1st edition
Established in January 2025

M3 Group Basic Policy on Information Security

1. Basic Approach

M3 Group (which refers to the Company and its affiliates, etc.[1], as defined in the "Code of Conduct" stated below; the same shall apply hereinafter) has declared in the "M3 Group Code of Conduct" (hereinafter referred to as "Code of Conduct"), which is a code of conduct to be observed by each and every director, officer and employee of M3 Group, that it respects the privacy of individuals, such as customers, employees of suppliers and business partners, and directors, officers and employees ("3.6 Personal Information") and that it will safeguard its own confidential and proprietary information as well as the information that suppliers, business partners or customers entrust to M3 Group ("3.8 Confidential and Proprietary Information").
This Policy clarifies M3 Group's approach to information management as set forth in the Code of Conduct and applies to all directors, officers and employees of M3 Group.

2. Purpose

This Policy establishes the basic policy for appropriately managing information security risks and protecting the information assets of M3 Group.

3. Management Involvement

The M3[2] Board of Directors shall direct the development of a risk management system for information security and personal information protection that conforms to business strategy and shall provide the necessary resources. Risk managers shall regularly report the results of the development and operation of the information security and personal information protection management system to the management and shall improve operations in accordance with instructions from the management regarding the necessity of change.

4. Establishment of Information Security Risk Management System

M3 has established the Information Security Committee, headed by the Chairperson of the Information Security Committee, to centrally manage the Group's information security and personal information protection risks.

5. Implementation of Information Security Risk Assessment

M3 Group shall identify information assets and threats to ensure the confidentiality, integrity and availability of the information it handles and shall implement an information security risk assessment.

6. Information Security Management Measures

M3 Group shall consider risk response methods based on the results of information security risk assessments and shall implement information security management measures, including protection against unauthorized access.

[1] It refers to (1) M3, Inc. (2) any company in which M3, Inc. directly or indirectly holds a majority of the outstanding voting shares or equity interests and (3) any other company that the Board of Directors of M3, Inc. decides to include in the scope of the Code of Conduct as appropriate.
[2] It refers to M3, Inc. The same shall apply thereafter.

7. Information Security Management for Business Partners and Suppliers

When M3 Group provides information to its business partners and suppliers in connection with outsourcing and other activities, it will provide the information only to appropriate parties after prior evaluation. In addition, it shall continue to communicate with them to ensure that the information provided is handled appropriately and also conduct security assessments on a regular basis and strive to understand the actual status of information management.

8. Principles of Information Management

M3 Group shall define the purpose of use of information, acquire information to the extent necessary to achieve that purpose and retain it for the necessary period.

9. Protection of Rights to Personal Information

M3 Group handles personal information in accordance with the laws and regulations regarding the protection of personal information, including the Act on the Protection of Personal Information and the personal information protection policies separately established by each M3 Group company while respecting the rights and interests of the individual.

10. Information Security Incident Response

M3 Group shall endeavor to prevent the occurrence of incidents related to information security, such as data breaches, and in the event of an incident, shall work to prevent the spread of damage and restore services quickly in accordance with the incident response plan.

11. Implementation of Education on the Information Security and the Protection of Personal Information

M3 Group shall provide opportunities for education to its employees, including contract and temporary employees, at the time of joining the company and on a regular basis to ensure that they are aware of the importance of properly handling information assets and protecting personal information.

12. Development of Internal Reporting Process

To facilitate the early detection and correction of violations of information security policies and information handling, M3 Group shall establish a contact point and response process for anonymous reporting by interested parties who have discovered violations in accordance with the Whistleblower Protection Act.