LIFCO
A SAFE HAVEN FOR YOUR BUSINESS

It was resolved by the Board of Directors of Lifco AB (publ) (Reg. No. 556465-3185) (the "Company") at a meeting held on 1 February 2024 to adopt this

IT Policy

Introduction and Purpose

Lifco is committed to safeguard people and information, while at the same time mitigating overall IT risk. This Policy constitutes a comprehensive, high-level framework and provides the overall requirements for Lifco AB and each subsidiary's IT strategy.

When using "Lifco" in this Policy, this should be read as any company in the group or the group as a whole.

Scope

This Policy is valid for all Lifco's subsidiaries and applies to all employees and directors, as well as consultants, contractors and agency personnel who work at Lifco's premises or under the direction of Lifco (all referred to in this Policy as "employees").

Principles

The IT structures of Lifco's subsidiaries adds value by providing the best possible service to the respective company, balancing risk and reward with return on IT investment. Every subsidiary must safeguard people and information, while at the same time mitigating overall IT risk. We direct and control our IT functions through structured management, consistent processes and by building strong relationships with the business.

Each subsidiary shall have its own IT strategy and organization. The IT strategies and organisations shall support the subsidiaries' strategic focus areas and thereby enabling successful business strategy implementation. Each subsidiary should strive for building the right level of service based on business needs with jointly elaborated scenarios and plans between operations and IT delivery.

The overall goal of each subsidiary's IT strategy is to ensure a user friendly, cost efficient and secure IT delivery. The use and development of IT shall comply with applicable laws, regulations and other principles such as Lifco's policies.

Information Security

Information security is the practice of defending information from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction.

All Lifco subsidiaries are required to manage information security risks and establish security controls required to protect its information assets regardless of the form the data may take, e.g. electronic or physical backups. The aim is to ensure confidentiality of information, ensure processes for access and availability of systems and ensure integrity of data. This applies to all computer information systems supporting business processes, including application infrastructure, networks and communications, provided IT services, desktops and laptops, mobile devices, and personal devices, i.e. BYODs used for Lifco-related business.

Cybersecurity

All subsidiaries are required to have a plan on how to respond to cyber incidents. The plan should describe roles and responsibilities for those involved with security incident response, defined parameters for declaring, classifying and triaging incidents as well as the security incident response process.

IT Use

All subsidiaries are required to effectively manage and safeguard the use of all IT properties. This includes not only computers and mobiles, but also the use of electronic information systems such as software, file shares, networks, internet access and the electronic mail system.

These systems are used for business purposes, serving the interests of the company and its clients and customers in the course of normal operations. All usage must be in accordance with applicable laws, ordinances, regulations and rules, and, where appropriate, with industry and consensus standards.

IT Cloud

Cloud computing is the delivery of computing services – servers, storage, databases, networking, software, analytics and more – over the internet ("the cloud"). Before selecting, implementing and operating cloud solutions or cloud services, risks and best practices should be considered.

Privacy Principles

Integrity, transparency, and responsibility characterize the way Lifco conducts business. We recognize our responsibility to respect privacy rights and to put in place appropriate standards of data protection when handling personal data of employees and other individuals such as customers´ or suppliers' employees. The purpose is to protect privacy and ensure the secure processing of personal data.

In all aspects of handling personal data Lifco shall comply with laws and regulations applicable to each subsidiary. Data subjects' applicable rights shall always be respected. Personal data is only shared – within and outside each subsidiary and Lifco AB – in accordance with policies, procedures and guidelines. The transfer of data to third parties must be subject to clear terms regarding collection, use, sharing and storage. Third parties must undertake to follow the Group's policy regarding data security and data management. Appropriate measures shall be taken so that the personal data processed is adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed, and that the data is accurate and, where necessary, kept up to date. Measures shall also be taken to consider privacy when designing and building products and services. Employees handling personal data shall receive regular training on data privacy management.

Implementation and Communication

This Policy has been adopted by the Board of Directors and the ultimately responsible for the implementation and follow up is Lifco's Group CEO. The Managing Directors of the subsidiaries are responsible for the respective subsidiaries' IT strategy and organisation as well as the implementation and communication of this policy to their organisations. The Managing Directors shall ensure that all employees have received relevant and up-to-date training in cyber security issues and data management.