

# Information and Cyber Security Policy

The FarEasTone Telecommunications Co., Ltd. and New Century InfoComm Tech Co., Ltd. (collectively “the Company”) has formulated the following Information and Cyber Security Policy (“the Policy”) to fully demonstrate the emphasis on and the importance of information security and personal data protection. The Company also establishes a comprehensive management organization structure, facilitates to build up an effective information security management system, and promotes it through education and trainings to enhance company-wide awareness and create an internal security culture.

The Policy applies to all employees. Every employee bears the responsibilities for information security and personal information management, must have clear understanding and comply with, and is required to report suspicious behavior or potential risks; moreover, suppliers and partners are required to comply to the Company’s security requirements, so that to ensure the confidentiality, integrity, availability and compliance in business operations, and the solid implementation of the security policies:

- Construct Secured and Reliable Networks
- Ensure Business Continuity and Resilience
- Comply with the Requirements of Competent Authorities and Laws
- Safeguard the Security of User’s Privacy Information

Through the above Policy, the Company aims to achieve the vision of information security and personal data protection - “Treasure customer entrusted; Respect for customer information; Win the trust of customers; Provide sustainable services”, while maintaining regular verification by independent third parties and continuously improve the information security system by regularly review and update security strategies and technologies, establish effective monitoring mechanisms, implement encryption, backup and other technical means to ensure data integrity and security, prevent data loss, tampering or unauthorized access, and to quickly discover potential security

risks. When potential threats or information security incidents are detected, it is required to report and response promptly, and explain countermeasures and follow-up preventive actions to affected stakeholders to deal with the evolving threats.

To ensure the continued appropriateness and effectiveness of this Policy, the Company may implement any appropriate updates and modifications in response to factors such as technology development trends, amendments to relevant laws or regulations or other environmental changes in order to carry out the intention of protecting information and cyber security. The amendment or modification of the Policy made will be approved by the President and published on the Company's website.