FOSUN 复星

Fosun Group
Information Security Management System

[IT_001 _V3.0]

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

Fosun Group
August 28, 2025

Chapter I General Provisions

Article 1 To enhance the information security awareness of Group employees, regulate their behavior, guide them in the reasonable and safe use of information assets, prevent intentional or unintentional actions that compromise information security, and improve the overall information security level of the Group, this system is established based on the current situation of the Group. It aims to clarify the Group's information security management requirements and the daily work norms for employees. At the same time, the Group has established and continuously improved its information security system, identified and evaluated business information security risks, implemented response and mitigation strategies to minimize information security risks. Given the dynamic changes in information security risks, the Group will continue to improve this system to ensure its effectiveness and adaptability.

Article 2 This system applies to Shanghai Fosun High Technology (Group) Co., Ltd., its directly or indirectly managed or controlled subsidiaries and affiliates, as well as all branches (hereinafter collectively referred to as the "Group"). It encompasses all departments, all employees, and third-party personnel.

Chapter II Statement

Article 3 Employees should use work computers, work phones, work electronic terminals, work email systems, and the internal network of the Group's IT devices and information systems solely for work purposes. Only work-related information should be stored on these devices. It is prohibited to use Group IT assets (including computers, phones, work email, etc., provided by the Group) for personal matters to prevent the Group from infringing on personal privacy in information security management. Employees should not expect any privacy regarding the information stored or transmitted on these devices or information systems.

Article 4 All information assets generated, processed, and stored by employees using Group assets are owned by the Group. The Group has the right to collect, monitor, process, or delete such information assets.

Article 5 The Group manages information assets to ensure the security, accuracy, and consistency of data throughout the entire lifecycle. For operational management, security management, and legal investigation and evidence

purposes, the Group's management department reserves the right to monitor, recover, replicate, disclose, use, and delete Group IT assets without prior notice to employees or the need for employee authorization. In cases where there is suspicion of attack, damage, or leakage of Group assets, the Group may intercept, delete, block, and take any necessary actions to protect Group assets. If violations by Group personnel are discovered, appropriate disciplinary actions or legal actions may be taken against them.

Chapter III Organizational Structure

Article 6 The organizational structure of Group Information Security Management includes:

(Ⅰ) Group Security Management Committee;

(Ⅱ) Group Information Security Management Team;

(Ⅲ) Operations and Execution Team;

(Ⅳ) Operation and maintenance execution team;

Article 7 Organization Members and Responsibilities

(Ⅰ) Group Security Management Committee:

1. Composed of the technical leaders of the Group headquarters and the heads of the technical divisions of each member company;
2. Responsible for overseeing and coordinating the implementation of the Group's information security management standards within the company;

(Ⅱ) Group Information Security Management Team:

1. Composed of the Group Digital Intelligence and AI Information Security Team;
2. Responsible for formulating, interpreting, and modifying Group information security management systems, technical regulations, emergency plans, etc. Other relevant departments should implement corresponding management systems according to their respective lines;
3. Responsible for coordinating with member companies to ensure the implementation of information security management requirements and supervising the execution of information security management within member companies;
4. Responsible for summarizing and compiling reports on the internal information security status and security incidents of the Group and member companies, and submitting them to the Group Security Management

Committee;

5. Organizes reviews of major information security policies and technical operational strategies, drafts overall information security strategic plans, and monitors their implementation;
6. Organizes information security inspections, analyzes the overall information security situation, proposes analysis reports, and preventive measures against security risks;
7. Tracks advanced information security technologies, organizes training, assessments, and publicity of information security knowledge;
8. Formulates and updates emergency strategies and contingency plans for Group networks and information systems;
9. Organizes annual tests and drills for information security emergency strategies and contingency plans;

(Ⅲ) Group Security Promotion Team:

1. Each member company shall designate at least one information security liaison officer;
2. Responsible for promoting the implementation of Group information security requirements within their respective units;
3. Responsible for reporting information security incidents discovered within their units to the Group Security Operations and Execution Team;

(Ⅳ) Operations and Execution Team:

1. Composed of the head of the operations team and operations personnel;
2. Responsible for network operation management, implementing network security policies and guidelines;
3. Ensure strict adherence to system security policies during system development and construction to ensure accurate implementation of system security features;

Chapter IV Security of the Working Environment

Article 8 Employees must adhere to access regulations for secure areas. When entering or leaving unauthorized areas, approval from relevant responsible persons must be obtained in accordance with Group regulations.

Article 9 Employees are responsible for securely storing their identification credentials. In case of loss, they must promptly report to the issuing department.

It is prohibited to lend identification credentials to others. Upon leaving the Group, employees must return issued identification credentials.

Article 10 External visitors accessing office premises must have their identities and reasons for visit verified with employees and registered. Visitors must be received at the entrance by the host employee and accompanied throughout their visit. Access and exit logs must be kept for a minimum of three years.

Chapter V User Account Security

Article 11 Any account must be requested according to the principle of "least privilege" and may only be used within the authorized scope approved at the time of application. It is strictly prohibited to access unauthorized resources using an account. The account owner takes all responsibilities and consequences arising from its use. Approval authorities must verify needs based on the principle.

Article 12 Before the account is officially activated, a password must be added to the account. All account passwords should comply with the Group's password management requirements.

Article 13 Passwords should be securely stored. Without reliable physical control measures, passwords should not be written on paper or stored in electronic files (cloud notes). Automatic saving of passwords in terminal software (such as browsers) is prohibited. It is forbidden to disclose one's own or others' password information, and attempting to steal or guess others' account passwords is strictly prohibited.

Article 14 When there are changes in job responsibilities, users should proactively apply for changes in account or physical key permissions. When access to a system is no longer required, users should actively apply for account or permission cancellation. For accounts or physical keys that cannot be deactivated, they should be promptly transferred to the designated responsible person in the department. Upon resignation, all accounts and physical keys should be promptly handed over.

Chapter VI Use of Information equipment

Article 15 All terminal computers must be equipped with desktop management software and antivirus software as required by the Group. Employees are not permitted to delete or modify these software settings.

Article 16 When leaving the workstation, the computer should be locked or turned off. Terminal information equipment must be securely stored, and portable devices should not be left on desks during weekends or holidays.

Article 17 It is forbidden to use Group-distributed equipment for non-work purposes. Working equipment should generally not be connected to networks outside the office environment. If such connection is necessary for work, virus scanning must be performed before reconnecting to the office network.

Article 18 Unauthorized use of mobile media is prohibited. Before authorized use, mobile media must undergo virus scanning and may only be used after confirming its safety.

Article 19 Terminal equipment, mobile media, physical information, and software must not be removed from the office area without authorization.

Article 20 No one is allowed to exchange information equipment without authorization. It is prohibited to dismantle, repair or replace computer hardware without authorization..

Article 21 Before submitting equipment and storage media for maintenance, recycling, or scrapping, important data on the equipment must be backed up and securely destroyed.

Article 22 Personal information devices should be kept safe. In case of loss, it must be promptly reported to the IT department to lock the corresponding account and prevent unauthorized use.

Article 23 Unauthorized connection of peripherals to Group computers is prohibited. This includes but is not limited to modems, wireless network cards, USB storage devices, optical disc burners, card readers, smartphones, and other devices that directly communicate with the Group's internal network.

Chapter VII The Use of the Software

Article 24 When initially installing or reinstalling the operating system on terminal equipment, the operating system provided by the Group must be used. It is prohibited to install other operating system installation packages arbitrarily.

Article 25 Employees must use software provided by the Group. Installing software unrelated to work, or modifying, disabling, or uninstalling software required by the Group without authorization is prohibited. Downloading or using unauthorized pirated software is strictly prohibited. Employees personally bear the corresponding infringement liability if disputes arise due to their personal

use of pirated software. If the company assumes compensation liability to external parties due to an employee's infringement, the company reserves the right to recover from the employee.

Article 26 Without authorization from the Group's security department, the use of scanning software, malicious scripts, and other attack tools to scan, test, or disrupt the Group's intranet and systems is strictly prohibited.

Chapter VIII The Use of Networks

Article 27 Prohibited to connect unauthorized computer devices to the Group network.

Article 28 Unauthorized modification of access device network settings is strictly prohibited.

Article 29 It is prohibited to disseminate Group WiFi password.

Article 30 Except for the internet access provided by the company, in the office environment, any means (such as wireless network cards, modems, etc.) to connect to the internet or other external networks without approval are prohibited. For approved usage, disconnecting from the company network is required before connecting to external networks.

Article 31 Access the Internet legally and civilly, and prohibit illegal activities on the Internet.

Article 32 Do not misuse Group network resources for activities unrelated to work, such as accessing websites and internet services unrelated to work, downloading files unrelated to work, playing online games, or using chat tools.

Article 33 Unauthorized computer terminals with one of the following conditions are prohibited from accessing the Internet:

(I). Involving Group top-secret or confidential information;

(II). Not installed with designated antivirus software and desktop management software, and other security management software, with virus definitions not timely updated;

(III). Evaluated to have other security risks, deemed unsuitable for internet access;

Chapter IX The Use of E-mail

Article 34 Strictly keep the password of own email account confidential. If it is used by others, all consequences arising from this shall be borne by the email account owner.

Article 35 Using email services to send non-work-related emails is prohibited. Personal privacy information must not be stored in work email.

Article 36 It is strictly prohibited to use the Group email for non-work purposes, especially for the registration of entertainment, shopping, dating, etc.

Article 37 Dedicated email must be assigned to specific individuals to be responsible for the secure use. Sharing dedicated email among multiple users is prohibited.

Chapter X Data Security Management

Article 38 According to the value of the Group information, the sensitivity of the content, and the scope of access, sensitive information is classified into three levels: top secret, confidential, and secret, as well as non-confidential information, with the classification level designated by the information owner. When information of different classifications is gathered together for processing, publication, or storage, the classification level is determined based on the highest level of information in the gathered set.

Article 39 Important work data should be backed up in a timely manner to prevent data loss.

Article 40 Do not provide sensitive corporate data (including "Top Secret," "Confidential," and "Secret" data) to unauthorized individuals or entities, or remove corporate information from the corporate network environment without authorization, including copying to personal devices, sending to personal public email accounts, or uploading to the internet.

Article 41 When authorized to provide sensitive data to external organizations or individuals, it must be transmitted through the approved channels and methods as authorized by the data owner management department.

Article 42 When transmitting and storing sensitive data using mobile media, the data or media should be encrypted, and sensitive data should be promptly cleared from the media after use.

Article 43 Any behavior involving the leakage of personal information/data of customers, employees, or users should be promptly reported to the relevant department of the Group.

Article 44 Leaking personal privacy or personal information of customers, employees, or users is illegal. Unauthorized copying, transmission, disclosure, and use of the Group's customer, employee, and related user personal

information data without following the Group's approval process is strictly prohibited.

Article 45 Unauthorized reprinting, copying, excerpting, and external transmission of external information purchased by the Group that has third-party copyright is prohibited. If the information contains copyright or confidentiality requirements, strict adherence is required.

Chapter XI Personal Information protection

Article 46 The industry should collect personal information legally and compliantly through self-developed applications or third-party software products.

Article 47 The corporation shall only use personal information within the scope necessary to achieve the purposes informed to the information provider. In the event of a change in the purpose of information use, prior consent from the information provider must be obtained.

Article 48 All business systems involving personal information must comply with national/industry/Group regulations. Systems that do not meet these requirements must be rectified before they can be launched.

Article 49 Various business systems should classify and categorize personal information based on its type, source, sensitivity, and purpose, and implement targeted management or security measures accordingly.

Article 50 Information should only be retained for the necessary period, and should be deleted or abandoned after the required period ends.

Article 51 Necessary technical measures, such as encryption and data backup, should be adopted to ensure the security of personal information.

Article 52 Unauthorized access and illegal use of user personal information is prohibited. Those causing impact shall be subject to relevant corporate penalties and national legal penalties.

Article 53 In case of incidents such as personal information leakage or loss, companies shall promptly and appropriately respond, take measures to limit the impact, and fulfill obligations as required by laws and regulations.

(I). Take timely measures to prevent losses or minimize losses caused by accidents;

(II). The company should promptly notify the information owners;

(III). Identify the cause of the incident and take necessary measures to prevent similar events from happening;

Article 54 Conduct corresponding security education and training for personnel who have access to personal information, including management, technical, and operational staff, to ensure they possess necessary knowledge and skills. Strengthen the awareness of all employees towards the protection of personal information through internal training, announcements, and other means.

Article 55 The Group and its subsidiaries shall regularly inspect and evaluate the work of personal information protection, promptly identifying and correcting any issues.

Chapter XII Antivirus Requirements

Article 56 Unless technically restricted, any device connecting to the Group network must first install designated security access control software or antivirus software prescribed by the Group. Virus scanning must be conducted, and only after confirming the computer is safe and virus-free can it be connected.

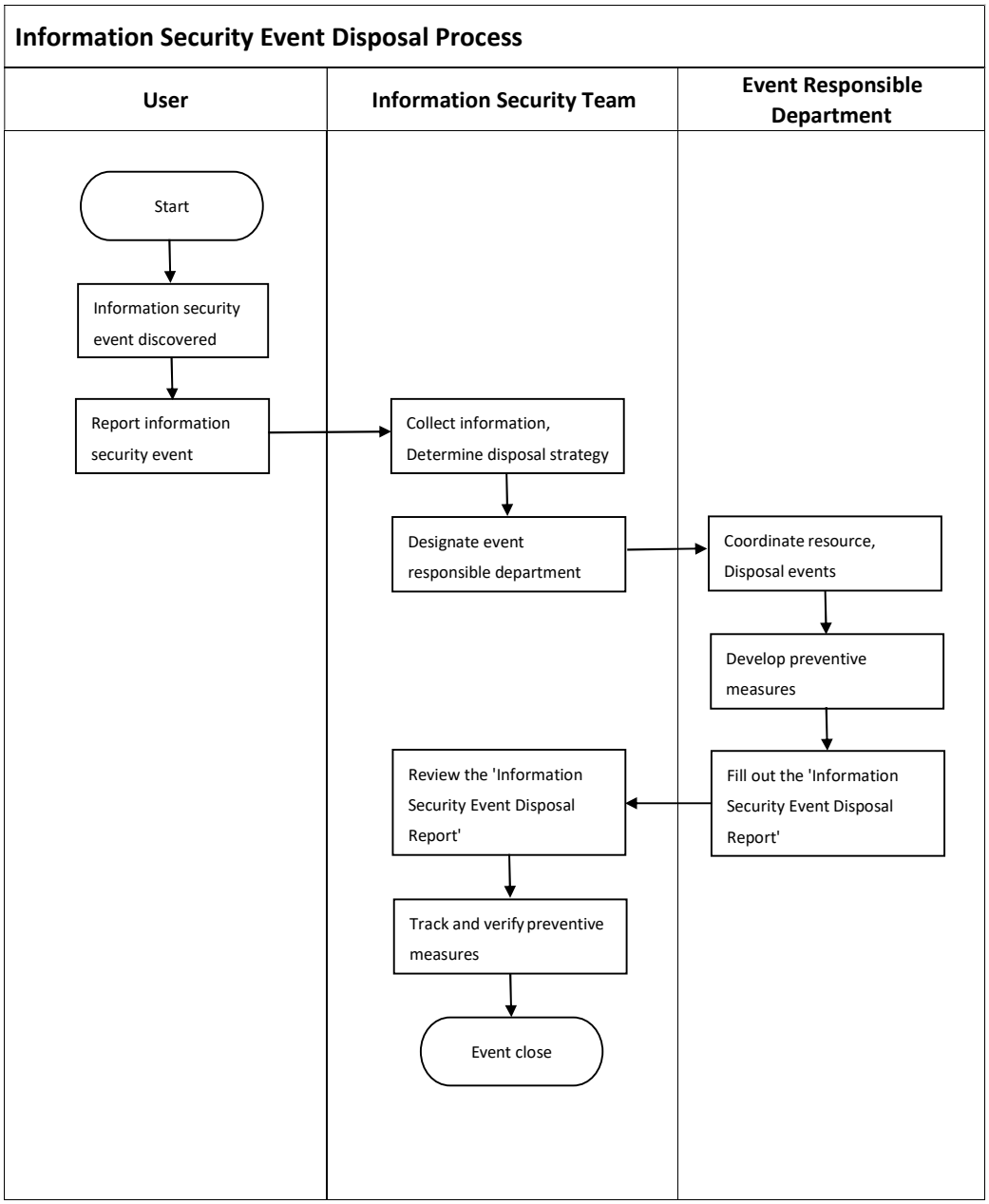
Article 57 When using personal computers, antivirus software must be run, virus databases updated in a timely manner, system patches upgraded, and regular virus detection and removal performed. Without permission, installing antivirus software or virus monitoring programs not specified is prohibited.

Article 58 Before using USB drives, CDs, and other removable media, virus detection must be conducted, and any removable media not tested by antivirus software should not be used.

Article 59 If a computer is found infected with a virus or data is abnormally deleted or damaged, immediately disconnect from the network and promptly report the virus situation to information security management team.

Chapter XIII Information Security Event

Article 60 After discovering an information security event, Group employees should report it to the information security management team according to the following process.



Article 61 After receiving the report, the information security management team should promptly formulate a disposal strategy and designate a responsible department for handling.

Article 62 Event responsible department shall coordinate resources to handle the incident. After the event is resolved, corrective and preventive measures shall be formulated and implemented, and an "Information Security Event Disposal Report" shall be filled out.

Article 63 After receiving the "Information Security Event Disposal Report", the Information Security Management Group should evaluate the report and track and verify corrective and preventive measures.

Chapter XIV Principles of Punishment

Article 64 For violations of the above requirements and Group information security policy, penalties will be imposed according to relevant Group regulations.

Article 65 Individuals violating this regulation will be subject to the following punitive measures based on the severity of the offense:

(I). Warning and advisory notice;

(II). Temporary suspension of account or computer terminal access to the network, accompanied by notification and criticism;

Article 66 For serious cases resulting in significant losses to the company or constituting criminal offenses, the individual will be handed over to judicial authorities for legal liability investigation.

Chapter XV Supplementary Provisions

Article 67 This system is interpreted and revised by the Group Digital Intelligence and AI Information Security Team and the Group Risk Control Legal Department.

Article 68 This system shall take effect from the date of its publication.