Information Security Policy

Information Security
Dimitri Goos

Level: Group-wide

Classification: Public

Approval:
Sanoma Corporation Board of Directors - 28.04.2022

1. Purpose and background of the Policy

Sanoma is a learning and media company. We aim at creating better understanding for people, communities and businesses to evolve and thrive. Our learning products and services enable teachers to develop the talents of every child to reach their full potential, while our Finnish media provide independent journalism and engaging entertainment also for generations to come. Data is a critical asset to grow our business and to provide better services to our customers; at the same time regulations require us to demonstrate our accountability in ensuring compliance with data protection laws. Sanoma is committed to secure and protect its data assets, and to continuously improve information security.

Information security controls and measures are selected and implemented so that they support modern digital developments while keeping the risks on an accepted level. This will increase the confidence of customers and business partners and enable Sanoma to be considered a trusted company within a competitive business environment.

This policy provides the information security principles and framework and defines information security practices for the protection of Sanoma's information assets. It forms the foundation for the framework used for implementing and managing information security in practice. Sanoma's security baseline is defined by a set of Sanoma security standards, which have been approved by the President and CEO of Sanoma Corporation and provide security requirements for the entire organization. These standards are supported by related guidelines describing information security practices in detail and are subjected to a continuous improvement cycle.

2. Scope and relationship to other policies

The Information Security Policy and related standards and guidelines apply to all of Sanoma and its subsidiaries. This includes all personnel working for or on behalf of Sanoma including its Business Units, Operating Companies and Domains.

Information and information systems must be protected from unauthorized access, use, disclosure, disruption, modification and destruction, regardless of the form the information may take.

Sanoma's information assets need to be sufficiently safeguarded, in line with the other policies. The following policies have a relationship to the Information Security Policy:

Sanoma Code of Conduct: explains how we aim to conduct our business in an ethical & responsible manner in order to win and retain our customers' trust, and sets out the principles of business conduct applicable to activities throughout the Sanoma Group.

Sanoma Enterprise Risk Management Policy: defines Group-wide risk management principles, objectives and responsibilities.

Sanoma Internal Control Policy: defines the internal control process applied in the Group. Internal controls are in line with the Corporate Governance Framework, and aim to assure that all Group policies and standards are up to date, communicated and implemented.

Sanoma Internal Audit Policy: Internal Audit brings a systematic, disciplined approach to evaluate and improve the effectiveness of corporate governance, risk management and internal control systems.

Sanoma Privacy and Data Protection Policy: enables fair and lawful data processing by establishing the privacy and data protection principles that Sanoma adheres to, and the governance model for organizing the implementation of those principles into our business operations.

3. Information security principles and framework

Information security controls and other measures support business management in ensuring continuity of business operations and mitigating risks to an acceptable level by considering the following components:

Confidentiality:	Information is protected from unauthorized disclosure.
Integrity:	Information is complete, accurate and protected from unauthorized, unanticipated or unintentional modifications.
Availability:	Information is accessible and usable when needed.

Security controls are selected and implemented based on the industry's leading standards (ISO/IEC 27001, ISO/IEC 27701) and their code of practices (ISO/IEC 27002, ISO/IEC 27018)

The aspects considered in information security management should cover at least

- Organization of information security
- Human resource security
- Asset management
- Access control
- Cryptography
- Physical and environmental security
- Operations security
- Communications security
- System acquisition, development and maintenance
- Supplier relationships
- Information security incident management
- Information security aspects of business continuity management
- Compliance

4. Roles and responsibilities

All employees within Sanoma and third parties acting for or on behalf of Sanoma are responsible for information security, individually and as a collective group. The following specific information security roles and responsibilities are necessary to determine, achieve and maintain the required level of security.

Sanoma Board of Directors (BoD) is responsible for ensuring appropriate protection of information assets within the organization and for approving the Sanoma Information Security Policy.

Executive Management Team (EMT) supports the goals and principles of the Sanoma Information Security Policy and is responsible for ensuring the appropriate resources for it.

Chief Information Security Officer (CISO) is the owner of the Sanoma Information Security Policy and as such responsible for defining and maintaining the policy, standards and guidelines and for reporting on compliance and security incidents. The CISO is accountable for Sanoma's information security and facilitates the delivery of high-quality security services to Sanoma.

CEOs of Strategic Business Units are responsible for ensuring the implementation of Sanoma Information Security Policy, Standards and Guidelines on a Strategic Business Unit level. Quarterly reports on the progress of planned security improvement programs and security KPIs are provided by the CISO team.

Local Security Professionals / Security Champions are the enablers for a Sanoma wide implementation of Information Security, responsible for delivering security services locally at their Business Units in cooperation with the CISO team.

Managers, Operations Managers, Architects and Engineers are responsible for designing and implementing Sanoma Information Security Policy, Standards and Guidelines within ICT systems and processes and communicating those to the personnel, contractors and partners.

Group Internal Audit shall give independent assurance on the implementation process and governance of the Sanoma Information Security Policy.

5. Implementation and policy review

This policy is effective until further notice and will be reviewed annually.

The President and CEO of Sanoma Corporation or a person authorised by him or her is entitled to make technical amendments to this policy when necessary.

Date	Approval
11.12.2015	Approved by the Board of Directors' meeting
25.04.2017	Update approved by the Board of Directors' meeting
26.04.2018	Update approved by the Board of Directors' meeting
24.07.2018	Technical amendments approved by the President and CEO
29.04.2019	Update approved by the Board of Directors' meeting
29.04.2021	Update approved by the Board of Directors' meeting
28.04.2022	Update approved by the Board of Directors' meeting