INFORMATION SECURITY POLICY

Kido DYNAMICS wants to protect its customers and business objectives by providing stakeholders with a secure working environment and information through appropriate control measures and operational processes.

The principles to be guaranteed are:

- **Confidentiality**: The information must be known only by authorised persons.
- **Integrity**: The information must be complete, accurate, valid and not subject to manipulation.
- **Availability**: The information must be always accessible to authorised users and ensure its persistence in the event of any eventuality.

Information security must be flexible, effective and support the company's business model:

- Access to information must be controlled and based on the person's role in the organisation.
- The services provided must be secure from any access point when connected to the company's infrastructure.
- Security measures must ensure the requirements of confidentiality, integrity and availability of information and services.
- Security measures must guarantee the privacy of personal data according to compliance with current legislation and contractual terms with customers and users.
- Information security must be aligned with the business' organisation, the security requirements of our customers, applicable legislation and good industry practices.
- The organisation counts with has an integrated Information Security Management System that has been approved and is driven by the Senior Management.
- The organisation relies on the continuous improvement of both the production processes and the effectiveness of the Management System in which preventing errors is a fundamental aspect.

This policy is reviewed and approved by the CEO of KIDO DYNAMICS on an annual basis or whenever significant changes occur to ensure its adequacy and effectiveness.

Applicability of the Policy

This information security policy is mandatory within its scope. Employees, collaborators, subcontractors, and suppliers of the company must know and comply with this policy in accordance with their role when dealing with information about the company or its customers.
This policy is based on the standards established by the international standard ISO/IEC 27001:2013. The application of the standard entails a risk analysis carried out on the organisation's information assets resulting in the provision of controls that eliminate or minimise such risks.

Scope of use of the policy

This policy lays down minimum requirements to ensure business continuity. Effective information security is a joint effort that requires the involvement of all employees and employees of the company who work with information assets. The information security policy applies to all information assets: services provided, people, technology, suppliers, and infrastructure.

CEO
KIDO DYNAMICS

Lausanne, May the 17th 2021