Boslan's management recognises the importance of identifying and protecting its information assets, avoiding destruction, disclosure, unauthorized modification, and unauthorized use of any information relating to customers, employees, strategy, management, and other concepts; committing to develop, implement, maintain, and continuously improve the Information Security Management System (ISMS).

Information security is characterised as the preservation of:

A) Its confidentiality, making sure that only people who are authorized can have access to this information.
B) Its integrity, making sure that the information and its processing methods are exact and complete.
C) Its availability, making sure the authorized users have access to the information and its associated assets whenever they require.

Information Security is accomplished by implementing a series of adequate controls, such as policies, practices, and procedures. These controls have been established to make sure that the specific security objectives set Boslan are met.

It is Boslan's security policy that:

1. Objectives relative to Information Security are annually established.
2. A process of risk analysis is developed, and given the results, corresponding action is taken and implemented with the means to treat the risks that are considered unacceptable according to the criteria established in the Management Manual.
3. Objectives relative to control and corresponding controls are established, based on the needs that arise relative to risks that come up in during the process of Risk Analysis.
4. To comply with business requirements, legal or regulatory requirements and contractual security obligations, both by BOSLAN suppliers and collaborators.
5. To provide information security awareness and training to all personnel.
6. To establish the necessary means to guarantee the business's continuity.
7. All personnel are required to register and report any breach of security in information, or violations of security, either confirmed or suspected.
8. All personnel are responsible for the preservation of confidentiality, integrity, and availability of information assets in the accomplishing of this here policy and of the policies and procedures inherent to the ISMS.
9. The Information Security Officer is directly responsible for the maintenance of this policy by providing advice and guidance for its implementation, as well as investigating any reported violation or security breach by staff.
10. This policy is available for all our clients and any relevant interested party, and our employees are conscious of our compromise and of content included in this policy.

Bilbao, 8th March 2023

Nekane Aguirre

General Director