

Zyxel Group Corporation

Responsible Artificial Intelligence Program

Last Updated: September 2026

Zyxel Group Corporation (hereinafter referred to as "the Company") is committed to the responsible and ethical application of artificial intelligence (AI) technologies, continuously strengthening its AI governance capabilities to balance technological innovation, information security, personal privacy, regulatory compliance, and social responsibility. Drawing upon international standards, including ISO/IEC 42001 and the NIST AI Risk Management Framework (AI RMF), the Company has established an AI governance framework founded on five core principles: Safety & Security, Transparency, Fairness, Accountability, and Human Oversight.

1. Risk-Tiered Governance and High-Risk Application Controls

In accordance with the *Responsible Artificial Intelligence Policy*, the Company has instituted an AI risk management mechanism that assesses and categorizes risks based on application scenarios and data sensitivity. High-risk applications involving facial recognition, biometric identification, or personal data analytics must undergo comprehensive information security, privacy, and regulatory compliance assessments, and require formal managerial approval prior to implementation. These requirements are fully integrated into the Company's AI risk-tiering and application review protocols.

In 2025, a dedicated technical and privacy risk assessment was completed for the facial recognition access control system deployed at MitraStar Wuxi; the project received full approval and has been officially launched into production.

2. Safeguarding Transparency, Model Stability, and Fairness

The Company requires AI-generated or AI-assisted content to be appropriately labeled in formal documentation, critical analytical reports, and public disclosures, while mandating human review processes to ensure data accuracy and sound decision-making. For in-house developed and high-risk AI deployments, periodic review mechanisms have been established to monitor performance, output quality, and operational risks, thereby mitigating model drift and performance degradation. Furthermore, potential biases and fairness risks are evaluated prior to initial deployment and whenever significant modifications occur, ensuring that AI technologies operate in an equitable, impartial, and responsible manner.

In 2025, quarterly audit mechanisms were implemented to monitor inference accuracy and output stability, preventing performance degradation and model drift. In addition, all high-risk applications launched in 2025 were subjected to a pre-launch fairness checklist review to verify dataset representativeness and neutrality, ensuring algorithms adhere to the principles of equity and fairness.

3. Generative AI Guidelines, Environmental Sustainability, and Grievance Channels

In 2026, the Company officially enacted internal guidelines governing the use of Generative AI, enforcing controls across sensitive data protection, intellectual property

compliance, and network-level blocking of unauthorized tools to prevent trade secret leakages. Regarding environmental sustainability, the Company prioritizes public cloud infrastructures with certified energy efficiency and implements dynamic computing resource allocation. In 2025, an audit and reclamation of dormant accounts and redundant computing nodes was completed, effectively reducing energy consumption and the ecological footprint of our computing environments.

For employees and stakeholders impacted by AI-driven decisions, the Company has designated the existing Information Security and Personal Data Protection grievance channels as the intake point. Dedicated personnel initiate formal human review investigations to ensure all objections receive independent oversight and actionable responses.

4. Organizational Culture, Empowerment, and Benefit Quantification

The Company cultivates a culture of responsible AI use via its internal learning platforms. In 2025, organization-wide training for the "Get started with Office 365" productivity suite was completed, alongside the curriculum design for 2026 AI programs. These courses cover AI operational risks, cybersecurity, data protection, responsible AI principles, and governance/compliance mandates, elevating employee awareness regarding AI applications and risk management.