Information Security Policy of Radium Life Tech Co., Ltd.

I. Purpose:

In order to strengthen information security management, to ensure the confidentiality, integrity and availability of our information assets, to provide an information environment in which this Company's business can continue to operate, to meet the requirements of relevant government regulations and internal and external stakeholders, to achieve information security and to protect it from any intentional or accidental threats, both internal and external, Radium Life Tech Co. (hereinafter referred to as this Company) hereby establishes this Information Security Policy.

II. Scope:

This Company's Information Security Management System is used for the maintenance of information rooms, the maintenance of business operations systems and security management.

III. Definition:

1. Information Assets: refers to the hardware, software, services, documents and people that are required to keep this Company's information business running properly.
2. Confidentiality: The Company shall ensure that only authorized users have access to information.
3. Integrity: The Company shall ensure that information systems are maintained and processed in a manner that is free from change and tampering.
4. Availability: The Company shall ensure that information and related assets are available to authorized users as and when required.

IV. Goal:

The objectives are to maintain the confidentiality, integrity and availability of this Company's information assets and to protect the privacy of user data. All staff must work together to achieve the following objectives:

The Company shall ensure legal access to data, the integrity of information systems and uninterrupted operations. In the event of an emergency, the Company shall take prompt and necessary action to restore normal operations within the shortest possible time in order to minimize the damage that may result from such an incident.

V. Management Plan:

1. This Company's internal audit unit and external accountants conduct annual information and communication security checks to review information security policies, information security organization, personnel security and management, asset classification and control measures, physical and

environmental security management, communications and operations management, and other matters related to information security risks, and report to the Board of Directors on a regular basis.

2. In order to reduce the risk of disruption to business operations due to the suspension of information systems and to regularly assess the impact of man-made operations and natural disasters on information assets, a disaster recovery plan has been developed and is regularly rehearsed to ensure the continued operation of the Company's business.
3. The Company has established access control and monitoring systems to prevent equipment theft and vandalism.
4. The digital age has led to challenges in information security. We will continue to pay attention to the changing trends in the information environment, regularly review our information security mechanisms and solutions, and build information security systems that include firewalls, anti-virus software, and email protection measures.
5. In line with our information security policy, we regularly promote information security-related knowledge to raise the awareness of information security among all staff.