business continuity and disaster recovery policy

Purpose

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

This document provides requirements for ensuring the resilience of atNorth's business processes across all sites and operations. Given the nature of atNorth's technology operations and the importance of ensuring uninterrupted services to customers, this document covers a wide range of areas, including, but not limited to, geographic coverage, data protection and recovery, data storage, process facilities, and third-party dependencies.

Scope

The scope of this Policy applies to atNorth's critical business processes and their critical applications, considering the potential impacts of disruptions on both a local and global scale.

The policy considers any standard or regulation related aspects 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 BCM related systems, operational locations including future expansions, and cloud infrastructure, personnel, and third-party services used across our EU data center operations. It encompasses all assets contributing to our business continuity and disaster recovery, including people, processes, data, systems, networks, and physical infrastructure.

Commitment & Principles

Business continuity and disaster recovery 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 business continuity concept is based on ISO 22301:2019. atNorth maintains a robust set of controls to support our resilience and critical assets as well as our continuity objectives:

- Reducing the likelihood of disruption and minimizing impact to ensure continuity of business processes
- Minimizing recovery time of predefined business processes through the availability of appropriate people, technologies, and infrastructure to enhance recovery capability after disruption
- Building mechanisms to maintain communication with staff and stakeholders
- Creating a robust framework to provide strategic direction on recovery, provide leadership and control overall coordination, decision-making and communication strategies
- Reserving resources (material, personnel, budget) and ensuring capabilities to maintain an effective and compliant BCMS,
- Ensuring the safety of human resources and effective response to interruptions or disasters through appropriately qualified human resources; and
- Ensuring compliance with regulatory legal and contractual requirements.

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 this and all other relevant policies, standards, plans, processes, procedures, instructions or any other documentation relating to business continuity and disaster recovery.

References

This policy is aligned with EU and national legislation and regulation related to business continuity, as well as ISO 22301:2019 standard, or specific contractual commitments.