Information Security Policy

1. Purpose

1.1. To provide security guidelines on information, ALPEK's or of third parties in custody, in the infrastructure where it is located with the purpose of implementing controls to help minimize any risk that may jeopardize information confidentiality, integrity and availability.

2. Scope

2.1. This policy is applicable to:

- Alpek, its subsidiaries and organizations under its control, in all countries where it holds operations.
- Every employee, executive, director or board member of the company, notwithstanding hierarchical levels or roles (duties).

3. Responsibilities

3.1. ALPEK Employees / Individual having any relationship with ALPEK:

- Carry out daily activities in compliance with provisions herein.

3.2. ALPEK Companies

- Ensure anything herein is enforced.

3.3. ALFA Internal Audit:

- Verify that anything herein is enforced.

3.4. Information Security Executive Committee:

- Validate and propose Information Security Policies and Guidelines.
- Promote in all areas of ALPEK and ALPEK Companies the need and importance of Information Security.
- Ensure Information Security program is implemented in ALPEK.

3.5. Information Security Tactical Committee:

- Define and document Information Security policies, guidelines and standards.
- Be updated on Information Security threats that may impact the organization.
- Keep updated on Information Security threats that may impact the organization as well as on applicable laws and external regulations.
- Investigate, evaluate and propose projects as well as technologies to keep ALPEK's Information Security practices updated.

3.6. Information Security Committee of the Company:

- Promote the implementation of methodologies, standards and guidelines applicable to the functions by this Committee.
- Promote Information Security culture in its Company.

4. Guidelines and Procedures

4.1. Definitions

4.1.1. Confidentiality

- A characteristic that guarantees information may only be provided to authorized individuals.

4.1.2. Control

- Policies, procedures, practices, technologies and organizational structures designed to achieve business objectives and to prevent, detect and correct undesired events.

4.1.3. IT infrastructure

- Hardware or software used to store, process or transmit information.

4.1.4. Guideline

- Security measure that must be implemented.

4.1.5. Safe operation

- Operation free from security incidents or interruptions that may jeopardize information confidentiality, availability and integrity.

4.1.6. Others in custody

- A characteristic that guarantees information may only be provided to authorized individuals. Assets in the custody of and not owned by ALPEK.

4.1.7. Information Security

- Measures, procedures and controls intended to preserve confidentiality, integrity and availability of information according to Company requirements.

4.1.8. IT systems

- Specific-purpose software partially or fully supporting business processes of the Companies.

4.1.9. Malicious software

- Computer code intentionally introduced in a system for unauthorized purposes.

4.1.10. Incident

- An unplanned event that impacts the operation of a Company.

4.2. Guidelines

- It is an ALPEK policy to have all its Companies implement proper measures to maintain security while information is being managed and controlled, to protect information against improper use, modification and unauthorized destruction and to ensure information confidentiality, integrity and availability.

  ALPEK and it subsidiaries shall abide by the following Security Guidelines.

4.2.1. Security Organization

- ALPEK has defined an Information Security Executive Committee to coordinate all efforts related to the definition and maintenance of this Policy and its Guidelines. Likewise, every Subsidiary shall have clearly defined and assigned roles within its organization to manage information security according to provisions herein.

4.2.2. Information Classification

- Every ALPEK Company shall classify its information based on sensitivity, criticality and value to regulate its use, safekeeping and destruction.

4.2.3. IT Infrastructure Control

- Every ALPEK Company shall implement a process to manage IT infrastructure assets in order to keep control of their location and to define proper protection measures.

4.2.4. Personnel Management

- Every ALPEK Company shall implement Information Security controls required in Selection, Recruitment and Human Resources Management processes to ensure this Policy is known and observed by all personnel, whether in-house, subcontracted or outsourced rendering services to ALPEK.

4.2.5. Physical Security

- Every ALPEK Company shall implement controls to establish and maintain a safe operation of its IT infrastructure with the purpose of preventing information loss or theft.

4.2.6. Systems and IT networks management

- Every ALPEK Company shall have processes and controls to ensure information is protected while the IT infrastructure is being operated and to guaranty confidentiality, availability, and integrity.

4.2.7. Logic access control

- Every ALPEK Company shall implement protection controls to ensure IT infrastructure and information is accessed by authorized personnel only in compliance with the guidelines defined for such purpose.

4.2.8. Systems development and maintenance

- Every ALPEK Company shall implement security controls while developing, deploying, processing and maintaining IT systems being used in order to protect ALPEK's intellectual property and to guarantee information integrity, confidentiality and availability.

4.2.9. Business continuity

- Every ALPEK Company shall implement Business Continuity programs for information assets supporting critical business processes that may affect business operations if they get interrupted due to acts of God, natural causes or actions by individuals.

4.2.10. Compliance with laws and regulations

- Every ALPEK Company shall abide by security requirements provided by laws and/or contract regulations of the countries it operates by implementing the necessary controls in the design, operation and use of its IT infrastructure and information systems.

4.2.11. Management of information security incidents

- Every ALPEK Company shall ensure incident management is organized and effective so as to have a communication that enables detection and correction of incidents on time.

4.2.12. Supplier management

- Every ALFA Company shall guarantee information and IT infrastructure are protected when business relations are established with Service Suppliers.

Every ALPEK Company is responsible for implementing an Information Security Risk Management process aimed at IT infrastructure and its operation in accordance with this Policy.
Every ALPEK Company shall carry out periodical checks to ensure compliance with this Policy. In the event faults are detected, corrective action plans shall be implemented.

General Premise: All Alpek subsidiaries must be aligned with the regulatory framework established in the Alpek Policies. The policies of each subsidiary may have different conditions, but never less restrictive than the framework established by the Alpek Policy.

Approvals

Name	Position	Date of Approval
José Armando Ramos Cantú	Vice President Human Capital	February 26th 2021
José Carlos Pons de la Garza	Chief Financial Officer	February 26th 2021
José de Jesús Valdez Simancas	Chief Executive Officer	February 26th 2021