Musti Group

Information Security Policy

March 2023

Version 2.4

Public

Table of Contents

Management statement

With this information Security Policy Musti Group commits to develop, implement and monitor the company's information security procedures and practices. The objective is that our customers, shareholders, personnel and other stakeholders may rely on the quality of Musti Group's information security operations to be in line with the requirements set by the operating environment. The policy is clarified with separate guidelines and instructions. Musti Group's data protection policy has been published as a separate document and it provides information of the requirements for the group wide data protection.

Information security principles and objectives

This policy outlines the principles and objectives for information security and establishes the management commitment for information security in Musti Group.

The objective is to protect company assets and ensure readiness for business continuity in all processes. Furthermore, the objective is to ensure that Musti Group services promote customer loyalty by providing an excellent reputation and brand awareness also from the information security perspective. Service quality will be maintained at a high level. This Policy is applicable to all companies at Musti Group.

The objective is to ensure the protection of the critical assets. Growth, digitalization, new services to customers in several countries and expectations for listed companies require the ability to operate and maintain a high level of data and privacy protection. Confidentiality, availability and integrity of the critical assets must be ensured. Furthermore, non-repudiation must be ensured in e-commerce and online business.

This policy is published internally and made available to relevant internal and external stakeholders.

This policy is owned by the CIO. Reviews and changes to this policy are conducted regularly and approved by the Group Management Team (GMT). Information security matters are followed up regularly in the GMT, Corporate Risk management, Internal Controls and Audit Committee.

Roles and responsibilities

The roles and responsibilities related to information security are defined in a separate document.

Definition of information security

Information security refers to measures taken to protect information, information systems and operations in order to guarantee their confidentiality, integrity and availability.

- **Confidentiality** means that only authorized persons have access to information by agreed means and at agreed times, and that the information is not disclosed or otherwise made available to third parties.
- **Integrity** means that the information and information systems are reliable, accurate and up to date, and they have not been changed or damaged as a result of hardware or software failures, natural events or unintentional, intentional or unlawful actions.
- **Availability** means that the data and information systems are available and usable in line with the agreed service and response times.

Information security principles

The following principles apply:

- Information must be protected against unauthorized access and use.
- Data privacy must be ensured.
- Integrity of the information must be ensured.
- Compliance with legislation, regulations and contracts must be fulfilled.
- Each business-critical asset must have a defined ownership and classification.
- Business continuity assessment must be performed and policies must be defined for business-critical assets prior to deployment.
- Security incidents, confirmed or suspected, must be reported to, and investigated by, the relevant parties.
- The employees receive training related to information security and are responsible for familiarizing themselves with Musti Group's information security guidance and complying with the same.
- All employees are required to comply with the information security practices of the company.
- All Musti Group sites and locations must adhere to and comply with the information security practices.
- All external service providers must meet Musti Group's security requirements.
- All managers are responsible for ensuring that the information security practices are followed in their respective areas of responsibility.
- Sanctions will be applied to intentional breach of information security.

Ensuring confidentiality

All information is classified according to their business criticality. Information is divided into the following confidentiality classes:

1. *Public* refers to information that may be made public outside the company.
2. *Internal* refers to information that may be shared among Musti Group personnel (e.g. internal policies, instructions, or training materials). Internal information must be kept in internal information systems only. Sharing with an external party is subject to a non-disclosure agreement (NDA).
3. *Confidential* refers to information that can only be accessed by a restricted group of Musti Group employees. Sharing is allowed need-to-know basis only. External sharing requires NDA and permission from the information owner.
4. *Secret* refers to information that may only be shared with approval from CEO or CFO. (e.g. M&A, inside information). Secret information requires extra care as it may cause serious risk to Musti Group's business, customers, or partners if disclosed without approval.

If not otherwise indicated, information must be treated as *internal*. Please note that information may be subject to restrictions imposed by other laws, e.g. *securities market act* or *competition law*.

The classification of information is defined in more detail in separate classification instructions. All instructions related to information classification are the subject of training for all personnel and stakeholders.

Ensuring Integrity

- System software updates are designed to comply with the recommendations.
- Document versions are controlled, and documents are archived appropriately.
- Backup copies of documents are made regularly.

Ensuring availability

Business continuity and disaster recovery readiness will be an integral part of all business-critical services and are mandatory for all services providers via agreements. The business continuity readiness and ability to recover will be included in frequent service provider assessments and audits.
The availability of information systems is monitored, and the quality of availability is measured. Group IT is responsible for the realization of information system services.

Information security efficiency

Separate information and IT-security instructions and guidelines are used to steer the information security operations and development on the operational level.

Efficiency monitoring will be a subject of follow-up in the Corporate Responsibility reports.

Other policies

Musti Group’s data protection policy has been published as a separate document and it provides information on the requirements for group-wide data protection.

Approval and confirmation

This information security policy has been reviewed and approved by the Musti Group Management Team.