INFORMATION SECURITY POLICY

Information, one of the most important assets of Kube and its partners, is exposed to internal or external, intentional or accidental risks and threats. Kube offers its customers, suppliers, consultants and workers a safe working environment through the appropriate procedures and safety measures, implementing an information security policy based on three basic principles:

• Confidentiality: information must be known exclusively by authorized persons

• Integrity: information must be maintained accurately, not manipulated neither altered by people or unauthorized processes

• Availability: information must be accessible to any authorized person at any time, when required

This policy involves all the staff of Kube Group and all departments of the organization. Management staff declares the commitment of Kube with the design, implementation and maintenance of an Information Management Security System that guarantees that the information of the organization, its collaborators and clients is reasonably protected.

Objectives and responsabilities

Kube faces risk taking, tolerating those that are understandable, controlled and treated when necessary.

All Kube Group staff will be informed and responsible for the security of information relevant to the performance of their work.

The risks in information security will be monitored and the relevant measures will be adopted when there are changes that imply a level of unacceptable risk.

The management team of Kube is responsible for ensuring that information security is properly managed. Each manager will be responsible for ensuring that the people working under their control protect the information in accordance with the rules established by the management team of Kube. Each employee is responsible for maintaining the security of the information within the activities related to their work.

Related policies

ISMS Policy
Data Protection Policy
Clean Desk Policy
Server Malware Protection Policy
Incidents Management
Acceptable Use Policy

ISMS POLICY

Information is one of the most important assets of Kube and its partners, and therefore information systems must be adequately protected. Inadequate protection affects the overall performance of the company, and can adversely affect the image, reputation and trust of customers and consultants.

The objective of information security is to ensure business continuity and minimize the risk of damage by preventing security incidents, as well as reducing their potential impact when unavoidable.

To this end, Kube has implemented a management methodology for analyse the degree of exposure of its assets to threats and vulnerabilities that may impact the activities or processes of Kube, whether they occur deliberately or accidentally.

The success of this methodology is based on the contribution of all employees in terms of security, by communicating to the heads of Kube of any relevant consideration in the annual meetings that allow adapting the policies in case of changes in the levels of protection.

The principles in the security policy seek to ensure that future decisions are based on preserving the confidentiality, integrity and availability of the relevant information of Kube. All employees collaborate in the application of the proposed policies.

The daily use of computers by Kube Group employees determines compliance with the principles and policies established, and an inspection process to verify their compliance.

Security policies will remain available on the company's internal server for consultation by Kube employees.

It’s the responsibility of Kube Head Directors to approve and develop this information security policy that ensures:

- The protection of information against any unauthorized access

- The confidentiality of information, especially the one related to the personal data of employees, consultants and customers
- The integrity of the information
- The availability of the information for the proper development of the business
- Compliance with current and future regulations
- The security policy update
- The awareness, education and training of Kube employees in information security
- The control, investigation and management of any event related to information security

To this end, the Board of Directors will take all appropriate measures, including support measures such as outsourcing and support from companies specialized in security management.

Compliance with this policy is mandatory for all personnel and collaborators of Kube.