1. Purpose

Diamond Biofund Inc. (In the following referred to as “the Company”) establishes this policy to ensure the confidentiality, integrity, and availability of its information assets, in compliance with the Cybersecurity Management Act and its sub-laws, as well as other relevant laws and regulations. The policy aims to protect the Company’s information assets from internal and external, intentional or accidental threats.

2. Scope of Application

(1) This policy applies to all Company employees, outsourced service providers, data users (including custodians), and visitors.

(2) The scope of cybersecurity management covers areas related to ISMS. It aims to prevent risks caused by human error, malicious intent, or natural disasters that may lead to misuse, leakage, alteration, or destruction of data, potentially resulting in various risks to the Company.

3. Objectives

To safeguard the confidentiality, integrity, and availability of the Company’s information assets, the implementation of this policy seeks to achieve the following objectives:

(1) Establish a secure and reliable information operation environment, ensuring the security of the Company’s data, systems, equipment, and networks, thereby protecting business continuity.

(2) Protect the security of the Company’s business services by ensuring that only authorized personnel can access information, thereby maintaining confidentiality.

(3) Protect the security of the Company’s business services by preventing unauthorized modification, thereby maintaining accuracy and integrity.

(4) Establish a business continuity plan to ensure the ongoing operation of the Company's information-related services.

(5) Ensure that the Company's operations comply with relevant government laws and regulations (e.g., Criminal Code, Classified National Security Information Protection Act, Patent Act, Trademark Act, Copyright Act, Personal Data Protection Act, and Guidelines for Cybersecurity Controls for TWSE-Listed and TPEx-Listed Companies).

(6) Safeguard personal data related to the Company's business from risks such as theft, alteration, damage, loss, or leakage caused by external threats or improper internal management and use.

(7) Enhance protection and management capabilities of information assets to reduce operational risks.

4. Responsibilities

(1) The Company shall establish a cybersecurity organization to coordinate and promote cybersecurity matters.

(2) Management shall actively participate in and support the cybersecurity management system and implement this policy through appropriate standards and procedures.

(3) All Company employees, outsourced service providers, data users (including custodians), and visitors shall comply with this policy.

(4) All Company employees, outsourced service providers, and data users (including custodians) are responsible for reporting cybersecurity incidents or vulnerabilities through appropriate reporting mechanisms.

(5) Any act that endangers cybersecurity will be subject to civil or criminal liability depending on the severity of the case, or disciplinary action in accordance with the Company's relevant regulations.

5. Management Indicators

(1) To assess the achievement of cybersecurity management objectives, the Company shall establish relevant management indicators and conduct regular monitoring, evaluation, and improvement.

(2) The Company shall periodically review the duties and responsibilities of its cybersecurity organization to ensure effective implementation of cybersecurity work.

(3) The Company shall comply with regulatory requirements and provide appropriate cybersecurity training based on employees' duties and responsibilities.

(4) The Company shall strengthen the environmental security of its information assets by adopting appropriate protection and access control mechanisms.

(5) The Company shall ensure that information is not disclosed to unauthorized third parties.

(6) The Company shall enhance access control to prevent unauthorized access, thereby ensuring proper protection of its information assets.

(7) Security requirements shall be considered in the development of Company information systems, and regular audits of security vulnerabilities shall be conducted.

(8) All cybersecurity incidents or suspected vulnerabilities shall be reported through appropriate mechanisms and properly investigated and addressed.

6. Management Review

This policy shall undergo management review at least once per year to reflect the latest developments in government regulations, technology, and business operations, ensuring the Company's ability to maintain business continuity. Feedback on cybersecurity matters from the cybersecurity organization, regulatory

authorities (or required by laws and regulations), or stakeholders such as experts shall be included in the management review discussion agenda.

7. Statement

Information is a valuable asset to the Company. Business continuity depends on the integrity and ongoing availability of information. Adhering to cybersecurity standards protects information from unauthorized use, modification, disclosure, or destruction, whether accidental or deliberate.

The Company hereby declares its cybersecurity policy principle, designed to be simple, easy to remember, and aligned with cybersecurity management objectives:

“Strengthen security protection, safeguard information security.”

8. Implementation

This policy shall be implemented upon approval by the Chairman of the Board and shall apply equally to all subsequent revisions