MANAGEMENT COMMITMENT.

The Management of PANGEANIC BI EUROPA, S. L., represented in the Information Security Management Committee composed of MANAGEMENT itself and the INFORMATION TECHNOLOGY and QUALITY departments, considers Information Security and personal data security to be vital aspects of the business strategy in order to ensure the achievement of business objectives, maintaining the obligation to ensure maximum security of the services provided, i.e. the confidentiality, integrity and availability of data, systems and/or communications managed by PANGEANIC BI EUROPA, S. L.

The Management of PANGEANIC BI EUROPA, S. L. is committed to leading and promoting security at all levels in accordance with the Security Policy and the objectives defined and approved therein, both in general and in particular, and has created an Information Security Management System (ISMS) that is articulated in a way that meets the legal or regulatory requirements, manages the protection and distribution of the organisation's assets, and is distributed and published in the corporate network for better employee awareness.

The present policy was elaborated with the consensus of the personnel included in the scope of the ISMS and has been accepted by the Information Security Management Committee of PANGEANIC BI EUROPA, S. L.

The Information Security Management Committee of PANGEANIC BI EUROPA, S. L. is committed to ensuring the understanding and involvement of all personnel in achieving the objectives of the ISMS.

This policy shall be reviewed annually and shall be modified when the Committee deems it appropriate for the continuous improvement of the policy.

SECURITY POLICIES

OBJECTIVE

Protect the information resources of PANGEANIC BI EUROPA, S. L. and the technology used for its processing, against threats, whether they be internal or external, deliberate or accidental, in order to ensure compliance with the confidentiality, integrity, availability, authenticity and traceability of information.

Provide management, direction and support for information security in accordance with business requirements and relevant laws and regulations.

Maintain the Security Policy updated, in order to ensure its validity and level of effectiveness.

SCOPE AND APPLICATION OF SECURITY

The information security policy shall be applied in all areas of the company as a basic policy, to its resources and to all processes, whether internal or external, linked to the entity through contracts or agreements with third parties.

RESPONSIBILITIES

All PANGEANIC BI EUROPA, S. L. managers are responsible for the implementation of this Information Security Policy, within their areas of responsibility, as well as the compliance to this policy by their work team.

The Information Security Policy is mandatory for all personnel of the organisation, in all areas and regardless of the level of tasks they perform.

Management is responsible for approving this Policy and is responsible for authorising its modifications. They shall be responsible for supervising that the ISMS is correctly applied by the users and themselves.

Area and Department heads shall perform functions related to the security of the organisation's information systems, including the supervision and implementation of all aspects of the topics covered in this Policy. They shall implement and monitor compliance with the policies, procedures and practices defined in this policy.

The Information Owners (from a technical, not legal, point of view) are responsible for classifying the information according to its degree of sensitivity and criticality, documenting and keeping the classification updated, and defining which users should have access permissions to the information according to their functions and competence.

The Quality Manager shall be responsible for notifying all incoming personnel of their obligations with respect to compliance with the Information Security Policy and all rules, procedures and practices arising therefrom. Likewise, they will be in charge of notifying all personnel of this Policy, of any changes that may occur, of the implementation of the confidentiality commitments subscription and of the continuous training tasks in security matters.

The users of the information and of the systems used for its processing are responsible for knowing, making known, complying with and enforcing compliance with the Information Security Policy in force.

GENERAL ASPECTS

This Policy consists of a series of guidelines on specific aspects of Information Security, which include the following topics.

- The information assets of PANGEANIC BI EUROPA, S. L. will be identified and classified in order to establish the necessary protection mechanisms.
- PANGEANIC BI EUROPA, S. L. will define and implement controls to protect information against violations of authenticity, unauthorised access, loss of integrity and to ensure the availability required by customers and users of the services offered by the organisation.
- All employees and/or contracted personnel providing a service shall be responsible for protecting the information they access and process, in order to prevent its loss, alteration, destruction or misuse.
- Only authorised software that has been legally acquired by the organisation will be allowed for use.
- It is the responsibility of all employees and contracted personnel providing a service to PANGEANIC BI EUROPA, S. L. to report security incidents, suspicious events and misuse of resources that they identify.
- Violations of Information Security Policies and Controls will be reported and dealt with according to contractual and legal provisions.
- PANGEANIC BI EUROPA, S. L. will implement all controls aimed at preventing infringements and violations of civil and criminal law, of obligations established by laws, statutes, rules, regulations or contracts, and of security requirements.

SPECIFIC POLICIES

In order to comply with the general policies, the necessary controls must be generated. Specific policies are generated, which may have procedures, guidelines or directives in order to be clear to all personnel of the organisation:

- Confidentiality agreements.
- Risks related to third parties.
- Proper use of assets.
- Telematic resources and Internet access.
- Email and messaging.
- Technological resources.
- Human Resources Security.
- Physical access control.
- Protection and location of equipment.
- Segregation of duties.
- Protection against malicious software.
- Backup copies.
- Removable media management.
- Logical access control.
- User password management.
- Clean desktop and screen.

- Segregation of networks.

In Valencia*, revised and confirmed in version 0, November 2020.*

Manuel Herranz

Manager of **Pangeanic B.I. Europe.**