10 MAY 2023

Sampo Group
Information Security Principles

SAMPO ⬡ GROUP

Sampo Group Information Security Principles

Approved by Sampo plc Board of Directors on 10 May 2023.

1.   The goal and principles

The goal of these principles is to ensure that Sampo Group protects all types and forms of information according to its sensitivity and importance to Sampo Group and in compliance with applicable rules and regulations.

Information security covers the availability, integrity and confidentiality of information regardless of its form or location, and includes electronic systems used for information processing, transporting or storage. Cybersecurity is a part of information security and comprises technologies, processes, and controls that are designed to protect systems, networks, and data from cyber events. Information security and cybersecurity are both important factors in ensuring that Sampo Group companies are successful in their business operations.

These principles cover the overall principles that apply to the protection of information owned by Sampo Group, and third-party information within the custody of Sampo Group.

2.   Responsibilities

Sampo Group's general governance rests on the idea that Sampo plc, as the parent company of the Group, provides Group companies with a framework of general principles within which the parent company expects the Group companies to organize and carry out their businesses. The responsibility to protect Sampo Group information in line with these principles lies with all Group companies. In addition, every person within Sampo Group is under an obligation to adhere to these Information Security Principles.

National legislation and authority regulations of the country in question are also applicable to Group companies registered outside of Finland. When necessary, the management of such Group companies shall ensure that the company in question has adopted additional directions on information security as required by national legislation.

Group companies shall implement controls protecting information in line with its criticality, internal requirements, external requirements, and identified risks. All controls shall be in line with Sampo Group's framework of general principles and policies as well as applicable laws and regulations and shall be aligned with well-renowned international standards, for example, ISO 27001. All Sampo Group companies shall undergo regular information security reviews, monitoring and audits.

Each Group company shall appoint a person responsible for directing, supervising, and reporting information security activities in line with these principles and in line with applicable legal and regulatory requirements. The role shall have a clear job description detailing the associated responsibilities and will be appropriately segregated to ensure the independence and objectivity of the information security function.

All Sampo Group companies shall provide regular information security and cybersecurity awareness training to their employees. In addition, all Group companies shall have a clear escalation process which employees can follow in the event an employee notices something suspicious.

3.   Reporting

The status of information security controls, risks and material incidents shall be regularly reviewed and reported by Group companies to the Group companies' Board of Directors, as well as to the Sampo Group CISO in line with Sampo Group's Reporting Policy, and Sampo Group Risk Management Principles.

4.   Implementation and compliance

These principles apply to all Sampo Group companies and Sampo Group employees. Breach of internal rules could result in disciplinary action and/or reduced variable compensation.

This document shall be reviewed at least annually.

SAMPO GROUP

Sampo plc

Fabianinkatu 27
00100 Helsinki, Finland
Phone: +358 10 516 0100
Business ID: 0142213-3

www.sampo.com
🐦 @sampo_plc
in Sampo plc
📷 @sampo_oyj