Policy Information Security – Artisti AS

Passed by Artisti AS board. Last modified April 3, 2025.

Policy Statement

We are committed to protecting all information we process. This applies to both our own and that of customers, suppliers, partners and employees.

We have a special responsibility to secure personal information (PII) and intellectual property rights (IPR). We are committed to handling all information in a legal, secure and ethically sound manner.

We recognize that good information security is a prerequisite for trust with our customers and partners. The policy is anchored in the company's board of directors and is reviewed at least once a year.

Scope

Artisti's information security policy applies to all information processing internally in the company and for which the company is responsible externally. This includes all processing, storage and transmission of information both verbally, on paper and digitally. All use of ICT tools is also included. The policy applies to all employees, consultants, suppliers and partners who process information on behalf of Artisti.

Information security goals and principles

Our work with information security is based on the following principles:

- Availability – that the information is available when it is needed.
- Confidentiality – that the information is only available to those who have the right to access it.
- Accuracy and integrity – that the information is and remains accurate, understandable, and complete.
- Traceability – that you can subsequently identify who did what and when.

In addition, the following principles apply:

- Protect customers' personal data and ensure compliance with GDPR and other relevant legislation.
- Protect partners' intellectual property rights and confidential information.
- Ensure that information security is integrated into all work processes and system changes.

Compliance

All information is processed and protected inn accordance with:

- The Working Environment Act
- Act on the processing of personal data (Personal Data Act) (GDPR EU 2016/679).
- Regulation on employers' access to e-mail boxes and other electronically stored material.

Assignment of responsibility

Responsibility for information processing and information security has been assigned to the company's senior management in collaboration with the group's information and data security department in Mediehuset Andvord AS.

Certifications

The group's information and data security department in Mediehuset Andvord AS is certified in ISO 27001:2022.

Risk analysis and system tests

Risk analysis is carried out by the group's security group in collaboration with external experts. Necessary measures for the protection of information are reviewed and followed up. The company's security routines are regularly assessed and if necessary adapted.

Training

There is mandatory training for employees in information and data security. The training covers all information processing, routines and basic data security, and involves online-based courses (Nano Learning). Reports are taken on complete online courses among employees. Through random tests, employees are tested in the safe use of digital platforms and data security.

Quantitative objective: >90% should have always completed both courses in information and data security.

Operational security

We ensure that changes in the business, business strategies or systems for information processing that affect information security are controlled. We have implemented monitoring and processes to identify, prevent and handle data leaks or other security-relevant incidents in the infrastructure.

Communication security

We have endpoint management that enables us to maintain, assess and protect apps and devices. We have established security solutions with monitoring of all devices and endpoints (pc/mac/servers). We have established security solutions with monitoring of all data communication such as file transfer, e-mail, and all cloud-based services.

The solutions involve detection, analysis, and notification to our security personnel if an incident occurs. In the event of serious incidents, the endpoint is automatically isolated until the cause has been clarified and approved by security personnel. We have solutions for analyzing firewalls and storing of logs.

Security procedures

Routines and procedures for information security are described in internal procedural documents. Procedures and routines are reviewed annually or in the event of deviations and incidents that require action.

Deviations and incident handling

All employees have access to the portal for registering deviations. The deviations are sent to the safety officer in the company. Measures are being taken. Deviations are reviewed and changes in infrastructure, processes and organization are assessed.

Whistleblowing

Notifications of unwanted incidents can be directed to the company's top management (ta@artisti.no) or directly to the group's IT operations department (it-avd@artisti.no).

Information and data security systems

This business uses the following software in our systems:

Software	Area of use
Microsoft Intune	Endpoint management solution to manage, assess and protect apps and devices.
XDR (Extended Detection and Response) fra Trend Micro Systems	Endpoint security with monitoring, detection, analysis and notification for all devices, communication channels and cloud-based services for storage.

NanoLearning	Online courses, education and training of employees within information and data security.
ManageEngine Firewall Analyzer	Analysis of firewalls and storage of logs.
Microsoft Azure med Single Sign-on	Access management for users, and provisioning of information to other systems.
NetSecurity / Palo Alto	Network Security from the Palo Alto firewall and network security platform.

Document version log:

Date	Changes applied	Responsible
13.04.2021	Changes in format	Monica Nilsen
24.11.2023	Name change – Artisti Profil AS -> Artisti AS	Monica Nilsen
03.04.2025	Updated clearer commitments and updated certifications and training programs.	Monica Nilsen