# INFORMATION SECURITY POLICY

At **iDISC INFORMATION TECHNOLOGIES, S.L.**, information must always be protected, however it is shared, communicated, or stored.

**Introduction**

Information can exist in different forms: printed or written on paper, electronically stored, sent by mail or electronic means, shown in projections, or orally in conversations.

**iDISC depends on ICT systems to achieve its aims.**
**These systems must be administered to protect them against threats and vulnerabilities that may affect the availability, integrity, or confidentiality of the information that we process or the services that we provide, in order to ensure business continuity, minimize business risks, and maximize return on investments and business opportunities.**

**Scope**

This policy supports the organization's general Integrated Management System Policy, it applies to all iDISC ICT systems, and it must be considered by everyone working or collaborating with the company, without exception.

**Information Security Aims**

- Avoid or prevent security incidents through risk assessment and treatment.
- Detect anomalies in the provision of services through monitoring and analysis mechanisms.
- Respond effectively to security incidents.
- Ensure the availability of critical services through continuity and recovery plans.
- Protect the confidentiality of personal data, in accordance with GDPR 2016/679.

**Information Security Principles**

- This organization evaluates risks and tolerates or treats those that, based on the assessment, must be monitored or treated.
- All personnel must be informed about any information security policies relevant to undertaking their work.
- Funding will be available for the operational management of information security-related controls.
- Possibilities of fraud relating to abusive use of information systems will be covered within overall information systems management.
- Information security risks must be monitored, and relevant measures must be taken for any changes that imply an unacceptable level of risk.
- The criteria for risk classification and acceptance are referenced in the ISMS documentation.
- Situations that may expose the organization to breaches of laws and legal regulations will not be tolerated.

**Regulatory Framework**

- *National Security Scheme (ENS - Esquema Nacional de Seguridad) - Provision 7191 of Spanish Royal Decree 311/2022, of May 3, regulating the National Security Scheme.*
- General Personal Data Protection Regulation (GDPR - EU*) 2016/679 of the European Parliament and of the Council of April 27, 2016*.
- Spanish Organic Law on the Protection of Personal Data and Guarantee of Digital Rights (LOPDGDD - Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales) - *Law 3/2018, of December 5*.

**Responsibilities**

- The management team is responsible for ensuring that information security is correctly managed throughout the organization.
- The management team appoints the individuals in charge of the Security Committee, in line with the procedure established in compliance with the National Security Scheme.
- Each head of department is responsible for ensuring that those working under him/her protect information in accordance with the standards established by the organization.
- The security manager advises the management team, provides expert support to the organization's personnel, and ensures that information security status reports are available.
- Each personnel member is responsible for maintaining information security within the activities related to his/her position.

**Related Policies and Standards**

- Integrated Management System (IMS) Policy
- Acceptable Use Policy
- Mobile Device and Remote-Working Policy
- BYOD (Bring Your Own Device) Policy
- Information Classification Policy
- Back-Up Policy
- Internal Personnel Statement on Personal Data Protection - GDPR
- Confidentiality Agreement - NDA

**These policies/standards/procedures must be communicated to employees and external stakeholders**.

Olesa de Montserrat, May 22, 2023

The Managing Director