# Weichai Power Co., Ltd.

# Information Security and Privacy Protection Policy

Weichai Power Co., Ltd. (hereinafter referred to as “Weichai Power”, the “Company” or “we”) acknowledges the paramount importance of information security and pledges to safeguard the information security as well as the privacy rights and interests of the Company and its stakeholders. Aligned with internationally recognized industry standards, the Company implements rigorous security measures to ensure the robustness of information security.

## I. Scope of Application

This policy applies to all products and services provided by the Company, as well as functionalities derived from these products and services, including but not limited to websites, client applications, mini-apps, and emerging service models driven by technological advancements.

## II. Governance Framework

The Company continuously refines its information security and data governance framework, establishing a top-down management structure with clearly defined responsibilities for information security and privacy protection. The Confidentiality Committee is responsible for reviewing the Company’s information security management objectives and strategies, as well as evaluating the overall effectiveness and efficiency of the annual information security initiatives. The Chairman of the Board oversees corporate-level data governance and information security. Relevant functional departments are tasked with driving, implementing, and executing specific information security and privacy protection measures.

## III. Information Security Management

The Company prioritizes information asset management by identifying and

categorizing critical information assets (including personal information and sensitive personal information). A multi-layered “cloud-network-end” defense system is implemented to enhance dynamic management and operational oversight of information systems, ensuring confidentiality, integrity, and availability, and preventing unauthorized access, disclosure, loss, or damage.

The Company conducts specialized information security governance and audit programs to minimize vulnerabilities, implementing regular internal and external audits that focus on the daily audits of departing employees and high-risk current employees, management of restricted areas, secure storage and transmission of confidential documents, implementation of confidentiality protocols, employee awareness of confidentiality obligations, and data security audits to ensure compliance with established policies.

The Company develops contingency plans for information security incidents and conducts regular emergency response drills to enhance its capabilities in handling unexpected events, thereby establishing a scientific, effective, and rapid-response mechanism.

The Company leverages multiple communication platforms to educate all employees on the common sense of information security, anti-fraud techniques, and the cultivation of a robust information security culture.

## IV. Information Collection

The Company strictly complies with national laws and regulations to ensure lawful collection and proper protection of information. During collection, the principle of data minimization is upheld, and explicit consent is obtained through prior notification. Collected data shall be securely managed. Specific practices include:

1. Account Registration: During registration, personal information such as name, account ID, password, email, and contact number is required.

2. Contact Information: When individuals engage with the Company (e.g., providing feedback, participating in events, or subscribing to marketing materials), they may voluntarily provide contact details (e.g., name, company, position, email, and phone number).

3. Third-Party and Public Sources: Data may be obtained from public or commercial third parties within legal boundaries, such as purchasing statistical data to support services.

## V. Personal Information Storage and Protection

### 1.Storage

The Company strictly complies with applicable laws, regulations, and supervisory requirements to ensure that all personal information collected and generated within China is stored domestically. Retention periods are rigorously aligned with legal and regulatory mandates. Extensions to retention periods are permitted only for business necessity, legal obligations, or regulatory compliance. Upon expiration of the retention period, personal information is securely disposed of in accordance with legal requirements.

### 2.Protection

(1) Technical Safeguards: In adherence to legal obligations, the Company employs a variety of technical measures, including but not limited to encrypted storage and secure data transmission protocols, to comprehensively protect personal information from unauthorized access, duplication, modification, transfer, destruction, processing, or misuse.

(2) Administrative Controls: To strengthen information security, the Company has established robust management systems and procedures, including the Corporate Information Security Management Regulations, Data Resource Sharing Security Guidelines, Privacy-by-Design Standards, Data Classification and Control Policies, and Data Security Requirements for Application Development. Access to information

is strictly limited under the principle of least privilege, with real-time monitoring of data access and processing activities. All relevant personnel are required to sign confidentiality agreements, ensuring that only authorized individuals have access to sensitive information.

(3) Incident Response: In the event of a personal information breach, the Company shall immediately act to contain the incident and prevent escalation. Affected parties shall be promptly notified through reasonable and effective channels (e.g., phone calls and public notices) to uphold their right to be informed.

## VI. Information Sharing and Transfer

The Company commits not to share or transfer personal information to third parties (e.g., companys, organizations, or individuals) without justification, except in the following cases:

1. With explicit prior consent or authorization.

2. To comply with legal, administrative, or judicial requirements.

3. To protect the legitimate interests, property, or safety of Weichai Power and its affiliates, partners, customers, or the public.

4. When the sharing of personal information is necessary to fulfill core product functionalities or provide the requested services.

5. To address disputes or resolve controversies at the request of customers or other stakeholders.

6. As stipulated in signed agreements (including electronic agreements and platform rules) or as otherwise required by legal documents.

7. For purposes of public interest, such as responding to public health emergencies, in compliance with legal requirements.

## VII. Rights in Personal Information Processing

In accordance with applicable Chinese laws and regulations, individuals retain the following rights regarding their personal information:

**1. Right to Access, Correct, and Update Personal Information**

The right to access, update, and download specific personal information held by the Company;

(1) The right to request corrections if the personal information held by the Company is inaccurate or incomplete.

**2. Right to Delete Personal Information**

Individuals may request the deletion of their personal information under the following circumstances:

(1) If the processing of personal information violates applicable laws or regulations;

(2) If personal information is collected without explicit consent;

(3) If the processing of personal information severely breaches contractual agreements;

(4) If the purpose of processing personal information has been fulfilled, cannot be fulfilled, or is no longer necessary;

(5) If the Company ceases to provide its products or services or if the retention period for personal information has expired.

**3. Right to Withdraw Consent**

Clients or other stakeholders have the right to withdraw their consent or authorization at any time. Once consent or authorization is withdrawn, the Company will no longer provide services corresponding to the withdrawn consent and will cease processing the relevant personal information. However, the withdrawal of consent does not affect the legality of personal information processing activities that were conducted prior to the withdrawal.

## VIII. Policy Update Rules

### 1. Revisions

The Company reserves the right to revise this policy as necessary in response to business development needs or changes in applicable laws and regulations.

### 2. Update Notification

In the event of vital changes to this policy, particularly those that may significantly reduce rights under this policy or expand the scope of data collection or use, the Company will promptly publish the updated version of the policy on its official website for public access.

The Company encourages clients and other stakeholders to regularly review the latest version of this policy to stay informed about our personal information processing practices.

## IX. Supplementary Provisions

Approved by the Board of Directors of Weichai Power, this policy shall take effect upon issuance. Weichai Power shall review this policy at least annually and update it in accordance with evolving national laws and international conventions.