

FOSUN 复星

Fosun Group Responsible AI Application Security Management and Usage Policy

[IT_011_V1.1]

[Group Digital Intelligence Committee and AI Line Information
Security Team、Group Risk Control Legal Department]

Fosun Group
2026-08-27

Chapter 1 General Provisions

Article 1 To ensure employees (including internal staff and external personnel working in the Group) comply with laws, ethical standards, and risk management requirements while using artificial intelligence (AI) technologies to enhance efficiency and innovation, and to prevent legal risks such as data breaches, illegal and infringing behavior, or non-compliance with national regulations, promote the safe, compliant, fair, transparent, accountable, and environmentally responsible use of AI, this standard is formulated in accordance with relevant laws and regulations including the Cybersecurity Law, the Data Security Law, the Personal Information Protection Law, the Interim Measures for the Management of Generative Artificial Intelligence Services, Regulations on the Management of Deep Synthesis of Internet Information Services, Measures for the Identification of Artificial Intelligence Generated Synthetic Content, Regulations on Promoting and Regulating the Cross border Flow of Data, as well as internal regulations such as the “Fosun Group Information Security Management Regulations” and the “Fosun Group Intellectual Property Management Measures”, to clarify the security management and usage standard of AI deployment and application in the Group.

Article 2 This standard applies to all departments, employees, and third-party personnel (including but not limited to outsourced personnel, vendor engineers, consultants, etc.) with access to information assets of Shanghai Fosun High Tech (Group) Co., Ltd. and its directly or indirectly managed subsidiaries and branches (hereinafter referred to as the Group). If industrial companies define their own AI policies, such policies must meet or exceed the standards set by the Group.

Article 3 Employees should proactively familiarize themselves with the Group's AI regulations, participate in AI usage training organized by the Group, enhance their security awareness and skills in AI usage, and strictly comply with the requirements of the Group's AI security management.

Chapter 2 Definition

Article 4 Group AI assets are a part of the Group's information assets, referring to various digital resources relied on or generated during the development and

operation of artificial intelligence technology, covering core elements such as data, algorithms, hardware, software, and services.

Article 5 Group AI applications refer to AI services independently deployed by the Group based on third-party or open-source models, accessible only to authorized users.

Article 6 Public AI applications refer to third-party AI services provided on public clouds or open platforms that can directly access AI capabilities through APIs, web pages, or applications without requiring self-built infrastructure and models. Public AI applications, including their models, must comply with national security technical standards and industry regulatory regulations.

Article 7 Confidential information refers to technical information, business information, and any other non-public information that employees or third-party personnel know or have access to during their employment or cooperation with the Group, which is considered confidential by the Group. This includes but is not limited to information disclosed by the Group to employees or third-party personnel, as well as any confidential information of others for whom the Group has confidentiality obligations.

Article 8 Personal data refers to various information related to identified or identifiable natural persons recorded in electronic or other forms, excluding anonymized information.

Article 9 Sensitive personal data refers to personal data that, once leaked or illegally used, is likely to cause harm to the personal dignity of natural persons or endanger their personal and property safety, including biometric, religious beliefs, specific identities, medical and health, financial accounts, travel trajectories, and personal data of minors under the age of fourteen.

Article 10 De-identification refers to the process of processing personal data to make it impossible to identify a specific natural person without additional information.

Article 11 Anonymization refers to the process in which personal data cannot be identified as a specific natural person and cannot be restored after processing.

Article 12 HITL (Human-in-the-Loop) refers to the introduction of human intervention, review, or feedback mechanisms at critical nodes during the operation of

an AI application system to ensure secure, accurate, and iteratively optimized decision-making.

Chapter 3 Declaration

Article 13 The Group shall strictly comply with the principles of legality, legitimacy, necessity, and data minimization when deploying and using AI application systems. Without employee consent or explicit authorization by laws and regulations, the Group shall not actively collect, store or process employees' personal data, including biometric data, communication content or location trajectories. If data collection is necessary for system operation, unless authorized by law, the consent of the personal data subject should be obtained, or the data should be anonymized.

Article 14 Employees shall not use the Group's AI assets for non-work-related purposes. The intellectual property rights of the job achievements generated, processed, and stored by employees using the Group's AI assets shall belong to the Group in accordance with the law, and shall not be disclosed or used without authorization.

Article 15 Within the scope permitted by laws and regulations, the Group may conduct necessary management, monitoring, evidence collection, and disposal of the Group's AI assets based on operational management, network security, confidentiality management, compliance auditing, and cooperation with regulatory or judicial authorities in accordance with the law. The relevant rules should be explained to employees and third-party personnel in advance through this standard, labor contracts, employee manuals, or notices. When an attack, leakage, infringement or illegal use occurs or is suspected to occur, the Group may take necessary protective measures such as interception, isolation, deletion, and account freezing in accordance with the law. The handling of violations shall be carried out in accordance with Chapter 7 and relevant regulations of the Group.

Chapter 4 Organization and Responsibilities

Article 16 Group Digital Intelligence Committee and AI Line Information Security Team

(1) Responsible for formulating, interpreting, and revising the Group's "AI Application Management and Usage Standards", as well as supervising and coordinating the implementation across the Group.

(2) Responsible for liaising with subsidiary companies to ensure the implementation of group "AI Application Security Management and Usage Standards". Supervise the execution of "AI Application Security Management and Usage Standards in subsidiary companies.

(3) Responsible for compiling reports on AI applications security status and incidents of the Group and subsidiary companies, and submitting them to the Group management.

(4) Organize security inspections, analyze overall security conditions for AI applications, and propose risk mitigation strategies.

Article 17 Group Business Departments

(1) Supervise department employees to ensure lawful and compliant use of AI applications.

(2) Ensure that department AI applications meet Group security standards and specifications, as well as applicable legal requirements, during design, development and deployment phases.

(3) Designate a person in charge of AI applications in the designated department, who will be accountable for AI output results, risk-related decisions, and compliance, and for investigating and handling the errors or harm caused by AI according to corresponding emergency procedures;

(4) Develop and update security emergency strategies and contingency plans for department AI applications, and organize regular testing and drills.

Article 18 Group Employees

(1) Lawful and compliant use of AI applications.

(2) Complete relevant AI application ethics and security training.

(3) Proactively report suspicious AI application usage behavior and potential infringement or leakage clues.

Chapter 5 AI Application Deployment Standards

Article 19 Group AI applications shall prioritize private deployment to mitigate data leakage risks. If non-private deployment AI models are used, approval of the Group Digital Intelligence Committee and AI Line Information Security Team and Group Risk Control Legal Department must be obtained. AI model suppliers must provide a protocol guarantee that the data will not land, or provide other data processing, retention, training and usage restrictions and audit clauses that meet the Group's requirements. AI model suppliers are not allowed to use group data for optimizing or training their general models.

Article 20 AI models deployment must comply with national security technology standards and industry regulatory requirements. All third-party or open-source AI models shall be evaluated by the Group Digital Committee and AI Line Information Security Team, followed by a technical assessment report.

Article 21 AI application deployment must adhere to the Group information security regulations:

(1) When using Group data as training data or deploying AI applications, data classification and grading control should be implemented in accordance with the “Fosun Group Information Security Management Regulation”, and the following principles should be followed:

- Confidential level and above: After approval, only use of AI applications deployed privately by Group for processing;
- Secret level: Only use Group self-built AI applications for processing;
- Non-confidential: Can use third-party public AI applications for processing;

(2) Ensure that the source of training data is legal and prohibit the use of illegally crawled, infringing on intellectual property rights, or unauthorized data as training data; Training data involving personal data must have a legal processing basis and undergo de-identification processing within the necessary scope to achieve the processing purpose. Sensitive personal data must obtain the individual consent of the personal data subject or have other legal processing bases, and additional encryption and de-identification measures such as privacy enhancement technology must be applied to

ensure data security. Before collection, a security assessment must be conducted on the data source to ensure traceability and timeliness. Legitimate authorization records for open source data, collection records for self collected data, transaction proof for commercial data, and clear authorization for user input information should be retained. After the personal data subject cancels their account, the relevant personal data should be deleted or anonymized within the commitment period or statutory period, except for those required by laws and administrative regulations to be retained or necessary for the Group to fulfill its legal obligations in accordance with the law. The requirements and deadlines for deletion or anonymization should be prominently stated in the privacy policy or user instructions.

(3) All AI applications of the Group must deploy a content security monitoring engine to block data input containing malicious code, adversarial samples, or beyond authorized scope. Establish an access control matrix for input data and business systems to ensure that only authorized modules can access confidential and higher-level data. Set the retention period for input data, and if long-term storage is necessary, implement encrypted storage after obtaining regulatory approval.

(4) All Group AI applications must deploy a content security monitoring engine to filter in real-time generated content involving illegal information, trade secret leaks, and violations of public order and good customs. The output results must be automatically verified to ensure compliance with the requirements of the Group's various rules and regulations.

(5) Encrypt data during storage and transmission to prevent data leakage or tampering.

(6) Unified identity authentication with least-privilege must be set in all Group AI applications.

(7) Before AI applications deployed by the Group within China provide services to overseas users of the Group, they shall assess potential data cross-border compliance risks. If involving two-way cross-border data flows, they must simultaneously comply with the data protection and AI regulatory requirements of both China and relevant foreign jurisdictions. Strictly prohibited from going live or providing services overseas before completing legal compliance assessments and obtaining corresponding approvals.

(8) The testing environment for Group AI applications must be physically isolated from the production environment.

(9) Deploy real-time monitoring system to detect model abuse.

(10) Group AI applications must develop emergency plans for data breaches, model attacks, and conduct regular disaster recovery drills. The emergency plans shall comply with the "Fosun Group Information Security Emergency Response Management Measures".

(11) Regularly conduct vulnerability scan and penetration testing on Group AI applications, identify potential threats, and fix high-risk vulnerabilities.

(12) Establish AI service access logs and keep records on schedule.

Article 22 To cope with the energy consumption, water resource use, and carbon emission risks brought by the growth of AI computing power, the Group and its partners should follow the following requirements in AI model training, deployment, and operation:

(1) Prioritize the use of energy-saving hardware (such as efficient GPUs, liquid cooling systems) and optimization algorithms to reduce computational load and energy waste.

(2) Third party AI service providers should prioritize data centers that use renewable energy and have green certification under the same conditions.

Article 23 The group shall deploy a mechanism for continuously monitoring the performance of AI models to detect model drift caused by changes in data patterns or external conditions. Specific requirements:

(1) Establish a model performance baseline and regularly evaluate key indicators such as accuracy and false positive rate.

(2) When a significant decrease in model performance is detected, corrective measures should be triggered immediately, including but not limited to retraining with new data, adjusting parameters, or switching model versions.

(3) All model updates should undergo testing and approval processes, and change logs should be recorded to ensure the long-term reliability of the application system.

Article 24 When using external AI model APIs for Group applications, the following regulations shall be followed:

(1) All external API must be evaluated by Group Digital Intelligence Committee and AI Line Information Security Team.

(2) It is prohibited to use APIs that fail to pass security certification in scenarios involving sensitive areas such as national security, finance, and medical.

(3) API suppliers shall provide corresponding security certification qualifications, privacy policies, and data storage instructions.

(4) Follow Article 20 standards.

Article 25 During the design, training, deployment and use of the Group AI applications, potential algorithmic biases should be actively identified, evaluated, and mitigated to ensure fair and non-discriminatory behavior. Specific requirements include:

(1) The collection and construction of training data should ensure diversity and representativeness, and avoid discrimination or adverse effects on specific populations due to imbalanced data.

(2) Regularly conduct bias audits and fairness assessments on AI models, test the output differences of the models in different population groups, and generate audit reports.

(3) Take corrective measures such as data rebalancing, algorithm adjustment, or retraining for biased models to prevent AI applications from continuing or amplifying existing social inequality.

Article 26: The Group shall fulfill its obligation to fully disclose the use, capabilities, limitations, data sources, and potential risks of AI application systems, and ensure that AI output results or decision-making processes have understandable reasons. Specific requirements include:

(1) All user-oriented AI applications should clearly define the boundary between "can do" and "cannot do" in the interactive interface or related documents, and should not exceed the authorized scope to intervene in key matters that should be independently judged by humans. It should also be clearly stated that "this is

generated/assisted decision-making by AI systems" and should not impersonate humans.

(2) For the output results that are required to be explained, the system should provide corresponding reasonable explanations.

(3) AI applications involving personal data processing or high-risk decision-making should be used with effective control measures in place, and their data sources, model versions, key parameters, and risk warnings should be actively disclosed.

Article 27 All content generated by AI application systems (including but not limited to text, images, audio, video, and decision suggestions) should be clearly labeled when output, prompting users that the content was generated by AI. Specific requirements include:

(1) The annotation method should be clear and not easily overlooked, such as adding the "AI generated" label at the end of the text, adding watermarks at the edges of the image, and broadcasting "The following content is synthesized by AI" at the beginning of the voice.

(2) For AI applications that assist decision-making, it should be noted next to the decision result that "this result is an AI assisted suggestion and requires manual confirmation".

Article 28 Establish an appeal process for individuals or entities affected by AI decisions, ensuring their right to raise objections to AI output results. The appeal process should:

(1) Easy to access (such as online forms, customer service hotlines), open and transparent, and without setting discriminatory conditions based on user identity.

(2) Fair and responsive, with clear processing deadlines and designated personnel for review.

(3) Record the appeal content, handling process, and results, regularly summarize and analyze them to improve the quality and ethical compliance of the AI system.

(4) Group users can contact the AI application team: AI@fosun.com.

Article 29 The Group requires AI application systems to undergo third-party evaluation and certification to ensure compliance with international standards for responsible artificial intelligence practices. Specific requirements include:

(1) Priority should be given to industry guidelines such as ISO/IEC 42001 (Artificial Intelligence Management Systems) and NIST AI Risk Management Framework.

(2) For AI applications involving high-risk scenarios or core businesses, external independent organizations should be commissioned to conduct compliance audits and certifications.

(3) The certification results should be publicly disclosed to relevant stakeholders in accordance with laws, regulations, and group information disclosure regulations to enhance system credibility and social trust.

Article 30 When Group AI application is decommissioned, the application owner shall retain or clear the data in accordance with Group regulations.

Chapter 6 AI Application Usage Standards

Article 31 Employees shall prioritize using AI applications built by the Group. If public AI applications need to be used, employees must utilize those recommended by the Group and comply with the relevant data security and compliance requirements outlined in this Code.

Article 32 Employees are prohibited from entering illegally crawled, infringing on intellectual property rights, or unauthorized data when using public AI applications. Prohibit unauthorized input of personal data and sensitive personal data. Only when the Group has a legal basis for processing, the system clearly allows it, and protective measures such as de-identification have been taken, can input be made within the scope of authorization. Prohibit the input of any confidential information of the Group.

Article 33 Employees are prohibited from entering illegally crawled, infringing on intellectual property rights, or unauthorized data when using the Group's AI applications. Prohibit unauthorized input of personal data and sensitive personal data. Only when the Group has a legal basis for processing, the system clearly allows it, and protective measures such as de-identification have been taken, can input be made within the

scope of authorization. Prohibit the input of any confidential information of the Group. Confidential information must be approved, authorized, and desensitized before it can be entered.

Article 34 When employees within China use AI applications deployed overseas, they must comply with China relevant laws and regulations concerning cross-border data. Sensitive personal data is strictly prohibited in overseas-deployed AI applications. When inputting non-sensitive personal data is genuinely necessary for business purposes, it must undergo a necessary legality assessment and be confined to the minimum scope necessary.

Article 35 When employees use AI applications outside China, they must comply with the data protection and AI regulatory laws and regulations of the country or region where they are located, while ensuring no violation of Chinese laws regarding data export, national security and personal data protection.

Article 36 Employees shall comply with relevant laws and regulations when using AI applications, and should not engage in any behavior that harms the legitimate rights and interests of the Group or others. It is prohibited to use AI applications to generate, produce, or disseminate any illegal content, including but not limited to:

- (1) Opposing the basic principles established by the Constitution.
- (2) Those who incite subversion of state power, overthrow the socialist system, and endanger national unity, sovereignty and territorial integrity.
- (3) Disclosing state secrets, endangering national security, or damaging national interests.
- (4) Those who incite ethnic hatred, ethnic discrimination, undermine ethnic unity or infringe upon ethnic customs and habits.
- (5) Disrupting national religious policies, promoting cults and superstitions.
- (6) Spreading rumors, disrupting social order, and disrupting social stability.
- (7) Disseminating obscenity, gambling, violence, or inciting crime.

(8) Insulting or slandering others, infringing upon the reputation rights, privacy rights, intellectual property rights, and other legitimate rights and interests of the Group or others.

(9) Using subconscious, intentional manipulation, or deceptive techniques, or exploiting loopholes such as age, disability, or specific socioeconomic status to substantially distort individual behavior.

(10) Real time remote biometric identification (RBI) conducted in public places without legal authorization

(11) Endangering social morality or the excellent cultural traditions of the nation.

(12) Other violations of laws and regulations.

Article 37 The key decisions made with the assistance of AI systems must maintain HITL, embed effective and traceable human supervision mechanisms, and grant human intervention, override, or escalation authority and capability. Specific requirements include:

(1) AI systems shall not make irreversible or high-risk decisions independently without human supervision or review mechanisms.

(2) The entire process of manual intervention should be documented in writing or electronically as a basis for compliance audits.

Chapter 7 Penalty Principles

Article 38 Those who violate the above requirements and the Group's information security management regulations will be penalized according to relevant regulations. If losses are caused to the Group, compensation will be sought in accordance with legal provisions.

Article 39 For serious violations causing significant losses to the Group, or cases constituting criminal offenses, the matter will be transferred to judicial authorities for legal liability investigation.

Chapter 8 Supplementary Provisions

Article 40 This regulation is interpreted and revised by the Group Digital Intelligence Committee and AI Line.

Article 41 This regulation shall take effect following the approval by the Board of Directors of Fosun International Limited.

Article 42 This regulation shall take effect from the date of promulgation.