P01. Group Information Security Policy

Ver 1.0

May, 2024

Information Security Management Statement

Enacted: May 02, 2022

1st Revision: May 28, 2024

As a leading ODM and OBM company in the cosmetics and bio fields, the COSMAX Group has made information security activities an essential element rather than an option to increase the value of the company and provide the best service to customers.

Therefore, all employees of the COSMAX Group must comply with the laws and regulations related to data protection and privacy, as well as the data protection requirements of our stakeholders, to build internal and external trust and fulfill our social responsibility.

In addition, we must do our best to take measures to protect critical information assets from a variety of information security threats, including leakage of COSMAX Group's core technology and personnel, and various breaches from internal and external sources.

COSMAX Group Information Security Policy

Chapter 1 Purpose

The purpose of the Group Information Security Policy (hereinafter referred to as the "Policy") is to set out the principles for the establishment of a global ONE COSMAX information security management system to ensure that the affiliates, domestic and international subsidiaries within the COSMAX Group (hereinafter referred to as the "Company") comply with all legal and regulatory requirements (hereinafter referred to as "Compliance"), including information security, privacy, and agreements with stakeholders, necessary to conduct business activities, and to safeguard the information assets used or managed in connection therewith.

Based on this Policy, the Company shall establish and enforce detailed information protection regulations and guidelines, etc. to effectively implement this Policy in consideration of the requirements for compliance with all other compliance related to the Target Company's business areas, business and information protection operating environment and risks.

Chapter 2 Scope

This Information Security Policy applies to all employees of Cosmax, including its subsidiaries and second-tier subsidiary. It also applies to all stakeholders, including customers, local communities, and residents related to Cosmax's business, employees of suppliers and national organizations who need access to Cosmax's information assets, and others, as well as to the Company's information assets and information assets entrusted to the Company.

National and international laws or government policies regarding data protection take precedence over this Policy.

Chapter 3 Definitions

1.1. The Data Protection Regulatory Framework and the Location of this Policy

Information security risks are always changing with the conduct of business activities and the development of information technology. In order to adequately protect the information assets of the COSMAX Group, it is necessary to regularly review information protection measures in response to changes in the company's status or the occurrence of new threats. Accordingly, the Company establishes the "COSMAX Group Information Protection Policy" as the higher information protection regulation, and the "Information Protection Regulations, Guidelines and Procedures" that need to be regularly checked in accordance with environmental changes as subregulations. However, national/international laws or government policies related to information protection shall take precedence over this policy or company-specific regulations and guidelines.

(1) COSMAX Group Information Security Policy
- The COSMAX Group's highest information protection policy, which establishes principles to unify and improve the COSMAX Group's information protection management system and information protection level.

(2) Company-specific Information Security Regulations

- Regulations that establish the principles necessary for the establishment and operation of an information security management system to ensure compliance and fulfillment of information security requirements that consider the specificities of each company based on this policy.

(3) Other, subregulations

- Information security-related regulations, such as guidelines, procedures, or guides that further specify detailed information security-related procedures to be followed within a specific scope for each company based on standards or how to perform them.

1.2. Definition of Terms

As used in this Rule, the following terms have the following definitions.

(1) Information: Information can be in any form, tangible or intangible, such as documents, drawings, electronic records, or knowledge gained through work.
(2) Information system: A system of hardware, software, networks, etc. that processes information. It can also refer to the individual components.
(3) Information assets: Information and the information systems that process it.
(4) Threat: A potentially damaging factor to an information asset.
(5) Cyberattack: A type of threat in which an attacker with malicious intent uses an information system to fraudulently manipulate data or execute programs.
(6) Information protection: Protecting information assets from all threats and ensuring and maintaining their confidentiality, integrity, and availability.
(7) Information security incident: An incident or accident in which a company's information assets are leaked or manipulated intentionally or due to user negligence.
(8) User, etc.: Refers to the following persons who use the Company's information assets to perform work under the direction of the Company.
   - Executives, etc. (representatives, officers, advisors, etc.)
   - Employees (anyone who has an employment relationship with the Company, including employees, contractors, temporary workers, and short-term workers)
   - Temporary employees under temporary contracts
   - Other third parties who need access to the Company's information assets through projects or outsourcing agreements with the Covered Company.

Chapter 4 Information Security Responsibilities

1.1. Chief Information Security Officer (CISO)

The CISO is responsible for overseeing the company's information protection activities and operating the information protection organization, and is responsible for continuously maintaining the direction of information protection and the consistency of the operation of the information protection management system.

1.2. Information Security Department

The information security department is responsible for planning, coordinating, and supporting the company's information protection, and is responsible for enacting and revising information protection regulations and guidelines, responding to information protection-related laws and regulations and stakeholders' information protection requirements, and periodically reviewing compliance with information protection regulations and guidelines and the adequacy of the information protection measures applied, and reporting to the Chief Information Security Officer.

1.3. Users, etc.

Users are responsible for using and managing only the information assets authorized to them, and the Company shall establish and enforce detailed information protection regulations and guidelines, etc. to effectively implement this based on this policy, considering the requirements for compliance with all compliance related to the target company's business areas, business and information protection operating environment and risks, etc.

Chapter 5 Quantitative Targets

To minimize and systematically manage information security-related risks, the Company will increase the percentage of workplaces conducting information security risk assessments to 100% by 2030.

Chapter 6 Information Security Code of Conduct

The Company shall properly operate a global-level information protection management system in accordance with relevant regulations on information protection and continuously strive to maintain and improve its level. To realize this, the Company shall implement the following items.

(1) Establish an information security management system
(2) Clarify the information security management processes

(3) Identify and assess risks of information assets
(4) Establishing information security measures

All employees (new employees, retirees, employees, etc.) of Cosmax and external partners sign and comply with the information protection and confidentiality pledge. In addition, users, etc. understand the necessity of such measures and practice the following items regarding the information assets they handle.

(1) Disclose information only to those who need it for business purposes.
(2) Perform work in accordance with the established rules for handling information assets.
(3) Participate in education and training on information security.
(4) If you become aware of any lack of information protection measures, leakage or manipulation of confidential information, you shall promptly report it according to the established procedures.

Chapter 7 Information Security Fundamentals

1.1. Handling Information Assets

Users and others shall implement the following items to protect the company's information assets from information protection risks such as leakage or manipulation.

(1) Information
- Information should be categorized according to its use and purpose.
- Classified information shall be evaluated according to its confidentiality, and appropriate information protection measures shall be established and implemented according to the evaluated importance.
- The information should be labeled with a classification.
- Information protection measures should be established and implemented according to the life cycle of information (creation, use, storage, and disposal).

(2) Information Systems
- Information systems should be categorized according to their use and purpose.
- Classified information systems shall be evaluated for importance based on confidentiality, integrity, and availability, and appropriate information protection measures shall be established and implemented based on the evaluated importance.
- Information systems must establish and implement information protection measures according to their life cycle, including planning, development, operation, protection, and disposal.

1.2. Human Security

The Company shall establish and implement human security measures, such as separately signing a confidentiality agreement to impose the obligation to comply with the information protection management system when there is an addition or change in the users of information assets, such as recruitment, transfer, or retirement of employees, etc. In addition, the Company shall regularly conduct training on information protection so that users understand the importance of information protection and handle information assets appropriately.

1.3. Physical Security

The Company shall establish and implement appropriate physical security measures for access to offices or business sites and access to places where information assets are stored and installed in order to safely protect the Company's information assets from physical threats such as disasters or crimes.

1.4. Technical Security

The Company shall implement technical security measures, such as access control, encryption of information, and virus countermeasures, to protect the Company's information assets from various threats, including cyberattacks.

1.5. Outsourcing of Information Protection

The Company shall establish and implement appropriate information protection measures in relation to external delegation, such as entering into a contract specifying information protection requirements, when outsourcing tasks that use information assets.

1.6. Private Information Protection Measures

The Company shall collect, store, and process information of Users and other third parties only for business purposes and to the extent necessary and to the minimum extent possible.

1.7. Countermeasures for Information Security Incidents

In the event of an information security accident, the Company shall establish and maintain response procedures to minimize damage.

1.8. Securing information protection in case of damage

When establishing or maintaining procedures for recovery and resumption in the event of a risk

that threatens business continuity, such as a large-scale disaster or failure of an information system, the company must also consider maintaining information protection.

1.9. Information Security Inspection or Audits

To assess the effectiveness of its information security measures, the Company shall regularly verify its compliance with information security regulations and review its information security measures as a result. The COSMAX Group shall check the implementation of the information protection management system of its companies, including the ongoing operation and improvement activities, and recommend information protection measures to the companies accordingly.

Chapter 8 Information Protection Compliance

To fulfill their social responsibilities, users and others must comply with this Policy or related laws and regulations, as well as laws and regulations not listed in this Policy, and internal regulations.

Chapter 9 Disciplinary Measures for Violations

The Company shall take measures based on the employment rules, personnel regulations, and individual contracts if the user or others violate the matters set forth in this Policy or subordinate regulations of each company.

Chapter 10 Exceptions

The COSMAX Group shall recognize exceptions to the provisions relating to data protection only for reasonable reasons. Reasonable cause means that the application of this policy is inconsistent with local characteristics or laws or would significantly interfere with the proper conduct of business, and the Company shall have procedures in place to deal with exceptions.

Chapter 11 Review and Revision of Information Security Policy

The Company should conduct regular reviews of their information security policies once a year, and should also conduct timely reviews when risks change, such as due to the emergence of new threats. Revisions to Information Security Policy shall be made in accordance with the company's

internal rules.

ADDENDUM

This policy is effective May 02, 20212

1. Enacted May 02, 2022
2. Revised May 28, 2024