4 FEBRUARY 2026

Sampo Group Information and Communications Technology Security Principles

SAMPO GROUP

Sampo Group Information and Communications Technology Security Principles

1. The goal and principles

The goal of these principles is to ensure that Sampo Group protects all types and forms of Information and Communication Technology (ICT) and information assets according to their sensitivity and importance to Sampo Group and in compliance with applicable rules and regulations.

ICT and information asset security covers the protection of availability, integrity, authenticity and confidentiality of information and electronic systems used for information processing, transporting or storage. Sampo Group ensures that data remains accurate, consistent, and safeguarded from unauthorised access, tampering, or destruction. The protection of these assets is important for ensuring that the Sampo Group companies are successful in their business operations.

These principles cover the overall principles that apply to the protection of ICT and information assets owned by Sampo Group, provided by third-party service providers, 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 the Group companies with a framework of general principles within which the parent company expects the Group companies to organise and carry out their businesses. The responsibility to protect Sampo Group ICT and information assets 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 and Communications Technology Security Principles.

National legislation and authority regulations of the country in question are also applicable to the 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.

The Group companies shall have in place policies and well documented tools, methods and processes to manage ICT risk and implement controls protecting ICT and information assets in line with their 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. The Sampo Group companies shall undergo regular information security reviews, monitoring and audits. The Group companies shall measure their performance regularly and commit to continuous development and improvement of the information security systems.

The Sampo Group companies shall identify the roles and responsibilities for the development, implementation and maintenance of ICT security policies, procedures, protocols, and tools in line with these principles and in line with applicable legal and regulatory requirements. The Sampo Group companies shall have an information security function appropriately segregated from ICT development and operations processes to ensure independence and objectivity.

The Sampo Group companies shall provide regular information security and cybersecurity training to their employees and Boards of Directors. The Group companies shall also have processes to escalate severe cases which employees have identified and reported as suspicious.

3. Reporting

Information security and cybersecurity events and anomalies are continuously monitored, recorded and acted upon according to documented and agreed incident processes. The status of ICT and information assets security controls, risks and material incidents shall be regularly reviewed and reported by the Group companies to their respective 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 can result in disciplinary action and/or reduced variable compensation. In addition, the requirements outlined here regarding information security and cybersecurity are expected to be met by external stakeholders (e.g. relevant partners, suppliers, third-party data processors), who are regularly assessed for risks and compliance.

These principles are reviewed annually and always when deemed necessary due to material changes in the regulatory framework, operating environment or within Sampo Group. All updates and amendments to these principles shall be approved by Sampo plc's Board of Directors.

SAMPO GROUP

Sampo plc

Fabianinkatu 21
00130 Helsinki, Finland
Phone: +358 10 516 0100
Business ID: 0142213-3

www.sampo.com
@sampo_plc
Sampo plc
@sampo_oyj