DUMAREY

DM-IS-0001

Information Security Policy

Rule Level/Type	Organization	Organizational Scope	Version	Review Frequency
Group Policy	Information Security	Global	1	1 year

Approvals

Dumarey Group CEO	Dumarey Group CFO	Dumarey Group CISO
Guido Dumarey	Kwinten Smits	Paolo C. Pomi

1. Purpose

The Information Security Policy of Dumarey Group company is a foundational document endorsed, approved, and supported by the company's leadership. This policy articulates the primary concerns and requirements concerning information security within our company and establishes the essential security standards and regulations to address these concerns.

This policy elucidates the strategic vision of our company's leadership and delineates the fundamental principles to be adhered to in matters of information security. It also outlines a set of measures integral to an Information Security Management System, designed for gradual implementation, as per a defined action plan. This phased approach is aimed at facilitating a sustainable progression of information security within the organization, ultimately leading to the achievement of our predetermined security objectives.

Our company recognizes the importance of safeguarding information, both physical and electronic, as a critical asset. This includes information pertaining to our business operations, whether generated internally or obtained through external sources. Such information encompasses a wide range of forms, such as product plans, design data, prototypes, strategic documents, records (both business and non-business), pricing details, financial and technical data, as well as various file types comprising text, audio, and visual content, stored across multiple locations and devices.

All users within our company must understand the intrinsic value of this information and acknowledge their individual responsibility in ensuring its protection. The Information Security Policy outlines the overarching direction and objectives to safeguard information security, focusing on three core principles:

- Confidentiality: All information must be protected from unauthorized access, disclosure, or sharing.

- Integrity: Information should remain accurate, reliable, and unaltered, safeguarding its trustworthiness.
- Availability: Information must be accessible and available to authorized users when required, ensuring business continuity.

The policy emphatically prohibits any illegal, unauthorized, or unethical actions related to the disclosure, modification, misuse, or disposal of our company's information assets. In the event of a breach involving our company's information assets, the company will take all necessary legal actions to protect its information, business interests, and reputation. This may include engaging government authorities for civil or criminal prosecution, as deemed appropriate.

By adhering to this Information Security Policy, our company is committed to fostering a secure information environment, upholding the trust and integrity of the organization, and fulfilling our duty to protect valuable information assets.

2. Scope

The information security policy applies to all information and processing resources within the company in the context of its activities.

The information security policy thus encompasses:

- All of the company's activities,
- All of the organization's roles and responsibilities,
- The entire information system, including outsourced and specific components,
- All individuals or legal entities contractually linked to the company or involved in its operations and likely to have access to the information system, such as suppliers or service providers.

Terms and definitions

Term	Definition
Confidentiality	Assuring that information is not disclosed to unauthorized individuals or systems.
Integrity	Protecting information from unauthorized alteration or tampering, ensuring its accuracy and reliability.
Availability	Ensuring that information and resources are accessible and usable when needed by authorized users.
Risk Management	The process of identifying, assessing, and mitigating security risks to protect an organization's assets.
Security Controls	Measures, safeguards, or countermeasures put in place to protect information and systems.
Incident Response	A plan and procedures for addressing security incidents, breaches, and emergencies.
Compliance	Adherence to laws, regulations, standards, and internal policies related to information security.
Training and Awareness	Programs that educate employees and stakeholders about security risks and best practices.
Monitoring and Audit	Continuous surveillance and assessment of security controls and activities to ensure effectiveness.
Review and Updates	The process of periodically revising and enhancing security measures to address changing threats and technologies.
Enforcement	Measures taken to ensure compliance with security measures, which may include disciplinary actions.

Access Control	Managing user privileges to restrict access to information and systems based on user roles and permissions.
Data Classification	Categorizing data based on sensitivity and importance to determine appropriate security measures.
Data Retention	Guidelines specifying how long data should be stored and when it should be securely disposed of.
Acceptable Use	Rules governing the proper and acceptable use of an organization's information systems and resources.
Security Awareness Training	Educational programs to promote security awareness among employees and stakeholders.
Vulnerability Assessment	Identifying and evaluating weaknesses in an organization's security posture.
BYOD (Bring Your Own Device)	A policy governing the use of personal devices for work purposes and setting security requirements.
Security Incident	Any event that compromises the confidentiality, integrity, or availability of information or systems.
Two-Factor Authentication (2FA)	A security method requiring two authentication factors for user access, typically something the user knows and something the user possesses.

3. Objectives

The company's Information Security Policy is guided by several key objectives, as described in the followings.

Information Assessment and Classification: The company places a strong emphasis on proper assessment and classification of all information, whether it is generated internally or acquired externally. Information owners are responsible for categorizing data based on its value and sensitivity regarding confidentiality, integrity, and availability. It must be managed in accordance with well-defined procedures for data coding, archiving, and ISMS risk assessment and risk treatment procedures relating to information assets.

Access Control and Compliance: The company is committed to ensuring that information access is regularly reviewed and updated in alignment with evolving business organization and regulatory requirements. All employees and users are expected to adhere to local laws, regulations, and contractual agreements that specify information security controls, encompassing areas such as copyright, patents, cross-border information and technology transfer, import and export regulations, and confidentiality and non-compete requirements.

Protection of Information: Safeguarding information is paramount. All information related to the company's business, irrespective of its form, must be shielded from unauthorized disclosure, modification, malware, misuse, and improper disposal, whether intentional or unintentional. Users, in accordance with their roles and responsibilities, play an active role in managing information during its entire lifecycle, strictly following company policies and procedures.

Incident Management: In cases of non-compliance, the company swiftly responds by implementing the Information Security Incident Management Process. This protocol is enacted to address any "information security breach" and to deploy necessary countermeasures, which may include enhanced training, system adjustments, or disciplinary actions.

Risk Mitigation: The company acknowledges the significance of its information assets and the associated computing and communication environment. It is vital to continuously assess these risks and establish mitigation plans to minimize the potential loss of information.

Responsibility and Oversight: The Information Security Management System and Policy are under the direct purview of the CEO and CFO of the company. The Chief Information Security Officer assumes the critical role of interpreting the policy, defining related policies, standards, and procedures, and promoting their adoption. Managers and Supervisors are responsible for ensuring that employees and contractors fully understand and comply with Information Security policies and related ISMS procedures.

Third-Party Information: The company is dedicated to safeguarding third-party information in strict adherence to the terms of agreements with the third party. In the absence of such an agreement, appropriate controls or mechanisms are established by the company.

Internal Audits and Continuous Improvement: Periodic internal audits are conducted to evaluate the effectiveness of the ISMS and identify non-conformities or areas for improvement. The company maintains a strong commitment to a continuous improvement approach for the Information Security Management System across the entire organization.

Employee Training: Employee training is a cornerstone of the company's information security approach. Employees are empowered with comprehensive knowledge and a clear understanding of their responsibilities in safeguarding sensitive information, making them the first line of defense against data breaches.

Policy Review and Availability: The Information Security Policy undergoes periodic review, at least annually, or in response to significant changes in company goals, incidents, risk assessments, or regulatory issues. This policy is readily accessible through electronic means, including the ISMS internal SharePoint, the company's websites, and material boards within the company's premises.

4. Revision History

Version	Date	Comment
01	15/12/2023	First Release