



DATA SECURITY AND PRIVACY PROTECTION POLICY



DATA SECURITY AND PRIVACY PROTECTION POLICY

LONGi Green Energy Technology Co. (hereinafter referred to as "LONGi") attaches great importance to data security and privacy protection, regarding them as one of the core responsibilities of the company's sustainable development. We strictly comply with relevant national laws, regulations and industry standards on data security and personal information protection, and have established a sound security management system for the entire data lifecycle, covering all links such as data collection, storage, processing, transmission, sharing and destruction. We are committed to preventing risks such as data leakage, abuse and tampering, ensuring the integrity, confidentiality and availability of data, and supporting the healthy development of the company's business and social trust with responsible data management practices.

I. Policy Basis

This policy is established in accordance with domestic and foreign laws and regulations such as the *Cybersecurity Law of the People's Republic of China*, *Data Security Law of the People's Republic of China*, *Personal Information Protection Law of the People's Republic of China*, *General Data Protection Regulation* (GDPR), and privacy protection standards *ISO/IEC 27001:2022 Information Security, Cybersecurity and Privacy Protection - Information Security Management Systems - Requirements* and *ISO/IEC 27701:2019 Security Techniques - Extension of ISO/IEC 27001 and ISO/IEC 27002 for Privacy Information Management - Requirements and Guidelines*, combined with the actual operational security needs of our own business systems. It aims to continuously improve the management level of information security and privacy protection of LONGi, ensure the safety, stability and efficiency of daily information security and privacy protection management activities, and enhance the core competitiveness.

II. Scope of Application

This policy applies to all employees of LONGi Green Energy Technology Co. and its branches, including



its subsidiaries and holding subsidiaries. In addition, we encourage suppliers, contractors, and other partners to actively comply with this policy.

LONGi has established an Information Security and Privacy Protection Working Group, composed of the Information Security Management Department, Risk Control Management Department, and relevant business units. The Information Security Management Department coordinates all work related to LONGi's information security domain, while the Risk Control Management Department coordinates privacy protection-related work. They respectively manage LONGi's information security and privacy protection objectives, integrating risk assessment results and management goals into LONGi's overall risk control processes to support comprehensive risk management decisions.

III. Data Security and Privacy Protection Commitments

1. LONGi conducts a comprehensive information security system audit at least once a year. By integrating the analysis results of data security and privacy protection-related security incidents, we comprehensively assesses the improvement priorities for aspects such as the protection capability of the information security system, response efficiency, and privacy protection level. Based on this, we clarifies the improvement tasks for relevant business departments to continuously enhance the information security system.
2. LONGi establishes quality control mechanisms for data entry, storage, transmission and other links to ensure the accuracy, consistency and integrity of data. Regular verification and backup of important data will be carried out to prevent data loss or damage. Additionally, data verification technologies will be adopted to validate whether data has been tampered with during transmission and storage.
3. Within the scope of its information security and privacy protection management system, LONGi identifies and monitors risks arising from the loss of information confidentiality, integrity, availability, and privacy protection compliance through information security and privacy protection risk assessment processes. Based on the conclusions of the risk assessment, we selects appropriate methods for tracking and addressing information security and privacy protection risks.
4. LONGi regularly organizes employees to participate in information security training to enhance their awareness and sense of responsibility for information security and privacy protection, enabling them



to understand the importance of information security, relevant laws and regulations, and the company's policies and systems.

5. LONGi has established a privacy security incident emergency response plan to strengthen privacy protection and safeguard the legitimate rights and interests of privacy subjects in response to information leakage incidents.
6. In contracts signed with third parties, we clearly stipulate the rights and obligations of both parties in terms of information security. This includes data confidentiality, data processing, security incident reporting and handling, etc., to ensure that third parties comply with LONGi's information security policies and relevant laws and regulations during the cooperation process.
7. To ensure compliance with this Information Security and Privacy Policy, LONGi regularly conducts data compliance assessments in accordance with applicable laws and regulations, and invites third-party institutions to carry out security evaluations for the classified protection of filing systems.

IV. Complaint Mechanism

We provide platforms for smooth communication and complaint reporting to ensure the effective implementation of this policy. Through phone calls, emails, mailbox or other channels, employees, suppliers, partners, customers, and other stakeholders can anonymously or openly complain and/or report risk concerns to our compliance department or supervision department. We will investigate and handle reported cases in a fair and objective manner in accordance with laws and regulations, with feedback provided. We also protect whistle-blowers from retaliation in accordance with relevant provisions, ensuring that they are free from threats, intimidation, harassment, or any other forms of unfair treatment due to their reporting. We value feedback from all stakeholders and encourage employees and others to raise questions and provide input regarding the content and application of this policy through the following channels:

- Communication Suggestions: chair@longi.com (Chairman's Mailbox)
- Longi Qingfeng Complaint and Report Acceptance Center WeChat mini program
- Sunshine Longi WeChat official account



- Tel: 0086-029-84193391, 18089282003
- Email: audit@longi.com; compliance@longi.com
- Letters and face-to-face complaints and reports, address: No. 8369, Shangyuan Road,
Economic and Technological Development Zone, Weiyang District, Xi'an City, Audit
Supervision Center of Longi Green Energy Technology Co., Ltd.

Based on updates to relevant laws and regulations, adjustments to company management policies, and industry best practices, we are committed to conducting a comprehensive review of this policy at least once a year. When necessary, we will revise and optimize the policy to ensure its alignment with the latest developments in the provisions and changes in the external environment.

LONGi Green Energy Technology Co., Ltd.

