Information Security and Privacy Protection Policy

BNBM strictly complies with all laws and regulations concerning information security and privacy protection in the jurisdictions where it operates. This policy aims to clarify the Company's responsibilities and obligations in information security and privacy protection, ensuring that while pursuing business development, the Company fully prioritizes and safeguards information security and customer privacy.

This policy applies to all employees of the Company and all affiliated companies, including full-time, part-time, and outsourced employees. The Company encourages suppliers to jointly adhere to the requirements set forth in this policy.

(The English translation of the Policy is for reference only and the Chinese version shall prevail in case of any inconsistency between the Chinese version and English translation thereof)

1 INFORMATION SECURITY MANAGEMENT REQUIREMENTS

1.1 All data collection, storage, processing, and transmission must comply with laws, regulations, and internal company standards to prevent data leakage, tampering, or destruction.

1.2 Continuously invest in the latest information security technologies, equipment, and solutions, such as firewalls, intrusion detection systems, data encryption technologies, and security audit systems, to strengthen the security protection of networks and information systems and guard against security risks such as hacker attacks and virus intrusions.

1.3 Regularly evaluate the effectiveness of investments in information security protection and make adjustments and optimizations as needed.

1.4 Clearly define the permissions of IT operation and maintenance personnel, and promptly revoke relevant permissions upon completion of operation and maintenance tasks.

1.5 Timely update the software and hardware facilities of information systems, upgrade protective measures, and regularly engage third parties to conduct external audits of the information security management system to ensure its effectiveness.

1.6 Continuously monitor the Company's information and network security status, regularly scan for vulnerabilities, and take measures to promptly repair and remediate any identified information security vulnerabilities and risks.

1.7 Develop information security contingency plans and regularly test information security emergency mechanisms and incident response procedures.

1.8 For suppliers, thoroughly review the security of their information and network systems to ensure the integrity and confidentiality of company information is not compromised due to supplier-related reasons.

2 PRIVACY PROTECTION MANAGEMENT REQUIREMENTS

2.1 Implement systematic and process-oriented management of information systems, establish access permissions for customer information, and strictly adhere to the principle of customer information confidentiality.

2.2 Sign confidentiality agreements with personnel and third-party companies involved in handling customer information, and monitor the implementation of these agreements to ensure the security of the Company and customer information.

2.3 Regarding the acquisition and recording of customer information, the Company shall only record basic customer information and periodically clean up important sensitive information.

2.4 Concerning information access, strive to ensure the data security of internal systems, implement account login permission management, and restrict internal personnel's access scenarios and usage conditions for customer information to maximize the protection of customer information security.

3 EMPLOYEE PARTICIPATION

3.1 Define the information security responsibilities of each employee, such as complying with information security operating procedures and consciously protecting company data and customer information.

3.2 Continuously promote information security-related training and awareness activities to enhance employees' awareness of information security.

3.3 When potential information security threats are discovered, they should be reported in accordance with the security risk reporting procedures.

3.4 For specific positions (including but not limited to information security positions), the Company incorporates information security and privacy protection as part of employee performance evaluations.

4 DISCIPLINARY ACTIONS

4.1 The Company implements a zero-tolerance policy towards any leakage of user privacy information and will take disciplinary measures against violations of this policy, including but not limited to warning, fine, and termination.