
# Information and Privacy Security Policy

## I.Policy Statement

Yutong Bus Co., Ltd. (hereinafter referred to as “Yutong Bus” or “Yutong” or “the Company” or “we”) always prioritizes information and privacy security as a cornerstone of robust operations and sustainable development. We are committed to building a solid comprehensive confidentiality and information security framework to safeguard information assets belonging to the Company, employees, customers and partners. This Policy, in conjunction with *Yutong Privacy Statement*, governs and guides our information and privacy protection practices.

## II. Scope of Application

This Policy applies to Yutong Bus and its subsidiaries, and extends to suppliers and other relevant business partners.

## III. Basic Principles

### Information and Privacy Security Management

1.1 We strictly comply with the *Cybersecurity Law, Data Security Law, Personal Information Protection Law, and Network Data Security Management Regulations of the People’s Republic of China*, alongside the laws and regulations of the countries and regions where we operate, such as the *European Union’s NIS2 Directive* and *Cyber Resilience Act*. We are fully committed to fulfilling our confidentiality and information security obligations. Aligned with the ISO 27001 standards and national cybersecurity classified protection requirements, we continuously optimize our information security and privacy protection management system. We establish business continuity plans to solidify the foundation of our secure operations.

1.2 In accordance with national confidentiality and information security requirements and actual corporate management needs, we have established a professional governance structure integrating personnel, technical, and procedural safeguards, clearly defining confidentiality responsibilities and accountability across all units.

1.3 The Intelligent Connected Electrical Department, Enterprise Informatization Management Department, Legal Affairs Department and various Business Departments jointly build the Company’s information and privacy protection framework. The Intelligent and Connected Electrical Department leads the implementation, evaluation, system operation and maintenance and data privacy management of security technology in telematics business. The Enterprise Information Management Department focuses on internal system protection and IT infrastructure guarantee. The Legal Affairs Department is responsible for compliance interpretation, legal documentation and dispute handling. Simultaneously, all business units implement full lifecycle management of personal information, ensuring compliance across collection,

classification, and storage. These units are accountable for the business necessity of data collected, defining clear retention periods and protection requirements to collaboratively safeguard data security.

1.4 Closed-Loop Audit Management: We have established a closed-loop audit system where dedicated personnel monitor alert logs for violations or anomalies. Audit reports are generated to ensure the timely mitigation of risky operations and security events. Furthermore, we issue monthly system-level and bi-monthly company-level security briefings to reinforce confidentiality and information security requirements and continuously enhance employee awareness of information security and data privacy responsibilities. We maintain a “zero-tolerance” policy toward any employee behavior involving the leakage of private information or the compromise of network security.

1.5 Internal Whistleblowing Mechanism: We operate an internal reporting system allowing employees to report security incidents, vulnerabilities, or suspicious content through channels such as departmental Information Security Administrators. All reports are reviewed and resolved by a dedicated department.

**2. Information and Privacy Security Protection Requirements**

2.1 Ensuring Data Integrity and Security: The Company strengthens security throughout the full data lifecycle, actively implementing control measures to prevent data breaches and privacy leaks.

1) Data Collection: Prior to collection, we clearly define the purpose, method, scope, usage, rights, and obligations with data subjects through documents such as personal information protection policies, privacy statements, and data subject consent forms. User data is collected only after obtaining the subject’s explicit consent. Data collection adheres to the principle of “minimum necessity,” gathering only information essential for business operations and strictly avoiding excessive collection.

2) Data Transmission: We employ appropriate encryption measures to secure transmission channels, nodes, and data, ensuring both confidentiality and integrity. For regions/countries with strict data protection standards (e.g., the EU), we conduct Transfer Impact Assessments (TIAs) and adopt technical, organizational, and contractual measures (such as Standard Contractual Clauses or SCCs) to ensure a level of data protection equivalent to local requirements. Additionally, for data transmission—especially cross-border transfers—we implement the above measures and obtain separate, explicit consent from data subjects.

3) Data Storage: Based on specific business scenarios, we define minimum and maximum retention periods for information. At the same time, We ensure storage security by using encryption and strict access controls for existing data, while clearly defining retention periods for new data.

4) Data Processing: In compliance with relevant laws, we adopt the “principle of least privilege.” Personnel can access only the minimum personal information necessary for their duties and possess the minimum data operation authority required.

5) Data Transfer, Sharing, and Disclosure: In principle, personal information shall not be shared or transferred. When strictly necessary for business, we prioritize risk management and conduct a prior Personal Information Protection Impact Assessment (PIA). For high-risk scenarios involving large-scale processing or automated decision-making, we further conduct a Data Protection Impact Assessment (DPIA) and implement effective measures to protect data subjects based on the results.

2.2 Monitoring and Responding to Security Threats: We actively monitor cybersecurity risks, establish emergency response protocols, conduct vulnerability analyses, and implement mitigation strategies to promptly address data and privacy leakage risks. We have formulated the *Vehicle Cybersecurity Report Filing Management Procedure* to standardize reporting management, clarify personnel responsibilities and processes, and strengthen our risk prevention and reporting mechanisms.

1) At the endpoint level, we deploy Data Loss Prevention (DLP) systems to prevent malware, patch vulnerabilities, and control data egress. At the network level, we utilize a defense-in-depth architecture to implement security domain controls, preventing attacks and intrusions while strengthening boundary defense.

2) We regularly test our emergency mechanisms and incident response procedures to validate their effectiveness.

2.3 Customer Data Rights: When using Yutong products or services, customers retain the right to access, correct, delete, and withdraw consent for their personal information, empowering them to effectively manage their data. For further details, please refer to the *Yutong Privacy Statement*.

**3. Information and Privacy Security Protection Training**

We continuously enhance employee awareness and capabilities regarding information security. This includes annual security awareness training for all staff and regular specialized skill training for key roles. We also conduct assessments to ensure training effectiveness.

**IV. Supplementary Provisions**

This Policy is reviewed and approved by the Company’s Strategy and Sustainability Committee. The Company will periodically review and update this Policy as necessary.