Information Security Policy

1 Purpose

The purpose of this policy is that the information security of Balco Group AB and its subsidiaries (hereinafter Balco) protects all information assets within the company and that the business goals are achieved.

The information security policy shall ensure that:

- Balco handles in a uniform way
  - Information security
  - IT security
- Integrity issues and personal data processing.
- We follow applicable laws and regulations.
- We have information and IT security that meets the demands made by the authorities, clients, employees and customers.

2 Scope

This policy applies to all activities (business areas, supporting units, staff) and employees or agency staff at Balco Group AB (hereinafter referred to as Balco).

In co-owned operations, Balco representatives shall work to achieve compliance with this policy.

Exemptions or dispensations from this policy must be clearly defined and documented. All applications for exemptions shall be submitted in writing to the information security officer, who is responsible for approval in consultation with the group CEO. Exemptions or requests for dispensation shall be accompanied by a plan for when compliance has once again been achieved.

3 The content of the policy

The information security policy at Balco shall contribute to achieving the objectives of the business and that the group is in line with applicable regulations and legislation in the area by managing information and integrity-related risks in a satisfactory manner. The information security policy covers all information that is stored or processed at Balco or, where applicable, its subcontractors, regardless of media.

3.1 Information security

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

- In order to protect confidentiality, integrity and access to information, good practice shall be applied.
- Strategic decisions on information security shall be taken by the management group to ensure that information security management supports business needs.
- The Balco shall regularly perform risk analyses and plan appropriate countermeasures to ensure good information security.
- Premises and technical facilities shall be protected by appropriate physical security measures.

- All personnel who are affected by the policy shall be regularly informed of the risks of breaches of information security and their responsibilities.
- When purchasing IT services or resources, the information security aspects shall be taken into account when setting requirements.

3.2 IT security

IT security is an essential element of information security and shall ensure an appropriate level of protection for the IT services, IT systems and IT infrastructure in which information is processed or stored.

- A system list shall be established for company-critical systems in which system owners, information content and other information necessary 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 the access is relevant to their role.
- Balco shall regularly perform authorisation reviews to ensure that users and their access rights are kept up to date.
- Systems (servers and virtual servers) shall be protected against malware and have access control, log functions, back-up routines, and other appropriate security measures.
- Working remotely shall be enabled with appropriate safety measures.
- Balco shall use relevant technologies and processes to ensure that communications, both externally and within the group, occur in such a way that the business is protected from attack.
- Security incidents shall be handled by suitably qualified and mandated personnel.
- Appropriate IT safety measures shall be defined and applied when contracts with suppliers are established; these shall enable follow-up.

3.3 Integrity and personal data processing

Balco shall comply with applicable legislation in all countries where it has activities to ensure that the rights of employees and other stakeholders relating 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 level of sensitivity. Processes and IT services shall be performed so as to ensure compliance with data protection legislation.

Preparations shall be made and appropriate governing documents and documented roles and responsibilities shall be in place so that Balco can demonstrate compliance with local legislation as well as the EU General Data Protection Regulation (GDPR) in the event of a request for investigation by the Swedish Data Protection Authority, so as to avoid sanctions and damage to the Balco brand.

- There shall be a list and classification of the personal data of employees and other stakeholders that is processed at Balco or by subcontractors on behalf of Balco, regardless of the media in which they are stored.
- System dependency shall be documented to ensure that there is a clear and up to date view of where personal data is processed, stored and transmitted.
- Systems that contain personal data shall be protected by IT security controls, including but not limited to access control, back-up routines and, if necessary, encryption.
- When procuring IT services or systems in which personal data can be processed, the principles of privacy by design shall be observed.
- When outsourcing, there shall be an agreement on how personal data is processed and where it is stored.

- A Personal Data Processor Agreement shall be signed with all subcontractors who handle any form of personal data on behalf of Balco.
- Periodic risk assessments shall be carried out to ensure corrective action on areas where sensitive personal data could be lost or compromised.
- IT incident management shall include a step to assess whether an event is subject to notification of a breach of data loss.

4 Roles and responsibilities

- This policy is approved by the board of directors.
- The CEO is ultimately responsible for ensuring that Balco fulfils the obligations of this policy by initiating the preparation of necessary governing documents, designating roles (which can be combined) and areas of responsibility, processes and controls.
- The CEO is responsible for maintaining this policy, for implementation and for monitoring compliance.
- The head of IT 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 Criteria for compliance

For compliance with this IT policy the following criteria shall be met:

- The policy shall be approved by the board of directors.
- The policy shall be communicated to and endorsed by the management group.
- The policy shall be communicated to all affected personnel annually in connection with quality monitoring.
- The policy shall be readily available to all affected personnel.
- The policy shall be reviewed annually and updated as necessary.

6 Other document

- IT policy