Grandblue Environment Co., Ltd.
Cybersecurity Policy

I. Purpose

To standardize cybersecurity management, protect information systems and data, prevent risks such as cyber threats, data breaches, and system vulnerabilities, and safeguard the Company's operational stability and long-term value, Grandblue Environment Co., Ltd. (the "Company") has formulated this Policy in accordance with applicable national laws and regulations and the Company's internal management policies and procedures.

II. Application Scope

This Policy applies to the Company and its wholly owned and controlled subsidiaries, as well as all Company employees and third parties involved in the Company's business activities, such as suppliers.

III. Basic Principles

1. The Company follows the principles of "unified leadership, coordinated planning, strengthened management, efficient operation, and prevention first," and implements tiered management, with responsibilities assigned to specific individuals in accordance with the principle that "those in charge are responsible, those who operate are responsible, and those who use are responsible."

2. Prevention First - The Company places primary emphasis on security protection and maintains a high level of vigilance, with a focus on safeguarding fundamental information networks and critical information systems. Through prevention, monitoring, emergency response, emergency support, and financial investment, the Company adopts multiple measures to establish a comprehensive information and network security protection system.

3. Rapid Response - In the event of a cybersecurity or information security incident, the Company follows its rapid-response mechanism to promptly obtain sufficient and accurate information, implement response measures in an orderly manner, and minimize the impact and resulting losses to the greatest extent possible.

4. Tiered Accountability - The Company and its subordinate entities assume responsibilities at their respective levels, strengthen coordination and

collaboration, assign cybersecurity responsibilities to specific individuals, and jointly fulfill their cybersecurity management duties.

IV. Policy Requirements

1. The Company has formulated and implemented the *Cybersecurity Management Regulations*, established an information security management system covering strategy, management, operations, technology, personnel, and other key elements, and put in place a cybersecurity accountability system.

2. The Company explicitly requires all subordinate entities to determine the security classification of their information systems in accordance with applicable national cybersecurity classification requirements and standards, implement cybersecurity classified protection requirements, and carry out security development, security management, and boundary protection in line with the latest classified protection requirements. The Company conducts management reviews annually to ensure the continued suitability, adequacy, and effectiveness of its information security management system and to continuously improve its information security protection capabilities.

3. The Company requires all subordinate entities to strengthen cybersecurity emergency management, establish and improve cybersecurity risk assessment and emergency response mechanisms, formulate emergency response plans for cybersecurity incidents, designate responsible leaders and personnel for cybersecurity emergency response, conduct drills on a regular basis, and further revise and improve relevant plans based on the results of these drills.

4. The Company has formulated and implemented the *Data Security Management Measures* and the *Data Backup and Recovery Specifications*. The Company implements security management throughout the entire data lifecycle through measures including data classification and grading, access control, encryption, secure transmission, backup and recovery, and regularly conducts data security audits to ensure data confidentiality, integrity, and availability.

5. The Company has formulated and implemented the *Third-Party Cybersecurity Management Measures* to identify and manage information security risks associated with services provided by third parties, clearly define the information security requirements that third parties must comply with in the course of their cooperation with the Company, prevent the loss of information assets, and protect shared infrastructure and data.

V. Implementation and Safeguard Mechanisms

1. The Company has established a Cybersecurity Leading Group, which assumes primary responsibility for cybersecurity and is responsible for providing guidance,

supervision, inspection, and assessment of cybersecurity activities. An office has been established under the Cybersecurity Leading Group to supervise and implement relevant day-to-day management activities.

2. The Company regularly conducts cybersecurity education, awareness programs, and training to enhance the information security awareness and personal accountability of all employees.

3. Where an entity refuses to fulfill its cybersecurity protection obligations, resulting in significant cybersecurity risks or a cybersecurity incident, the Company will hold the relevant entity and responsible personnel strictly accountable and impose disciplinary measures in accordance with applicable rules. Where such conduct constitutes a criminal offense, criminal liability will be pursued in accordance with the law.

In the event of any discrepancy in meaning or interpretation between the English and Chinese versions of this document, the Chinese version shall prevail.