Blendhub

INFORMATION SECURITY POLICY

We inform our customers and suppliers of the existence of Information Security Guidelines established in our organisation to show Blendhub's commitment to protecting and guaranteeing the principles of: confidentiality, integrity, availability, authenticity and traceability of the information handled in the organisation.

The Management of BLENDHUB has established the Information Security Policy, whose main purposes are:

- To protect, through controls/measures, assets against threats that may lead to security incidents.
- Mitigating the effects of security incidents.
- To establish an information and data classification system in order to protect critical information assets.
- To define the responsibilities in terms of information security generating the corresponding organiza tional structure.
- To develop a set of rules, standards and procedures applicable to management bodies, employees, partners, external service providers, etc.
- To specify the effects of non-compliance with the Safety 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 conducted by independent auditors.
- To train users in security management and information and communications technologies.
- To control information and data traffic through communications infrastructures or by sending optical, magnetic, paper data carriers, etc.
- To observe and comply with legislation on data protection, intellectual property, labor, information society services, criminal, etc., that affect the assets of BLENDHUB.
- To protect the intellectual capital of the organization so that it is not disclosed or used illicitly.
- 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 control the operation of security measures by finding out the number of incidents, their nature and effects.

The Management of BLENDHUB assumes the responsibility of supporting and promoting the establishment of the organizational, technical and control measures necessary for compliance with this Information Security Policy. As well as, to provide those resources that are necessary to resolve as quickly and effectively as possible, the nonconformities and incidents of information security that may arise, and the implementation of the necessary measures so that they do not occur again.

This Policy will be maintained, updated and appropriate to the purposes of the organization, aligning with the context of risk management of the organization. For this purpose, it shall be reviewed at planned intervals or whenever significant changes occur, in order to ensure that its suitability, adequacy and effectiveness are maintained. For its part, all policies and procedures included in the ISMS will be reviewed, approved and promoted by the Management of BLENDHUB.

Henrik Stamm Kristensen

November 15, 2022