Barrabés

Information Security Policy

Security Committee

1.0 Version

Policy

InnovaNext's Security Policy reflects the principles and objectives in terms of information security, the results of which allow our company to achieve its purpose of increasing our clients' sales through the acquisition, generation and quality control of leads.

Through the development, communication and maintenance of this policy, InnovaNext's management shows its commitment to protecting the **confidentiality** of the information with which it operates in the provision of its services, guaranteeing its **integrity** in all the processing processes it carries out, as well as the **availability** of the information systems involved in this processing.

To this end, the Management has defined and implemented an Information Security Management System that allows the company to guarantee that the information systems and the information created, collected, stored and processed comply with:

- Security in Human Resources Management, before, during and at the end of the employment relationship.
- Proper asset management involving the classification of information and handling of media, and the establishment of robust logical access control to its systems and applications, managing user permissions and privileges.
- Protecting the facilities and the physical environment by designing secure work areas and securing equipment.
- Ensuring the security of operations by protecting against malware, backing up, logging and monitoring, and controlling software in operation.
- The management of technical vulnerabilities and the choice of appropriate techniques for auditing systems.
- The security of communications, protecting the networks and the exchange of information.
- The assurance of security in the acquisition and maintenance of information systems, limiting and managing change.
- The realization of a secure software development, separating development and production environments, and performing the appropriate functional acceptance tests.
- The control of relationships with suppliers, contractually demanding compliance with the relevant security measures and acceptable levels in their services.
- Efficiency in the management of security incidents, establishing the appropriate channels for their notification, response and timely learning.
- The implementation of a business continuity plan that protects the availability of services during a crisis or disaster.

- Identifying and complying with applicable regulations, with special emphasis on intellectual property and personal data protection.
- Periodic review and continuous improvement of our information security management system to ensure compliance and effectiveness of these requirements.

All the staff of the organization has the duty to comply with this policy, for which the Management has the necessary means and sufficient resources for compliance, and assumes the responsibility to communicate it and keep it accessible to all interested parties.

CEO of Barrabés
Madrid, July 5th, 2021

[redacted]