Musti Group
Information Security Policy

April 2021

Public

Table of Contents

Management statement

With this Information Security Policy Musti Group’s management commits to develop, implement and monitor the company's information security procedures and practices so that our customers, shareholders, staff and other stakeholders can 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 sub-policies and instructions. Musti Group’s data protection policy has been published as a separate document and it provides information of the requirements for group wide data protection.

Information Security Principles and Objectives

This document 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 in providing excellent reputation and brand also from the information security perspective. Service quality will be maintained on a high level. This Policy is applicable in all companies at Musti Group.

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

Information security management in Musti Group is based on ISO 27001 (ISO/EIC 27001-13) information security management framework. The controls and objectives per sub-section are assessed and evaluated in the risk assessment process and controls are applied as countermeasures to manage the risks. Information security is under continuous improvement according to the framework selected.

This Information security policy is published internally and made available to relevant external stakeholders and partners.

The information security policy document is owned by the CIO. Reviews and changes to this document are conducted regularly and approved by the Group Management Team (GMT). Information security is followed up regularly in 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.
- Information 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.
- This information security policy and related sub-policies and information security instructions are distributed to staff for their information.
- The employees receive training related to these policies and instructions and are responsible for familiarizing themselves with their content and complying with them.
- Information security is also part of the induction training in the HR process for the new employee.
- All employees must commit to and comply with 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 our company'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 the confidentiality

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

1. *Public information* refers to information that has officially been made public outside the company.
2. *Internal information* refers to information that can be shared among Musti Group's personnel and persons who have signed a non-disclosure-agreement.

3. *Confidential information* refers to information that can only be accessed by a restricted group.
4. *Secret information* is information that may place a customer's, partner's or Musti Group's business operations at risk if disclosed.

If not otherwise indicated, information must be treated as *confidential*.

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

Ensuring the Integrity

- System software updates are designed to comply with.
- 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 ICT 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. 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 management of Musti Group.