IT Security Policy for NH Towage A/S

Purpose

This IT Security Policy defines the framework for NH Towage A/S and anchors the work in the international maritime conventions that form the basis for our operations and safety, both at sea and on shore.

We work with IT security as a natural part of our overall safety and quality management, and as an important contribution to protecting people, the environment and our business.

The policy supports our obligations under international maritime conventions, which establish the framework for safe ship operations and responsible conduct.

Including:

- The International Maritime Organization (IMO)
- The International Convention on Maritime Search and Rescue (SAR)
- The International Convention for the Safety of Life at Sea (SOLAS)
- The International Convention for the Prevention of Pollution from Ships (MARPOL)
- The International Convention on Standards of Training, Certification and Watchkeeping for Seafarers (STCW)
- The Maritime Labour Convention (MLC 2006)

NH Towage A/S follows the IMO guidelines on maritime cyber risk management (MSC-FAL.1/Circ.3 Rev. 3).

IT security, both on shore and at sea, follows the General Data Protection Regulation (GDPR), the Danish Data Protection Act, as well as NH Towage A/S' internal IT guidelines and procedures.

Scope

This IT Security Policy applies to all employees of NH Towage A/S and to all use of and access to NH Towage A/S' information systems.

Objective

NH Towage A/S works actively with the management of IT security with the purpose of ensuring the availability, integrity and confidentiality of NH Towage A/S' information assets, systems and data.

At sea: IT security is considered an integrated part of maritime safety and environmental protection, in accordance with the requirements of SOLAS, MARPOL and MLC 2006.

IT security within NH Towage A/S follows Danish data protection legislation, GDPR and NH Towage A/S' internal IT guidelines.

NH Towage A/S applies a risk-based approach, where the level of protection and associated costs must be based on a business-related risk and impact assessment, which must be carried out at least annually.

NH Towage A/S prepares and maintains IT guidelines that describe the specific measures, requirements and procedures for employees' use of IT systems in accordance with this policy.

NH Towage A/S seeks to comply with relevant legislation, including, for example, GDPR.

NH Towage A/S seeks to comply with agreements entered with external parties, including data processing agreements.

This IT Security Policy must be evaluated on an annual basis.

Organisation and Responsibilities

The Board of Directors holds the ultimate responsibility for IT security at NH Towage A/S.

Executive Management is responsible for governance principles and delegates specific responsibilities for security measures, including ownership of IT systems. Executive Management determines how security measures are applied and managed in accordance with the IT Security Policy.

The IT function, which is external and provided by Onehouse, advises, coordinates, monitors and reports on the status of IT security.

Each individual employee is responsible for complying with the IT Security Policy and is informed of this through the "IT Usage Policy".

At sea: The shipmaster holds full responsibility and overriding authority to make decisions relating to safety, including IT security, when incidents affect the vessel's operation or environmental protection.

Exemptions

Exemptions from NH Towage A/S' IT Security Policy and guidelines are approved by the Board of Directors based on guidelines set by management.

Reporting

Cyber incidents are handled as part of the general incident management structure.

At sea: This incident handling applies on board, where all security breaches or cyber-related incidents must be reported, first by telephone to the responsible person in the technical department. Thereafter, an Incident Form (Marad) must be completed and submitted to the technical department (TEK) and subsequently handled through evaluation at a Safety Meeting.

Violations

Intentional violations and misuse must be reported to the immediate manager and to management.

Violations of the IT Security Policy or supporting guidelines may result in employment-related consequences.

Remediation and improvement

In the event of identified cyber incidents or breaches of IT security, NH Towage A/S will immediately initiate remediation in accordance with our procedures for dialogue, restoration and compensation.

The policy is evaluated at least once annually and updated to ensure continued compliance with international standards, applicable legislation and the company's values.

Approval and entry into force

This policy has been reviewed and approved by the executive management of NH Towage A/S.
The date below indicates the latest revision and formal approval by management:

18062026

Date of revision and approval

Niels Henriksen

Owner & CEO

Approval and Effective Date
Document: IT Security Policy
Version: 1.0

Effective Date: 01 July 2026
Last Revision Date: 01 July 2026