
AI MANAGEMENT REGULATION

Responsible Department	Information Security	Classification No.	Ⅱ
Revision No.	1.0	Effective Date	August 13, 2026

August 2026

Ownership

The copyright in this document is owned by SK Square Co., Ltd.

This document may not be copied or disclosed outside the Company without the prior written consent of the head of the responsible department.



Classification No.	-	Information Security AI Management Regulation	Enactment Date	Aug. 13, 2026
Page	2 / 9		Revision No.	1.0

Enactment and Revision History

Revision No.	Revised Pages and Description	Revision Date

Classification No.	-	Information Security AI Management Regulation	Enactment Date	Aug. 13, 2026
Page	3 / 9		Revision No.	1.0

Chapter 1 General Provisions.....4

Article 1 (Purpose) 4

Article 2 (Definitions)..... 4

Article 3 (Scope of Application)..... 5

Chapter 2 Basic Principles.....6

Article 4 (Respect for Data Privacy) 6

Article 5 (Cybersecurity) 6

Article 6 (Bias Prevention) 6

Article 7 (Identifiability of AI Outputs) 7

Article 8 (Transparency and Explainability of AI Systems)..... 7

Article 9 (Human Oversight and Intervention) 7

Article 10 (Accountability for AI Use)..... 7

Article 11 (Scope of Use and Guidelines) 8

Article 12 (Prohibited AI Uses)..... 8

Chapter 3 Disclosure of Status and Results.....9

Article 13 (Disclosure of Status and Results)..... 9

Addendum.....9

Classification No.	-	Information Security AI Management Regulation	Enactment Date	Aug. 13, 2026
Page	4 / 9		Revision No.	1.0

Chapter 1 General Provisions

Article 1 (Purpose)

The purpose of this AI Management Regulation (hereinafter "this Regulation") is for SK Square Co., Ltd. (hereinafter "the Company") to set forth the standards and procedures for using AI responsibly and ethically across all of its business activities and for fulfilling the ethical and social responsibilities that accompany such use. The Company establishes this Regulation in full recognition of the impact that advances in AI technology have on corporate management and society as a whole, and in support of international norms on AI, including the OECD AI Principles (OECD Recommendation of the Council on Artificial Intelligence), the UNESCO Recommendation on the Ethics of Artificial Intelligence, and the EU Artificial Intelligence Act (EU AI Act).

Article 2 (Definitions)

1. "Artificial intelligence (AI)" refers to any technology or system of devices that artificially implements, through computer programs or systems, human intellectual capabilities such as perception, learning, reasoning, natural language processing, and problem solving, so as to perform comparable functions.
2. "Cyber threat" refers to any hostile attack or harmful act carried out through information and communications networks that causes, or creates a risk of, damage to information and communications systems, data, national or public infrastructure, or the information assets of individuals, including through unauthorized access, destruction, alteration, leakage, or disruption of functions.
3. "User" refers to any person who is provided with or uses an AI system.

Classification No.	-	Information Security AI Management Regulation	Enactment Date	Aug. 13, 2026
Page	5 / 9		Revision No.	1.0

4. "EU Artificial Intelligence Act (EU AI Act)" refers to the law enacted by the European Union (EU) to ensure the safe use of AI technologies and to protect fundamental rights (Regulation (EU) 2024/1689).
5. "AI system" refers to any software, model, service, or tool, or any system incorporating these, that uses AI to process input data and produce outputs for specific purposes, such as predictions, recommendations, classifications, generated content, or decision support.
6. "AI output" refers to any output generated by an AI system or created or processed with the assistance of an AI system, including text, images, video, audio, code, and analysis results.
7. "Social scoring" refers to an evaluation system that collects and analyzes, over an extended period, a wide range of social and personal data on individuals or groups, such as their everyday behavior, social trustworthiness, beliefs, and compliance with legal obligations, and on that basis rates or scores an individual's creditworthiness or reputation.
8. "Real-time remote biometric identification" refers to any technology or system that remotely collects data on human biological or behavioral characteristics (such as facial features, fingerprints, iris patterns, and gait) through devices such as information and communications terminals or video surveillance equipment installed in public places or elsewhere, and identifies or verifies specific individuals in real time, without their knowledge, by matching the data against databases.

Article 3 (Scope of Application)

This Regulation applies to all business activities of the Company, including all forms of AI-related activities such as the in-house development of AI systems, the adoption and use of external AI systems, and the provision of AI systems to third parties, and to all officers and employees of the Company.

Classification No.	-	Information Security AI Management Regulation	Enactment Date	Aug. 13, 2026
Page	6 / 9		Revision No.	1.0

Chapter 2 Basic Principles

Article 4 (Respect for Data Privacy)

The Company shall rigorously protect personal information throughout the use and development of AI systems. The Company shall comply with applicable personal information protection laws and regulations across the entire data lifecycle, including collection, processing, storage, and disposal, and shall implement appropriate technical and administrative safeguards to ensure that AI systems do not compromise personal information or infringe on individual privacy.

Article 5 (Cybersecurity)

The Company shall establish and maintain a security framework to protect its systems from cyber threats in the use and development of AI systems. The Company shall implement technical security measures, such as data encryption, access control, and security monitoring, to protect AI systems and the Company's data against unauthorized access, manipulation, and leakage, and shall maintain the capability to respond promptly to security incidents.

Article 6 (Bias Prevention)

The Company shall strive to prevent potential bias in the use and development of AI systems. The Company shall conduct reviews to identify and mitigate biases that may be embedded in training data and algorithms, and shall manage its AI systems so that they do not produce unfair or discriminatory outcomes against any particular group.

Classification No.	-	Information Security AI Management Regulation	Enactment Date	Aug. 13, 2026
Page	7 / 9		Revision No.	1.0

Article 7 (Identifiability of AI Outputs)

The Company shall ensure that users can identify AI outputs as such. The Company shall clearly inform users when AI outputs, such as text, images, and video, have been generated by an AI system, and shall implement appropriate labeling and notification measures so that users are aware that they are interacting with an AI system.

Article 8 (Transparency and Explainability of AI Systems)

The Company shall provide stakeholders in AI-enabled operations with information on the purpose, limitations, data sources, and potential risks of its use of AI at a level they can reasonably understand. The Company shall work to ensure that the rationale for and outcomes of AI-driven decisions can be explained in a manner consistent with the needs and rights of users and stakeholders, and shall maintain procedures to verify the reliability and accuracy of AI outputs.

Article 9 (Human Oversight and Intervention)

The Company shall, as a matter of principle, operate AI in a human-centered manner, and shall maintain an appropriate level of human oversight over decisions that may materially affect people's rights, safety, or interests. The Company shall ensure that outputs produced by AI systems remain subject to final human review and confirmation, and shall provide for the authority and procedures needed to override, modify, or suspend such outputs where necessary.

Article 10 (Accountability for AI Use)

Classification No.	-	Information Security AI Management Regulation	Enactment Date	Aug. 13, 2026
Page	8 / 9		Revision No.	1.0

The Company shall maintain a clear accountability framework for the adoption and operation of AI systems and for AI outputs. The Company shall designate responsible departments and personnel for each area of AI use, and shall have in place procedures to investigate the causes of any errors, incidents, or harm to stakeholders arising from AI systems and to take appropriate corrective and remedial measures.

Article 11 (Scope of Use and Guidelines)

The Company shall define and manage in detail the permitted scope of AI use, prohibited activities, and procedures for use through the separate “Guidelines for the Safe Use of Generative AI Tools” so that officers and employees use AI in accordance with the Company’s information security principles and ethical standards. The Guidelines shall cover matters such as approved AI systems, requirements for their use, prohibited conduct, and standards for data input, and shall be reviewed and updated regularly to reflect changes in the internal and external environment.

Article 12 (Prohibited AI Uses)

The Company shall not develop, adopt, or use AI systems prohibited under the EU Artificial Intelligence Act (EU AI Act). These include AI systems that use subliminal, manipulative, or deceptive techniques to distort an individual’s behavior; AI systems that exploit vulnerabilities related to age, disability, or socioeconomic circumstances; AI systems that perform social scoring based on social behavior or personal characteristics; and real-time remote biometric identification systems that are not permitted by law.

Classification No.	-	Information Security AI Management Regulation	Enactment Date	Aug. 13, 2026
Page	9 / 9		Revision No.	1.0

Chapter 3 Disclosure of Status and Results

Article 13 (Disclosure of Status and Results)

The Company shall report current issues, such as AI security, and related improvement measures to its key decision-makers. Approved reports may then be shared with relevant departments to enhance the effectiveness of AI management.

The Company shall also disclose the implementation status of this Regulation and the results of its key activities through channels such as its corporate website and Sustainability Report, thereby communicating transparently with all stakeholders.

Addendum

This Regulation shall become effective on the date of its enactment.