

INFORMATION SECURITY POLICY

BLINKAY, aware of the challenge of maintaining the security of both their data and those that their clients trust, adopts and promotes this Information Security policy.

The information must be generated, processed, and controlled under the security levels established by BLINKAY so that it remains protected against loss, manipulation or unauthorized disclosures. These security levels are on the controls of the ISO / IEC 27002 in accordance with the objectives established in the ISO / IEC 27001 current Standards.

For this, BLINKAY establishes an Information Security Management System whose main objective is the preservation of the Security dimensions:

- **Confidentiality:** ensuring people and processes that have the respective authorization or permissions can only access the information.
- **Integrity:** preserving the veracity and completeness of the information and the processing methods.
- **Availability:** granting that authorized users have access to the information and the processes or technology that support it, when required.

The Management undertakes the following commitments:

- Develop controls and control objectives that allow identifying and evaluating the risks of information assets.
- Comply with business requirements, legal provisions, regulations and contractual security obligations.
- Provide the resources and responsibilities to implement and maintain the process of continuous improvement in the management of Information Security.

All BLINKAY staff must assume and support the achievement of these objectives. Likewise, it is responsible for preserving the confidentiality, integrity and availability of the information assets in compliance with this policy and the objectives of the organization.

Barcelona, April the 4th, 2023


The CEO