Information Security and Privacy Protection Policy

443.6 Fg0 Q EMC /Span <</MCID 3 /Lang (en-US)>>BDC q 780 0873 0 59.44 841.9 re W* n BT /F2 12.48 Tf1 0 0 1 57.344 69.2

BNBM strictly complies with all laws and regulations concerning information security and privacy protection in the jurisdictions where it operates. This policy aims

rity and privacy protection clarify 252(y)-57(t) 12 Tf1 0(j)-48(a)-57(r)-51(i)-57 CC (i)-48(t)-55(s)-57(M)-57(r) MCID 7 (en-US) BDC

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.