INFORMATION SECURITY POLICY

We inform our customers and suppliers of the existence of Information Security Guidelines established within our organization to demonstrate BLENDHUB's commitment to protecting and guaranteeing the principles of: confidentiality, integrity, availability, authenticity, and traceability of the information handled within the organization.

BLENDHUB's management has established an Information Security Policy, the main purposes of which are:

- To protect, through controls and measures, assets against threats that could lead to security incidents.
- To mitigate the effects of security incidents.
- To establish an information and data classification system in order to protect critical information assets.
- To define responsibilities in the area of information security by creating the corresponding organizational structure.
- To develop a set of rules, standards, and procedures applicable to management bodies, employees, partners, external service providers, etc.
- To specify the consequences of non-compliance with the Security Policy in the workplace.
- To assess the risks affecting assets in order to adopt the appropriate security measures/controls.
- To verify the functioning of security measures/controls through internal security audits.
- To train users in security management and information and communications technologies.
- To control the traffic of information and data through communications infrastructures or by sending optical, magnetic, paper, etc. data media.
- To observe and comply with legislation on data protection, intellectual property, labor, information society services, criminal law, etc., that affects BLENDHUB's assets.
- To protect the organization's intellectual capital so that it is not disclosed or used illegally.
- To reduce the chances of unavailability through the proper use of the organization's assets.
- To defend assets against internal or external attacks so that they do not become security incidents.
- To monitor the functioning of security measures by determining the number of incidents, their nature, and effects.

BLENDHUB Management assumes responsibility for supporting and promoting the establishment of the organizational, technical, and control measures necessary for compliance with this Information Security Policy. It also assumes responsibility for providing the resources necessary to resolve any non-compliance issues and information security incidents that may arise as quickly and effectively as possible, and for implementing the necessary measures to prevent them from recurring.

This Policy will be maintained, updated, and adapted to the organization's purposes, aligning with the organization's risk management context. To this end, it will be reviewed at planned intervals or whenever significant changes occur, in order to ensure that it remains suitable, appropriate, and effective. For its part, all policies and procedures included in the ISMS will be reviewed, approved, and promoted by BLENDHUB Management.

Raúl Fernández

Guillermo Canovas

febrero 2026

www.blendhub.com
info@blendhub.com