information security policy

Purpose

This public release policy document serves as a company statement of commitment regarding information security within atNorth. The contents are derived from our internal policy which sets out our commitment in terms of legal, regulatory, customer and internal requirements.

Scope

The policy considers any organizational, people-related, physical, and technological controls to protect its operations and ensures the integrity of information assets belonging to atNorth, customers or other stakeholders in regards of confidentiality, integrity and availability, and covers both internal and external parties.

The policy applies to all information systems, operational locations including future expansions, and cloud infrastructure, personnel, and third-party services used across our EU data center operations. It encompasses all information assets, including data, systems, networks, and physical infrastructure, regardless of the medium on which the information is stored or transmitted.

Commitment & Principles

Information Security within atNorth is executed holistically on a risk-based approach that aims to reduce the overall risk profile of atNorth in partnership with all stakeholders. atNorth´s information security protection concept is based on ISO 27001:2022 ISMS domains: Organizational, People, Physical and Technological. For each of these domains atNorth maintains a robust set of controls to support our dedication to secure all data assets and as well as our strategic objectives:

- To maintain a risk-based, certified Information Security Management System (ISMS) embedded into our business processes that is regularly reviewed and thrives for continuous improvement.
- To ensure compliance with relevant laws, regulations, standards, and internal and external stakeholder requirements.
- To regularly assess threats, test controls, and audit our procedures and systems to ensure resilience, compliance and timely incident management to protect information assets related to our business.
- To verify that information is trustworthy, reliable, available and adequately protected (CIA principle), and to be trusted to process, store and transmit data in a secure and compliant manner.
- To maintain the trust of atNorth among employees, customers, and business partners by ensuring robust protection of both physical and intangible information assets.
- To ensure that information security supports all stakeholders promptly and effectively in their own drive to achieve business objectives.
- To ensure security awareness training of both internal and external stakeholders to efficiently protect information assets related to our business.

atnorth

Responsibilities

atNorth´s Security Committee and Security & Compliance function are responsible for the policy.

Employees and any other third parties are responsible for adhering to the security policy, and all relevant policies, standards, processes, procedures, instructions or any other documentation relating to information security.

References

This policy is aligned with EU and national legislation and regulation related to information security, as well as ISO 27001:2022 standard, or specific contractual commitments.