Privacy Policy

1. Purpose

Guangdong Dongpeng Holdings Co., Ltd. (hereinafter referred to as "Dongpeng Holdings" or "the Company") aims to safeguard personal information security and the legitimate rights and interests of individuals. In accordance with the *Personal Information Protection Law of the People's Republic of China* and the International Standard ISO 27701, and in combination with business needs, the Company has established a privacy protection system to ensure the confidentiality, integrity, and availability of information assets, and to reduce the risk of privacy breaches both internally and externally. This policy is hereby formulated.

2. Scope

2.1 This policy applies to all employees of the Company, as well as to related entities, manufacturers, clients, suppliers, or third-party personnel involved in business dealings.

2.2 In the event of a conflict between local laws or regional regulations and this policy, this policy shall be the highest standard to follow. However, if local regulations are stricter than this policy, the stricter local regulations shall prevail.

3. Definitions

Dongpeng Holdings: This includes Dongpeng Holdings and its subsidiaries, related enterprises, and any other companies under its direct or indirect substantial control globally.

4. Responsibilities

4.1 The Information Security Committee (comprised of members of the Management Committee) is the highest leadership body for the Company's information and data security, bearing overall responsibility for the Company's information security management. It is responsible for overseeing and approving significant adjustments to the privacy protection policy and supervising the effectiveness of its implementation. The following are the leadership responsibilities for information security:

1. Approving information security policies and regulations to ensure alignment with the organization's strategic direction;
2. Organizing, guiding, and supervising the fulfillment of information security system

responsibilities by all departments, and promptly coordinating solutions to major issues related to information security management.

4.2 The heads of each business unit, platform, center, and first-level functional department are the primary persons responsible for information security within their respective departments, and are in charge of information security management within their departments.

4.3 The Digital Empowerment Platform is the Company's information and data security execution organization, responsible for the overall planning and management of the Company's information security, as well as the formulation and implementation of the privacy policy.

4.4 The Company's Audit Department is responsible for conducting audits.

5. Content of Document Management

5.1 Personal Information Protection Responsibilities

5.1.1 The management should support the information security and personal data protection management system, and actively participate in related activities.

5.1.2 The Company should establish a comprehensive personal data protection system in accordance with the law and the regulations of the competent authorities, ensuring that personal data within the scope of business operations are properly managed to maintain the Company's reputation.

5.1.3 In the event of information security incidents, personal data breaches, or information security vulnerabilities, the Company's employees and outsourced vendors should report them in a timely manner in accordance with the Company's information security incident reporting mechanism and escalation process. The escalation process is clearly defined and communicated to employees, ensuring that any suspicious activities or potential breaches are promptly escalated to the appropriate levels of management and the information security team for immediate action.

5.1.4 The Company's operations related to the collection, processing, and utilization of personal data within the scope of business should prevent personal data from being stolen, tampered with, damaged, lost, leaked, or otherwise unreasonably and illegally used.

5.1.5 The Company prohibits the collection, processing, and utilization of personal data without the consent of the data subject, unless the collection of such personal data is exempt from the requirement of obtaining the data subject's consent under the law.

5.1.6 When undertaking new projects or developing new business processes, privacy protection measures should be considered as one of the core elements in risk assessment to ensure that all activities involving personal data processing comply with current legal requirements.

5.1.7 Regular internal audits of the privacy policy's compliance should be conducted, with specific improvement suggestions proposed and the implementation of corrective measures tracked.

5.1.8 Any relevant units or employees who violate this policy or engage in behavior that endangers the Company's information security or personal data management will be punished or subject to legal action according to the severity of the harm, in accordance with the Company's personnel management regulations. Additionally, information security/cybersecurity performance will be incorporated into the employee performance evaluation system. Violations related to information security/cybersecurity may lead to disciplinary actions as part of the performance assessment process.

5.2 Information Security Objectives

5.2.1 Information security is one of the elements for the Company to fulfill its statutory tasks. The Company needs to maintain an appropriate level of information security to ensure the confidentiality, integrity, and availability of information assets.

5.2.2 The Company regularly tests, assesses, and optimizes information security technology, processes, and control measures to adapt to the ever-changing threat environment. Business continuity/contingency plans and incident response procedures are in place and tested at least 1 times per year to ensure their effectiveness.

5.2.3 Implement data classification and grading management, and ensure the security of sensitive data through technical means such as encryption and access control, preventing it from being tampered with, leaked, or destroyed. All information-related measures must ensure the security of the Company's information and prevent the leakage or loss of important data.

5.2.4 Establish a real-time monitoring mechanism to promptly detect and analyze information security incidents, and develop emergency response plans to minimize the impact.

5.2.5 Appropriately protect information assets (including software, hardware, network communication facilities, and databases), prevent damage to information assets caused by unauthorized access or operational negligence, and develop relevant disaster recovery plans and conduct regular drills.

5.2.6 Regularly conduct information security/cybersecurity awareness training, and all employees must receive information security/cybersecurity training and fulfill their information security responsibilities corresponding to their roles, enhancing their awareness of the importance of privacy protection.

5.2.7 When entering into agreements with suppliers, partners, and other third parties, the Company should include information security clauses to ensure that they meet the Company's security standards.

5.3 Personal Information Management Objectives

5.3.1 The Company should establish a comprehensive personal data protection system in accordance with legal requirements and international standard norms to ensure that all personal data subject to protection are properly safeguarded.

5.3.2 The operations related to the collection, processing, and utilization of personal data within the scope of the Company's business should prevent personal data from being stolen, tampered with, damaged, lost, leaked, or otherwise unreasonably used, to establish a foundation of trust for personal data providers and protect the rights and interests of the data subjects.

5.3.3 The processing of personal information should have clear and reasonable purposes, and should be directly related to the processing purposes, adopting methods that have the least impact on individual rights. The collection of personal information should be limited to the minimum necessary to achieve the processing purposes, and excessive collection of personal information is prohibited.

6. Supplementary Provisions

This policy should be reviewed and assessed annually in accordance with changes in

government regulations, the environment, business operations, and technology. Any amendments must be approved and announced for implementation.