Grand Pharmaceutical Group Limited
Information Security and Privacy Protection Policy

Chapter I General Provisions

Article 1 In order to further safeguard the information security and privacy protection of Grand Pharmaceutical Group Limited and its member companies (hereinafter referred to as "Grand Pharma", the "Company", "we" or "us"), to ensure the confidentiality, integrity and availability of data, to prevent risks such as information leakage, tampering and loss, and to require contractors, suppliers and business partners to comply with the same or higher standards of information security and privacy protection, the Company has formulated this policy in accordance with applicable laws and regulations, including but not limited to the Cybersecurity Law, the Data Security Law, the Personal Information Protection Law, the Measures for Data Export Security Assessment and the Measures for Standard Contracts for Cross-border Transfer of Personal Information.

Article 2 This policy applies to the Company and all its member companies, including all employees, contractors, suppliers, business partners and relevant third parties, and covers all information systems, data processing activities and information assets related to the Company's business operations.

Chapter II Principles of Information Security and Privacy Protection

Article 3 Grand Pharma shall adhere to the following principles in carrying out all business activities:

(i) Principle of Compliance and Legality. The Company strictly complies with applicable laws and regulations on cybersecurity, data security and personal information protection in China and in the countries or regions where it operates, including but not limited to the Cybersecurity Law, the Data Security Law, the Personal Information Protection Law, and the Measures for Standard Contracts for Cross-border Transfer of Personal Information, ensuring that all information processing activities are lawful and compliant.

(ii) Principle of Data Minimisation and Purpose Limitation. The Company shall collect, use, store and process personal information and data only to the extent necessary to achieve specific business purposes, shall not exceed the authorised scope, and shall not use such data for unrelated purposes. All data processing activities shall have clear, lawful and legitimate purposes.

(iii) Zero-Tolerance Principle. The Company explicitly prohibits any conduct in violation of this policy. Disciplinary actions shall be imposed for violations such as data leakage, unauthorised access, or misuse of personal information.

Chapter III Information Security Protection Commitments

Article 4 Grand Pharma attaches great importance to information security and strives to ensure the confidentiality, integrity and availability of the Company's information assets. The Company undertakes to implement the following principles and measures in all business activities:

(i) Continuous Improvement of Information Security Management System. The Company has established and continuously improves its information security management system, regularly assessing, updating and optimising security strategies, technical measures and management processes, and enhancing its security capabilities to address the evolving cybersecurity threat landscape.

(ii) Ensuring Data Integrity. The Company adopts effective technical and managerial measures to prevent data from being tampered with, leaked, damaged or accessed unlawfully. Sensitive data shall be encrypted and subject to enhanced technical controls to ensure integrity, accuracy and security throughout its lifecycle, including generation, storage, transmission, use and destruction.

(iii) Proactive Monitoring and Timely Response to Security Threats. The Company deploys advanced threat detection and response mechanisms to continuously monitor network and system activities, and to promptly identify, analyse and handle abnormal behaviour, security incidents and potential risks, thereby minimising the impact of security incidents. In the event of an information security incident, the Company shall maintain transparent communication with affected parties and communicate measures taken to remediate vulnerabilities and prevent future risks.

(iv) Establishment of an Responsibility Mechanism for the Entire Workforce. The Company's information security management system applies to all employees. Responsibilities and obligations at all levels are clearly defined. Through confidentiality agreements, training and assessment mechanisms, and accountability systems, the Company strengthens employees' awareness of information security, adhering to the principle of "Systematic planning and comprehensive control; information security as everyone's responsibility; disaster prevention and sustainable operation; inspection, evaluation and continuous improvement."

(v) Requiring Third Parties to Comply with Information Security Standards. The Company requires all third parties (including but not limited to suppliers and business partners) engaging in business cooperation with the Company to comply with the Company's information security and privacy protection standards in data processing, system access and service provision. All third parties must undertake, through contractual commitments, to comply with data protection obligations equivalent to or higher than those set out in this policy. Any violation shall result in termination of cooperation and pursuit of legal liability.

Chapter IV Privacy Protection

Article 5 Personal information collected by Grand Pharma may include:

(i) Personal identity and contact information of data subjects, such as name, email address, telephone number, country and city of residence.

(ii) Employment information, such as employer, job title and employment history.

(iii) Information obtained through communications, such as comments, questions, feedback and other content provided when using website functions.

(iv) Adverse event information, such as age, weight, medical history, allergy history, description of adverse reactions and medication usage.

(v) Other sensitive personal information necessary for fulfilling statutory obligations or conducting specific business activities, such as clinical trial data, patient health records, and personal identity and health information contained in pharmacovigilance reports.

Article 6 The Company may use personal information for the following purposes:

(i) Reviewing opinions or inquiries submitted by data subjects and providing corresponding service support.

(ii) Enforcing the terms and policies of the Company's website.

(iii) Processing and responding to requests, inquiries, applications, complaints and feedback from data subjects.

(iv) Providing support and responding to requests, feedback and inquiries from data subjects.

(v) Monitoring, operating, maintaining and managing the Company's website.

(vi) Processing and resolving technical issues and malfunctions of the Company's website.

(vii) Ensuring the effective and efficient operation of the Company's website.

(viii) Detecting, preventing or otherwise addressing security, fraud or technical-related issues.

(ix) Improving and enhancing the functionality and performance of the Company's website and related services.

(x) Properly managing and maintaining the relationship between the Company and users.

(xi) Supporting the Company's day-to-day business management.

(xii) Protecting, enforcing or maintaining the Company's lawful rights and interests, including rights and interests arising from violations of the Company's website terms and conditions.

Subject to obtaining consent from the data subject and where permitted by law, the Company may also process information for other purposes disclosed in advance.

Article 7 Data subjects have the right to independently determine the collection, use, retention and processing of their personal data and enjoy the following rights:

(i) Right of Access. Data subjects have the right to request confirmation as to whether we process their personal information and to obtain a copy of such personal information.

(ii) Right to Rectification. Where any personal information collected by us is incomplete or inaccurate, data subjects have the right to request correction or updating of such information.

(iii) Right to Erasure. Under specific circumstances, data subjects may request deletion of all or part of their personal information, including but not limited to the following situations:

- Our processing of personal information violates applicable laws or administrative regulations;
- Personal information has been collected or used without the consent of the data subject;
- Our processing of personal information breaches any agreement between us and the data subject;
- The purpose of processing has been achieved, cannot be achieved, or is no longer necessary for achieving the purpose; or
- The data subject has withdrawn his or her consent for the processing of personal information.

(iv) Right to Opt-in Consent. For processing of sensitive personal data or for non-essential purposes, the Company shall clearly inform data subjects of the necessity of such processing and its potential impact on personal rights and interests, and shall obtain explicit, voluntary and affirmative "opt-in consent". Default selection or forced consent is strictly prohibited.

(v) Right to Withdraw Consent. Where the processing of personal information is based on the consent of the data subject, the data subject has the right to withdraw such consent at any time.

(vi) Right to Data Portability. Data subjects have the right to receive their personal information provided to us in a structured, commonly used and machine-readable format and to transmit such personal information to another entity.

(vii) Right to Be Informed. Data subjects have the right to be informed of the purposes, methods, scope, retention period and third-party sharing arrangements relating to the processing of their personal information.

Article 8 The Company shall retain personal information for the period necessary to provide the Company's website, related services and business operations, or for the period required to achieve the purposes of information collection. Depending on the nature of the information collected, such information shall generally be deleted 18 to 36 months after retention.

Article 9 The Company implements security measures in accordance with this Privacy Policy and has established physical, electronic and administrative safeguards to ensure the security of user information processed by the Company.

Article 10 The Company shall disclose data to third parties (including service providers, affiliates, law enforcement agencies and competent authorities) only under lawful circumstances, such as performance of contracts, obtaining user consent, compliance with legal obligations, or response to security incidents. Such third parties must comply with the information security and privacy protection standards established by the Company.

Article 11 Where the Company conducts any form of cross-border data transfer (including provision of personal information, important corporate data, technical secrets or other assets to overseas recipients) it shall strictly comply with the applicable laws and regulations of both the data exporting and receiving jurisdictions. For cross-border transfers involving personal information, the Company shall fulfil its statutory obligation to provide comprehensive notification to individuals (including but not limited to information regarding the overseas recipient, processing purposes, methods, categories of data and methods for exercising rights) and shall obtain separate consent from the individual in accordance with applicable laws.
The Company shall update its management measures in a timely manner in response to changes in laws, regulations and business environment.

Chapter V Oversight

Article 12 The Company's Information Management Department shall be responsible for organising and guiding the day-to-day implementation of this Policy within the Company to ensure its effective execution. The Board of Directors of Grand Pharmaceutical shall oversee the implementation of this Privacy Policy and its key performance indicators.

Article 13 The Company incorporates privacy policy management into the Group-level compliance management system, conducts internal audits on privacy compliance, and, where necessary, engages independent third parties to conduct external audits.

Chapter VI Supplementary Provisions

Article 14 Any matters not covered in this Policy, or any inconsistency between this Policy and applicable laws, regulations or normative documents, shall be governed by such laws, regulations or normative documents.

Article 15 This Policy is formulated, amended and interpreted by the Company's ESG Working Group and shall take effect from the date of issuance.