Document	Document ID	First version	Last revised	Classification	Page
Policy	KP0007	2017-07-14	2024-12-03		1 (4)
Document Owner: IT Manager			Approved by: Balco Group Board of Directors		

Information security policy

Content

1. Purpose

The purpose of this policy is to ensure that Information Security in Balco Group AB and its subsidiaries protects all information assets within the company and that the business objectives are achieved. The information security policy shall ensure that:

- Balco Group handles in a uniform way
  - Information security
  - IT security
  - Privacy issues and handling of personal data
- We comply with applicable laws and regulations
- We have an Information and IT security that lives up to the requirements set by authorities, clients, employees and customers

2. Extent

This policy applies to all operations (business areas, supporting units, staffs) and employees or temporary staff within the Balco Group.
In part-owned businesses, representatives of Balco Group shall work to ensure compliance with this policy. Exceptions or exemptions from this policy must be clearly defined and documented. All applications for exemptions must be submitted to the Information Security Officer, who is responsible for approval in consultation with the Group's CEO. Exemptions or requests for derogations shall be accompanied by a plan for when compliance has been achieved again.

3. Content of the policy

Balco Group's information security policy shall contribute to the achievement of the company's objectives and to ensure that the Group is in line with applicable regulations and legislation in the area by managing information and privacy-related risks in a satisfactory manner. The Information Security Policy covers all information stored or processed within Balco Group or, where applicable, by its subcontractors, regardless of media.

3.1 Information security

Information security shall protect Balco Group's operations, employees, customers and other stakeholders and by defining appropriate information security requirements based on applicable legislation, the expectations of the above-mentioned groups, good practices and regular risk assessments. The requirements are intended to ensure that accurate information is available, when needed, but only to the intended audience.

- To protect confidentiality, integrity and access to information, good practices must be applied.
- Strategic decisions on information security shall be made by the management team to ensure that information security governance supports business needs.

- Balco Group shall regularly carry out risk analyses and plan appropriate countermeasures to ensure good information security.
- Premises and technical facilities must be protected with appropriate physical security measures.
- All personnel affected by the policy shall be regularly informed of the risks of deficiencies in information security and their responsibilities.
- When purchasing IT services or resources, information security aspects must be taken into account in the specification of requirements.

3.2 IT security

IT security is an essential part of information security and must ensure an appropriate level of protection for the IT services, IT systems and IT infrastructure where information is processed or stored.

- A system list shall be drawn up for business-critical systems where system owners, information content and other information needed to enable effective IT security management are documented.
- Access control shall be used to ensure that only intended users have access to the systems and that access is relevant to their role.
- Balco Group shall regularly carry out authorisation reviews to ensure that users and their access rights are kept up to date.
- Systems (servers and virtual servers) must be protected against malware, have access control, log functions, backup routines and other appropriate security measures.
- Teleworking shall be enabled with appropriate security measures.
- Balco Group shall use relevant technology and processes to ensure that communication both externally and within the Group takes place in such a way that the business is protected against attacks.
- Security incidents must be handled by staff with appropriate skills and mandates.
- Appropriate IT security measures shall be defined and applied when agreements with suppliers are drawn up, these shall include opportunities for follow-up.

3.3 Privacy and handling of personal data

Balco Group shall comply with applicable legislation in all countries where operations occur to ensure that employees' and other stakeholders' rights in relation to personal integrity are not violated. IT and information security requirements shall be applied to ensure that appropriate security measures are taken to protect personal data based on the degree of sensitivity. Processes and IT services shall be carried out to ensure compliance with data protection legislation. Preparations must take place and appropriate governing documents as well as documented roles and responsibilities must be in place so that Balco Group can demonstrate compliance with local legislation as well as the EU Data Protection Directive (GDPR) in the event of

a request for review from the Swedish Data Protection Authority in order to avoid sanctions and damage to Balco Group's brand.

- There shall be a list and classification of employees' and other stakeholders' personal data that is processed within Balco Group or by a subcontractor on behalf of Balco Group, regardless of the media on which it is stored.
- System dependencies must be documented to ensure that there is a clear, up-to-date view of where personal data is processed, stored and transferred.
- Systems containing personal data shall be protected through IT security controls, including but not limited to access control, backup procedures and, if necessary, encryption.
- When procuring IT services or systems where personal data can be processed, the principles of privacy by design must be taken into account.
- In the case of outsourcing, there must be an agreement on how personal data is handled and where it is stored.
- Data processing agreements must be signed with all subcontractors who handle any form of personal data on behalf of Balco Group.
- Periodic risk assessments must be carried out to ensure corrective action in areas where sensitive personal data may be lost or compromised.
- IT incident response shall include a step to assess whether an incident is subject to notification of data loss violation.

4. Roles and responsibilities

- This policy is approved by the Board of Directors.
- The CEO is ultimately responsible for ensuring that Balco Group fulfils the obligations in this policy by initiating the establishment of the necessary governing documents, appointing roles and areas of responsibility, processes and controls.
- The CEO is responsible for enforcing this policy, for implementing and monitoring compliance.
- The IT manager is responsible for IT security, including defining requirements and implementing them.
- System owners are responsible for data protection requirements and must ensure that the necessary IT security controls are implemented in their systems.

5. Compliance criteria

In order for this policy to be considered compliant, the following criteria must be met:

- The policy must be approved by the board
- The policy must be communicated and anchored in the management team
- The policy shall be readily available to all staff concerned
- The policy shall be revised annually and updated as necessary