information Security Management System (ISMS), policies, and all controls applicable to the organization's perimeter are followed and implemented.

Specifically, the purpose of the Information Security Management System (ISMS) is to ensure:

- full knowledge and assessment of the criticality of the managed information through appropriate **risk analysis** activities;
- **secure logical access** to information under the principle of “need to know”;
- full **awareness** of all those involved in processes related to information security;
- that the **organization and any third parties** involved cooperate in the processing of information by adopting procedures to comply with appropriate levels of security, in accordance with ISMS procedures and policies;
- the **timely recognition** of events, anomalies and vulnerabilities so that their proper management ensures the protection of information and minimization of impacts on business processes and stakeholders.
- that **physical access** to the premises and areas is allowed only to authorized personnel;
- compliance with legal requirements and security commitments established in contracts with relevant parties;
- the **continuity of business processes** through the definition and application of appropriate Business Continuity Plans that include adequate Disaster Recovery Plans.
- That personnel and third parties involved in processing and management of data are appropriately **trained** in information security, acquiring the necessary awareness for the proper handling of data and information.
- That **suppliers** are properly audited, as applicable, through contract clauses, audits, monitoring activities, sharing of plans and improvement actions;
- that in **projects**, both internal and for clients, security requirements are appropriately considered from their design (according to the principle of security & data protection by design), as well as in the implementation of products and throughout the service provision phase;
- that information security **events** and **incidents** are promptly identified, analysed, evaluated and dealt with in order to prevent them or reduce their impacts, balancing them with business risk, its sustainability and its predisposition to innovation
- that every opportunity for **improvement** is identified and analysed so that it can be seized

- that the **processing of personal data**, is done in compliance with the European Data Protection Regulation (GDPR) 679/2016.

The organization has established a **risk assessment methodology** based on the guidelines of ISO/IEC 27005, and has identified appropriate **targets** (KPIs), together with related monitoring parameters, for the performance management of the ISMS.

The information security management system is constantly monitored and updated to ensure its **continuous improvement**, also with the help of periodic audits to which all stakeholders are subjected on a regular basis, in order to maintain a high level of awareness of information security.

This policy is shared and made available with the organization and all stakeholders through the intranet system and specific **communication** channels.

The organization has also defined precise **responsibilities** for the definition and management of the ISMS, in particular by providing a specific role assigned to the Information Security Manager (Security Manager).

Grugliasco, **26/09/2024**