Information Security Policy

We offer flexible executive implementation power in a robust secure way

Nordic Interim offers solutions for our clients' needs, based on solid competence and a long experience of leadership. Our customers turn to us in situations when they need qualified managers and experts who at short notice can operationally implement strategies and action plans and thereby create lasting results. This applies in situations where a key role is vacant and needs to be filled as soon as possible when a process, function or business unit must be improved, when a radical change in the company or organization must be carried out or when a company or organization is in serious crisis.

Our mission and vision are to deliver the right solution for each business-critical challenge through our own expertise, competence, and experience, in collaboration with the best interim managers on the market and a global network. Nordic Interim's goal is to deliver quality that meets our customers' expectations. Our work is based on our core values – Sustainability, Simplicity, Team spirit, Ambition, and Innovation.

Introduction to our Security Policy

- Nordic Interim shall maintain an information security management system (LIS/ISMS) adapted to our business in accordance with the ISO 27001 standard. This policy demonstrates the direction of our information security work and establishes our ambition to protect our information assets and ensure the confidentiality, integrity and availability of our information. See the overall information security routine.

Scope of the Security Policy and Overall Goal

- This policy applies to all employees and applies to the management of all Nordic Interim's information assets. The policy also applies to all third parties who in any way come into contact with Nordic Interim's information assets.
- Our overall goal is to ensure that information in processes and technical systems is protected in a way that meets the requirements of our customers, Interim Managers, owners and the legal requirements that affect our business.

Objectives of Information Security

The primary objectives of the Information Security Policy are to:

- Protecting the confidentiality of our information from unauthorized access
- Ensuring that the integrity of our information is maintained throughout its lifecycle
- Ensuring the availability of information when needed
- Comply with legal, regulatory, and contractual requirements related to information security
- Promote a conscious culture of information security within the organization

Management responsibilities

- It is the company's management that is responsible for establishing, implementing and maintaining systematic information security work in the business. This is done by maintaining our information security management system with clearly allocated resources and awareness-raising efforts for employees. This is done by, among other things, allocating resources that are necessary for the effective implementation and maintenance of the information security system.

Information Security Officer

- The company has appointed an information security officer to manage the management system and to ensure that our systematic information security works by identifying, assessing and remediating information security risks.

Employee Responsibilities

- Employees are responsible for complying with the information security policy and its processes.
- Employees also have the responsibility to immediately report any information security incidents or vulnerabilities occurring.

Risk Management

- Nordic Interim has a process for regular risk assessment to identify, evaluate and manage information security risks.

Access to information

- Access to information assets is restricted based on job roles and responsibilities within the company. Assigning, modifying, revoking and regularly reviewing user access is regulated in the established procedure for access management.

Information Security Awareness and Training

- All employees have undergone training on the information security policy and associated procedures. The information security officer keeps staff informed about the latest threats and best practices.

Incident Management

- An incident management process is in place to address any information security incidents. The process includes Discover/Report – Assess – Manage – Restore – Exit.

Compliance

- The organization shall comply with all relevant legal, regulatory, and contractual requirements related to information security. Periodic compliance assessments are conducted.

Monitoring and Review

Regular review of the management system and continuous monitoring of agreed safety measures.

- Regular monitoring and review is carried out to ensure the effectiveness of the management system and safety measures. The information security policy is reviewed annually or as necessary to reflect changes in the organization's structure or regulatory environment.

Through work based on the philosophy of continuous improvement (where we continuously identify ideas for improvement), and with clear routines regarding preventive and corrective measures, we ensure that we achieve our goals.

Stockholm 2 October 2023

Cecilia Brinck Managing Partner Sverige	Björn Henriksson Managing Partner Nordic Region