Zyxel Group Corp.
Privacy Policy

Version 1.0, January 2026

Zyxel Group Corp. (hereinafter referred to as "Zyxel Group" or "the Company") attaches great importance to the protection of personal data and is committed to safeguarding the privacy and statutory rights of data subjects. To ensure proper personal data protection and management, this Corporate Privacy Policy has been established in accordance with Taiwan's Personal Data Protection Act, the European Union's General Data Protection Regulation (GDPR), and other applicable privacy laws and regulations in the jurisdictions where we operate. This Policy serves as the highest guiding principle for personal data protection within the Company's corporate governance and legal compliance framework.

The Company maintains a comprehensive governance structure, internal management systems, and information security measures to mitigate risks such as unauthorized access, leakage, loss, or improper use of personal data. We ensure that the collection, processing, and use of personal data comply with applicable laws and regulations as well as this policy.

Scope of Application

- This Policy applies to the personal data processing activities of the Company, its subsidiaries, and joint ventures over which it exercises significant influence in the course of their business activities.
- It applies to individuals who interact with the Company, including but not limited to website visitors, users of products or services, employees of corporate customers and contractors, job applicants, visitors, investors, contractual counterparties, and other legally relevant stakeholders (collectively referred to as "You").
- The Policy covers personal data from online and offline sources, including website, and non-website channels.

Definition of Personal Data and Processing Roles

"Personal Data" refers to information relating to an identified or identifiable natural person.

Depending on the specific business scenarios, the Company acts as a "Data Controller", or for certain products or services, as a "Data Processor" as agreed upon by contract.

The Company processes your Personal Data only when one of the following legal bases applies:

- Necessity for the performance of a contract.
- Necessity for compliance with a legal obligation.
- Necessity for the legitimate interests of the Company or a third party, provided that such interests do not override your fundamental rights and freedoms.
- Your explicit consent for a specific purpose.

Purposes of Data Collection, Processing, and Use

The Company processes Personal Data for the following purposes:

1. Inquiries and Contact: Processing contact information provided via email or other communication channels to respond to inquiries (Legal basis: Contract performance or Consent).
2. Website Usage: Processing technical data (such as IP address, location, browser type, etc.) to ensure website operation, maintain security, and improve user experience (Legal basis: Consent or Legitimate interest).
3. Service Provision and Account Management: Processing names, email addresses, and authentication credentials to provide services and maintain system security (Legal basis: Contract performance or Legitimate interest).
4. Product Registration and License Management: Processing registration information and device identifiers to fulfill purchase contracts and provide services.
5. Subscriptions, Marketing, and Customer Service: Sending marketing information with your consent (which may be withdrawn at any time) and conducting anonymized analysis for service improvement.
6. Offline Business Data: Processing contract and supplier-related information to

manage business relationships and fulfill contractual obligations.

Cookies and Similar Technologies

The Company's website uses cookies and other tracking technologies ("Cookies") to provide personalized content and improve the browsing experience and services. Where required by applicable law, the Company will obtain your prior consent before using Cookies. You may manage or withdraw your consent at any time through your browser settings or via the Cookies preference panel available on the Company's website.

Cookies may technically process certain data in real time, including IP addresses, browsing duration, and browser information. The Company does not permanently store IP addresses as personally identifiable data, nor does it use such data for purposes other than those described above. You may manage or disable Cookies through your browser settings; however, please note that disabling Cookies may limit certain website functions or features.

Disclosure and Third-Party Sharing

The Company does not disclose your Personal Data to unrelated third parties except where permitted or required by applicable law, necessary for contract performance, based on legitimate interest, or with your consent. Such disclosures may include, but are not limited to:

- Authorized government, regulatory, or judicial authorities.
- Parent companies, subsidiaries, or affiliated entities.
- Suppliers, service providers, or data processors acting under confidentiality agreements.
- Business partners with your explicit consent.
- Professional consultants with a legal duty of confidentiality.
- Relevant entities as necessary to protect the rights and interests of the Company or its users.

Except where required by law or necessary for the performance of a contract, you may choose to refuse or withdraw your consent to the provision of Personal Data to specific third parties. For circumstances involving data use or disclosure that require your explicit consent by applicable laws, the Company will not proceed without first obtaining such consent.

Personal Data Retention Period

The Company retains Personal Data only for the period necessary to fulfill specific and lawful purposes of collection. Retention periods are determined based on applicable legal requirements, contract obligations, and reasonable periods necessary for asserting legal claims. Once the purpose for retention no longer exists, or when the applicable retention period expires and deletion is required by law, the Company will delete, anonymize, or cease the use of such data, or otherwise retain or dispose of it in accordance with customer instructions.

Cross-Border Transfer of Personal Data

Due to the Company's global operational needs, your Personal Data may be transferred to and processed by the Company's affiliates or service providers located in different countries. The Company ensures that such cross-border transfers comply with applicable data protection laws. Where Personal Data originating from the European Economic Area (EEA) is transferred to a third country that has not been recognized by the European Union as providing an adequate level of data protection, the Company will prioritize the use of Standard Contractual Clauses (SCCs) approved by the European Commission or implement other appropriate supplementary measures to ensure a level of protection essentially equivalent to that required under the GDPR.

Automated Decision-Making and Profiling

As a general principle, the Company does not engage in solely automated decision-making, including profiling, that produces legal effects concerning you or similarly significantly affects you. If such processing is necessary for specific services or recruitment processes, the Company will obtain your explicit consent in advance

and provide you with the right to request human intervention, express your views, and contest the decision, in accordance with applicable laws.

Personal Data Rights

In accordance with applicable data protection laws, you may exercise the following rights:

- The right to refuse to provide your Personal Data; however, this may affect the availability or functionality of certain website features or services provided by the Company.
- The right to inquire about or request access to your Personal Data.
- The right to request a copy of your Personal Data.
- The right to request supplementation or correction of your Personal Data.
- The right to request the deletion of Personal Data, where there are legitimate grounds to do so.
- The right to request restriction of, or to object to, the processing of your Personal Data.
- The right to data portability, to request that your Personal Data be transferred to another data controller in a structured, commonly used, and machine-readable format, where technically feasible.
- The right to lodge a complaint with a competent data protection authority.
- The right to withdraw your consent at any time where the Company processes your personal data based on your consent. Please note that the withdrawal of consent does not affect the lawfulness of the processing carried out prior to such withdrawal.

Children's Privacy

The Company does not target children as the intended audience for its products or services, nor does it knowingly collect Personal Data from children. If the Company becomes aware that such information has been collected inadvertently, it will be

deleted promptly.

Information Security and Personal Data Protection Measures

The Company has established a multi-layered information security and personal data protection management system and has implemented the following measures:

1. Technical Measures: Data encryption, anonymization and/or pseudonymization, firewalls, intrusion detection systems, vulnerability scanning, system redundancy, and regular data backups.

2. Administrative Measures: Access control and internal permission hierarchy management, application of the principle of least privilege, and regular information security and privacy risk assessments.

3. Incident Response and Auditing: Establishment of notification and response procedures for information security and personal data incidents; where required, notifying competent authorities and affected data subjects in accordance with the law, and conducting regular internal or third-party audits.

The Company also follows internationally recognized information security management standards (such as ISO/IEC 27001) to continuously strengthen its management system.

Internal Governance, Risk, and Compliance

The Company has formally integrated personal data and privacy protection into its Enterprise Risk Management (ERM) and legal compliance management frameworks, recognizing them as critical risk areas in corporate operations and governance. Risks related to privacy and data protection are identified, assessed, controlled, and continuously improved through existing risk management processes, with regular management reporting to the Board of Directors.

To ensure the effective implementation of this Privacy Policy, the Company has established and enforced the "Personal Data Protection Management Regulations." These regulations clearly define operational procedures for the collection, processing, use, retention, deletion, incident notification, access and permission management, as well as outsourced services and third-party management. Execution responsibilities are allocated among organizational units according to their respective business functions. Compliance with these regulations is incorporated into

the Company's Internal Control System (ICS) and annual audit plans. Through regular inspections and follow-up improvement mechanisms, the Company continuously reviews the effectiveness of its management system and its legal compliance status.

Education and Training

The Company conducts regular (annual) education and training programs for employees on privacy and personal data protection to enhance awareness and ensure compliance across all levels of the organization.

Whistleblowing and Reporting Mechanism

If any circumstances arise that may affect the security of Personal Data or constitute a violation of this Privacy Policy, any individual with relevant information may submit a complaint, inquiry, or report by email at ethic@zyxelgroup.com. Matters specifically related to employee data may also be reported to employeeprivacy@zyxelgroup.com. The Company will maintain the confidentiality of the whistleblower's identity and the content of the report. Anonymous reports are accepted to ensure that the whistleblower does not suffer any undue influence as a result of making a good-faith report.

Sanctions for Violations

The Company adopts a zero-tolerance approach toward any behavior that violates this Policy or applicable personal data protection laws. Where an investigation confirms a violation, the Company will take appropriate measures based on the nature and severity of the violation, including but not limited to warnings, re-education and training, disciplinary action, suspension, termination of employment, or the pursuit of legal liability in accordance with applicable laws.

Data Protection Representative and Management Responsibility

The Company has designated a dedicated unit responsible for personal data and privacy management. This unit serves as the contact window for data protection authorities and data subjects and is responsible for coordinating policy implementation, legal compliance, complaint handling, and external

communications. Where the Company's business activities in the European Union trigger the requirement to appoint a representative under the GDPR, an EU-based representative will be appointed in accordance with applicable laws to assist with relevant data protection matters. In addition, **the Company's internal audit unit periodically conducts audits under the Internal Control System (ICS), based on the annual audit plan, to review the collection, processing, and transfer of Personal Data. These audits assess the effectiveness of management mechanisms and ensure compliance with applicable laws, regulations, and internal codes of conduct.**

Policy Changes

The Company may update this Policy from time to time in response to changes in laws and regulations or operational requirements. The most recent version will be published on the Company's official website and will take effect upon publication.

This Policy, and any subsequent amendments, shall be implemented upon approval by the Board of Directors.

Chief Operating Officer, Zyxel Group Corp.