

A Plus Biotechnology Co., Ltd.

Information Security Maintenance Plan

Table of Contents	Page no.
I. Basis and Objective	2
II. Applicable Scope	2
III. Significance of Core Business and Description of Non-core Business	2
IV. Information Security Policy and Objectives	4
V. Information Security Promotion Organization	5
VI. Dedicated Personnel and Budget Allocation	6
VII. Inventory of Information and Information Systems	7
VIII. Information Security Risk Assessment	7
IX. Information Security Protection and Control Measures	7
X. Information Security Incident Reporting, Response, and Exercise Mechanisms	12
XI. Assessment and Response to Information Security Intelligence	12
XII. Management of Outsourcing of Information Systems or Services	14
XIII. Information Security Education and Training	15
XIV. Assessment Mechanism for Information Security Matters Involving Company Employees	16
XV. Continuous Improvement and Performance Management Mechanisms for the Information Security Maintenance Plan and its Implementation	16
XVI. Implementation	18

A Plus Biotechnology Co., Ltd.

Information Security Maintenance Plan

I. Basis and Objective

This plan was formulated in accordance with the “Cybersecurity Control Guidelines for TWSE/TPEx-Listed Companies” and the Company's “Information Security Policy”.

II. Applicable Scope

The scope of management of this procedure includes four parts: personnel, application systems, hardware equipment, and network facilities.

1. Personnel

This policy shall apply to all employees, contractors, consultants, temporary employees, customers, and third-party personnel involved in the Company's information operations or data usage.

2. Application Systems

Software, procedures, services, and systems for information operations or data usage.

3. Hardware Equipment

Various types of mainframes, workstations, servers, and personal computers.

4. Network Facilities

The local area network in the Company office, and dedicated data lines and related network facilities connecting the office with the computer room and the internet.

III. Significance of Core Business and Description of Non-core Business

1. Core Business and Importance

The Company's core business and importance are shown in the table below:

Core Business	Description of the Impact of Business Failure	Maximum Tolerable Downtime
Mail Server	Inability to deliver mail and communicate in real time	12 hours
ERP System	Impact on the Company's operations	12 hours
Server Host	1. Unable to grasp the operating status 2. Lack of records of operating activities	12 hours

Note: Definitions of each field.

(I) Core business name: The name of each operating procedure within that business.

(II) Description of importance: Describe the importance of such business to the Company, such as the impact on the Company's finances and reputation, the impact on the public, the impact on the social economy, the impact on the operations of other Company businesses, the impact on legal compliance, or other descriptions of importance.

(III) The unit of maximum tolerable downtime is hours (external services in hours, internal services in working hours).

2. Non-core Business and Description

The Company's non-core business and description are shown in the table below:

Non-core Business	Description of the Impact of Business Failure	Maximum Tolerable Downtime
Firewall	External network interruption or uncontrolled connection	24 hours
Domain Server	Unable to establish a proper connection to provide services	12 hours

3. Identify core business annually

A Plus Biotechnology Co., Ltd.

Information Security Maintenance Plan

Assessment of compliance with core business elements:

- (I) Data management: Protect data from unauthorized access and damage. Data leakage may lead to legal issues, damage the enterprise's reputation, and affect business continuity.
 - (II) Infrastructure maintenance: Ensure the security and normal operation of networks, hardware, and software. Infrastructure failures lead to business interruption, affecting the Company's operating capability and profitability.
4. Identify applicable legal and contractual requirements
- (I) Legal Compliance
 - (1) Confirm compliance with relevant information security laws, regulations, and standards, including but not limited to the Personal Data Protection Act, Electronic Signatures Act, and information security management systems.
 - (2) Regularly communicate with external consulting advisors to ensure the timeliness of legal compliance.
 - (II) Identification of Contractual Requirements
 - (1) Respect all contractual requirements with customers, suppliers, employees, and other relevant parties, and ensure full compliance therewith during information system operations.
 - (2) When entering into new contracts or updating existing contracts, consult external advisors for review as appropriate to ensure contractual compliance.
5. Regular vulnerability scanning operations shall be conducted on core information and communication systems, and system vulnerabilities shall be remediated.
- (I) Vulnerability Scanning
 - (1) Conduct regular vulnerability scanning on core information and communication systems.
 - (2) Scanning assessment shall use state-of-the-art or recognized vulnerability scanning tools, or be entrusted to a professional information security team for execution.
 - (3) When any vulnerability is identified, its impact shall be evaluated immediately and prioritized for handling, and the vulnerability shall be remediated as soon as possible.
 - (4) Remediation shall be carried out by the information security team or outsourced as appropriate.
 - (5) After remediation is completed, vulnerability scanning shall be conducted again.
 - (II) Penetration Testing
 - (1) Regularly conduct penetration testing on core information and communication systems.
 - (2) Evaluate the use of state-of-the-art or recognized penetration testing methods, or entrust professional information security teams to perform them.
 - (3) When a penetration breach is identified, its impact shall be assessed immediately and prioritized for handling, and the breach shall be remediated as soon as possible.
 - (4) Remediation shall be carried out by the information security team or outsourced as appropriate.
 - (5) Follow-up penetration tests are conducted once patching is complete.
 - (III) Source Code Scanning Security Testing

A Plus Biotechnology Co., Ltd.

Information Security Maintenance Plan

- (1) Security testing is required for core information and communication systems that are owned or controlled, where additions or changes are made to the program source code and the compiled core information and communication system is then launched online.
- (2) Use commercial or open-source Static Application Security Testing (SAST) tools to scan source code.
- (3) For security issues identified during testing, high-risk and medium-risk vulnerabilities must be remediated, while low-risk vulnerabilities are recommended to be remediated.
- (IV) Information and Communication Security Threat Detection and Management Mechanism (SOC)

In accordance with Article 37, Chapter 10 of the Information and Communication Security Control Guidelines for Public Companies, after assessing the Company's scale and the risks faced, the Company is temporarily using the monitoring and detection mechanism of network communication equipment (firewalls, etc.).

IV. Information Security Policy and Objectives

1. Information Security Policy

This policy is established to build and protect the information assets related to all of the Company's information and communication systems—including the physical environment, hardware and software facilities, networks, clouds, data, information, and personnel—and to safeguard them against information and communication security risks arising from internal or external threats, such as damage, loss, leakage, or improper control.

The Company shall adopt the following measures:

- (I) Adhere to laws and regulations by establishing relevant information security management regulations and providing appropriate protective measures for the Company's information assets to ensure their confidentiality, integrity, availability, and legal compliance.
- (II) The Company regularly assesses the impact of various man-made and natural disasters on its information assets and establishes disaster prevention measures and disaster recovery plans for important information assets and critical business operations to ensure the Company's continued operations.
- (III) Supervise the implementation of information security protection work by the Company's employees, establish the concept of “information security is everyone's responsibility,” and enhance the awareness of information security among all business departments and personnel.
- (IV) The Company's employees and business partners connecting to the Company's information and communication systems or providing services shall strictly comply with the Company's relevant information security regulations. In the event of violations, depending on the circumstances, they shall be punished in accordance with the Company's regulations or handled in accordance with contractual penalties. Those with serious circumstances shall additionally be subject to prosecution under relevant laws.

2. Information Security Objectives

(I) Quantitative Objectives

- (1) Upon becoming aware of an information security incident, complete notification, response, and recovery operations within the prescribed time.
- (2) The email opening rate and attachment click rate of the email social engineering exercise shall each be below 5%.

A Plus Biotechnology Co., Ltd.

Information Security Maintenance Plan

(II) Qualitative Objectives

- (1) Adjust the content of information security maintenance in a timely manner in response to changes in laws, regulations, and technology, so as to prevent information systems or information from unauthorized access, use, control, disclosure, destruction, alteration, deletion, or other infringement, and ensure their confidentiality, integrity, and availability.
- (2) Achieve the requirements of information security responsibility level classification and reduce threats from information security risks.
- (3) Enhance personnel's information security protection awareness, and effectively detect and prevent external attacks.

3. Information Security Policy and Objectives Approval Procedure

(I) The information security policy shall be approved by the Company's General Manager.

(II) Information Security Policy and Objectives Dissemination

- (1) The Company's information security policy and objectives shall be communicated to all personnel in the Company annually through education and training, internal meetings, email announcements, and other means.
- (2) The Company shall conduct annual information security audits of outsourced vendors for stakeholders (such as IT service providers and units related to the Company's connection operations).

V. Information Security Promotion Organization

Group	Unit/Job Title	Job Responsibilities
Dedicated Information Security Supervisor	IT Department Head	Supervise information security-related matters
Information Planning Group	Information security personnel	1. Deliberation on information security policy and objectives. 2. Establish the Company's information security-related regulations, procedures, and system documents, and ensure that their content complies with legal and contractual requirements. 3. Formulate the Company's annual work plan based on the information security objectives. 4. Planning of other information security matters. 5. Communicate the Company's information security policy and objectives. 6. Conduct internal information security audits. 7. Report the implementation status of information security matters regularly at management meetings every year.
Information Security Protection Group	Information security personnel	1. Research, implementation, and evaluation of information security technologies. 2. Implementation of information security-related regulations, procedures, and systems. 3. Inventory and risk assessment of information and information operations.

A Plus Biotechnology Co., Ltd.

Information Security Maintenance Plan

		4. Implementation of security protection matters for data and information operations.
		5. Implementation of the information security incident reporting and response mechanism.
		6. Implementation and promotion of other information security matters.

VI. Dedicated Personnel and Budget Allocation

1. Human Resources and Resource Allocation

- (I) In accordance with the "Regulations on Classification of Cyber Security Responsibility Levels," the Company is classified as information security responsibility level D and is required to appoint at least one **cybersecurity personnel holding concurrent positions**. The division of labor is as follows. The list and duties of the Company's existing dedicated information security personnel shall be documented and updated in a timely manner.
 - (1) Responsible for information system classification, internal information security audits, protection baselines, and education and training.
 - (2) Responsible for the promotion of the establishment of information security protection facilities and information security incident reporting and response operations.
- (II) The Company shall strengthen the training of information security personnel and enhance their management capabilities; if information security manpower or experience is insufficient, the Company may engage relevant scholars, experts, professional companies, or institutions to provide advisory and consulting services.
- (III) Personnel responsible for the management, maintenance, design, and operation of important information equipment shall be assigned duties appropriately, with powers and responsibilities dispersed. Those responsible for confidentiality maintenance shall sign a written agreement, and personnel rotation shall be implemented as needed to establish a manpower backup system.
- (IV) The head of each unit shall be responsible for supervising the information security operations of subordinate personnel and preventing illegal and improper conduct.
- (V) The allocation of professional human resources shall be reviewed regularly every year and incorporated into the management review of the continual improvement mechanism of the information security maintenance plan.

2. Budget Allocation

- (I) When planning and allocating relevant funds and resources, the dedicated information security supervisor shall consider the Company's information security policy and objectives, and provide the resources necessary to establish, implement, maintain, and continuously improve the information security maintenance plan.
- (II) When planning to establish information systems, each unit shall concurrently plan the information security protection requirements of the information systems and reasonably allocate the proportion of the information security budget within the overall budget.

A Plus Biotechnology Co., Ltd.

Information Security Maintenance Plan

(III) If any unit has a need for information security resources, the dedicated information security supervisor shall allocate them in view of overall information security resources, and relevant establishment shall proceed after approval by the dedicated information security supervisor.

(IV) The allocation of cybersecurity funds and resources shall be reviewed regularly on an annual basis and incorporated into the management review mechanism.

VII. Inventory of Information and Information Systems

The Company conducts an annual inventory of information and information system assets and designates corresponding asset managers according to management responsibility.

VIII. Information Security Risk Assessment

1. The Company shall conduct an annual risk assessment of information and information equipment assets.
2. The Company shall conduct annual evaluations based on the dimensions of confidentiality, integrity, availability, and legal compliance in accordance with the "Regulations on Classification of Cyber Security Responsibility Levels."
3. The Company shall periodically evaluate the adoption of information security management system standards such as ISO 27001 and CNS 27001, or other systems or standards with equivalent or better effect, obtain third-party certification, and continuously maintain the validity of such certification to maintain the Company's sound information security.

IX. Information Security Protection and Control Measures

Based on its information security risk assessment results and the mandatory requirements of its information security responsibility level, the Company has adopted the following protective and control measures:

1. Management of Information and Information Equipment
 - (I) The Company's employees shall comply with relevant management regulations when using information and information equipment.
 - (II) When using information and information equipment, the Company's employees shall pay attention to the relevant information security requirements and bear corresponding responsibilities.
 - (III) After using information and information equipment, the Company's employees shall return them in accordance with prescribed procedures. The return of information-type information shall ensure that the relevant information has been properly transferred and securely erased from the original equipment.
 - (IV) Non-employees using the Company's information and information equipment shall strictly comply with the Company's relevant information security requirements, and shall not arbitrarily copy information without authorization.
 - (V) Information and information equipment shall be readily identifiable and documented and implemented as rules for acceptable use.
2. Access Control and Encryption Mechanism Management
 - (I) Network Security Control
 - (1) The Company's firewalls are managed by the Company itself, and the zones are divided as follows:
 - A. External network: An outbound network zone connected to a wide area network (WAN).

A Plus Biotechnology Co., Ltd.

Information Security Maintenance Plan

- B. Local Area Network (LAN): The network segment used by the Company's internal unit personnel and internal servers.
- (2) Connections between the external network and the internal local area network must undergo access control through firewalls, and non-permitted services and sources may not enter other areas.
- (3) The Company shall regularly review whether firewall policies are appropriate and adjust rules in a timely manner.
- (4) The areas of the Company's internal network shall be reasonably segregated, and users shall be authorized and access network resources within the scope of authorization.
- (5) Detailed records shall be established for operations by network system managers or information security supervisors.
- (6) Users shall access network services in the manner prescribed by the Company.
- (II) Information Operations Access Management
 - (1) The Company's information operations shall establish password management, and the password requirements shall be met:
 - A. Password length shall be 8 characters or more.
 - B. Users shall change their passwords every 90 days.
 - (2) Users shall be authorized before handling information operations, and shall use a unique user ID. IDs shall not be shared unless approved and documented due to special operational or work necessity.
 - (3) When information users no longer continue handling information operations, user IDs shall be disabled or removed immediately, and information operations managers shall regularly review user permissions.
- (III) Privileged Account Access Management
 - (1) Privileged accounts for information equipment may be used only upon formal application and authorization. Before authorizing privileged accounts, their necessity shall be properly reviewed, and authorization and review records shall be retained.
 - (2) Privileged accounts for information equipment shall not be shared.
 - (3) For privileged accounts, a user ID distinct from the one used for the user's daily business operations shall be assigned.
 - (4) The managers of information equipment shall annually review system privileged accounts and define the handling method for expired privileged accounts.
- (IV) Operations and Communications Security Management
 - (1) Control Measures for Preventing Malware
 - A. The Company's hosts and personal computers shall install antivirus software, and necessary software and hardware updates or upgrades shall be carried out.
 - B. Managers shall conduct annual software inventories of the equipment under their management.
 - C. Users shall not privately use websites known or suspected to be malicious.
 - D. Users shall regularly update operating systems and software to prevent malware from exploiting system or software vulnerabilities to launch attacks.
 - (2) Security Measures for Remote Work

The Company does not allow remote work, but applications may be made for use under special circumstances.

A Plus Biotechnology Co., Ltd.

Information Security Maintenance Plan

- (3) Email Security Management
 - A. Users shall remain vigilant when using email, and browse in plain text mode to avoid reading emails of unknown origin or emails containing macro files.
 - B. As a principle, email shall not transmit confidential or sensitive data. If there is a business need, encryption or other protective measures shall be implemented in accordance with relevant regulations.
 - C. The email service provided by the Company shall not be used to engage in acts that infringe upon the rights and interests of others or are illegal.
 - D. Users shall ensure the accuracy of email transmission.
 - E. Employees shall cooperate with the Company's email social engineering exercise and review the implementation status.
- (4) Information security requirements analysis shall be reviewed regularly every year, and shall include:
 - A. Access control methods for systems and data, especially access control for sensitive data.
 - B. Establish appropriate monitoring measures for systems and related equipment, including identity authentication access records (such as failed logins, off-hours logins, and successful logins by multiple users using the same source IP), access resource records, important actions, important data changes, detection of attacks and unauthorized connections, functional errors, and administrator behavior, and establish appropriate protection mechanisms for logs.
 - C. The system shall ensure processing validity and data authenticity through authorization control by user ID and password.
 - D. The system shall be protected against unauthorized tampering or modification.
 - E. Data shall be copied and backed up regularly.
 - F. In addition to regular copying and backup, backup shall be performed before processing version updates, major processing, and large-volume data changes to ensure data security.
 - G. According to the requirements of each unit, highly sensitive data shall be protected by encryption during transmission or storage.
 - H. Establish control mechanisms for remote access systems, such as establishing secure remote connection mechanisms (such as VPN and VDI), adopting multi-factor authentication, adopting encrypted connections, adopting the principle of least privilege, retaining complete user operation audit trails, monitoring and alerting abnormal operation behavior, implementing security vulnerability updates and other security control measures, and educating home-based workers to remain vigilant against network risks.

(V) Ensure Physical and Environmental Security Measures

- (1) Management of Communication Room (Cabinet)
 - A. Communication rooms (cabinets) shall be physically isolated.

A Plus Biotechnology Co., Ltd.

Information Security Maintenance Plan

- B. Company personnel or visitors may enter communication rooms (cabinets) only upon application and authorization, and their managers shall regularly review the list of authorized personnel.
 - C. Personnel entering controlled areas shall at all times pay attention to unidentified or suspicious persons.
 - D. External support personnel may be permitted to enter communication rooms (cabinets) only when necessary.
 - E. Records shall be retained for personnel and equipment entering and exiting communication rooms (cabinets).
- (2) Environmental Control of Communication Room (Cabinet)
- A. Backup measures may be established for the air conditioning and power of computer rooms (cabinets).
 - B. Computer rooms (cabinets) may be equipped with security detection and protection measures, including heat and smoke detection equipment, fire alarm equipment, temperature and humidity monitoring equipment, water leakage detection equipment, and intruder detection systems, to reduce hazards caused by unsafe environments.
 - C. All safety equipment shall be inspected and maintained regularly, and appropriate training on the use of safety equipment shall be provided regularly to equipment managers.
- (3) Physical and Environmental Security Measures for Office Areas
- A. A clear desk policy should be considered to reduce the opportunities for documents and removable media to be accessed by unauthorized personnel, lost, or damaged outside office hours.
 - B. Documents and removable media shall be stored in cabinets when not in use or outside working hours.
 - C. Confidential and sensitive information shall be locked when not in use or after work.
 - D. Confidential information or information operations processing confidential information should avoid being stored in or located at places accessible to the public.
 - E. Directories and internal personnel telephone books showing locations where confidential information is stored or where operations processing confidential information are conducted should not be easily obtainable by unauthorized persons.
 - F. Information or equipment related to information operations shall not be taken away from the office without authorization from the manager.

(VI) Data Backup

- (1) Important data shall be backed up, and the backup frequency shall meet the target requirements of the recovery point in time, and off-site storage shall be implemented.
- (2) Confirm backup of important data, rather than directly overwriting it back to the original information equipment.
- (3) Backups of sensitive or confidential information shall be protected by encryption.

A Plus Biotechnology Co., Ltd.

Information Security Maintenance Plan

- (4) Security equipment shall regularly back up log records, review them regularly and have the execution results reviewed by supervisors, and review the implementation status.
- (VII) Security Management of Computer Use
 - (1) If the computer operating system is not used for more than 15 minutes, users shall immediately log out or activate the screen saver function.
 - (2) Unauthorized installation of peer-to-peer files and sharing software or software without legal authorization is prohibited.
 - (3) Networked computers shall at all times cooperate in updating operating systems, application vulnerabilities and patches, or antivirus codes.
 - (4) Laptop computers and physically isolated computers shall regularly update operating systems, application vulnerabilities and patches, or antivirus codes manually.
 - (5) Computers and monitors shall be turned off after work.
 - (6) If an information security issue is identified, it shall be proactively reported in accordance with the Company's reporting procedures.
- (VIII) Security Management of Mobile Devices
 - (1) Confidential data shall not be accessed, processed, or transmitted by unauthorized mobile devices.
 - (2) Unauthorized mobile devices shall not be brought into sensitive meetings or locations.
- (IX) Email Security Management
 - (1) Upon receipt of email, recipients shall manage its security on their own.
 - (2) If sensitive information must be transmitted by email, it shall be encrypted before transmission.
 - (3) To prevent emails from being sent under the guise of the Company's employees, and to achieve identity recognition and non-repudiation, emails shall be sent by electronic signature where necessary.
 - (4) Emails from unknown sources should not be opened at will, so as to avoid activating malicious executable files and causing damage to the network system; the email system administrator shall be notified to handle such matters.
 - (5) Sending emails to harass others, causing unease and inconvenience to other users, is prohibited.
 - (6) Sending anonymous letters or forging another person's name to send emails is prohibited.
 - (7) Email servers shall have a filtering mechanism in place (currently available through firewall functions).
- (X) Handling of Network Intrusion
 - (1) If a network intrusion or suspected intrusion is identified (such as webpage tampering, distributed attacks, illegal data access, password cracking, etc.), necessary action shall be taken immediately.
 - (2) Immediately reject any access action by intruders to prevent the disaster from continuing to expand; when the protective network is breached, uniformly set rejection of any access; or if the intruder is under strict monitoring, access actions may be appropriately allowed for the purpose of tracing the intruder, provided that internal network security is not endangered.

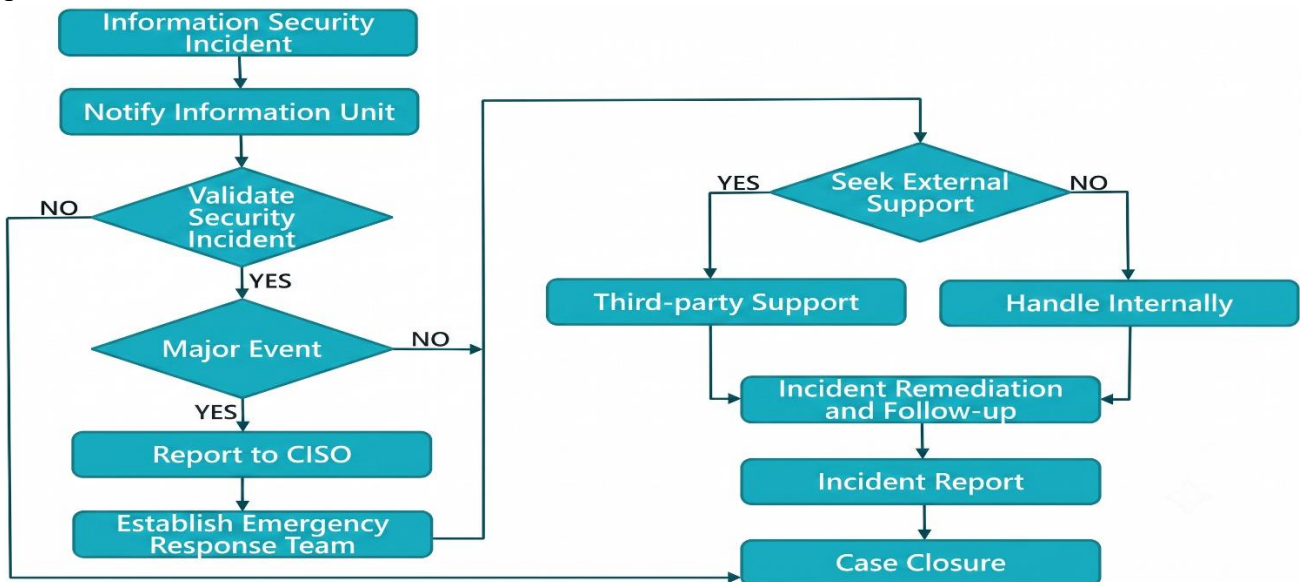
A Plus Biotechnology Co., Ltd.

Information Security Maintenance Plan

- (3) Cut off the intruder's network connection. If it cannot be cut off, the firewall must be shut down; or for the purpose of tracing the intrusion, the intruder may be allowed conditional connection. Once the intruder endangers internal network security, the intruder's network connection must be cut off immediately.
- (4) Network security measures and firewall settings shall be comprehensively reviewed and revised to prevent similar intrusions and attacks.
- (5) The intrusion situation and the scope of impact assessment shall be formally recorded. Immediately report the intrusion situation to the responsible supervisor and report to the relevant emergency response team to obtain necessary external assistance.

X. Information Security Incident Reporting, Response, and Exercise Mechanisms

To ensure the timely monitoring of information security incidents and effectively mitigate the damage caused thereby, the Company shall establish information security incident reporting, response, and exercise mechanisms, as detailed in the information security incident reporting and response procedures.



XI. Assessment and Response to Information Security Intelligence

Upon receiving information security intelligence, the Company shall evaluate the content of such intelligence and determine the most appropriate response in view of its impact on the Company, the Company's acceptable risk, and the Company's resources. Where necessary, the control measures of the information security maintenance plan may be adjusted, and records shall be made.

1. Classification and Assessment of Information Security Intelligence

After receiving information security intelligence, the Company shall designate dedicated (part-time) information security personnel to conduct intelligence analysis, and classify and assess the intelligence according to its nature. The classification and assessment of intelligence are as follows:

(I) Information security-related information intelligence

If the content of information security intelligence includes major threat indicator intelligence, intelligence on information security threat vulnerabilities and attack techniques, analysis reports on major information security incidents, experience sharing on information security-related technologies or issues, or suspected system vulnerabilities or suspicious programs, it constitutes information security-related information intelligence.

A Plus Biotechnology Co., Ltd.

Information Security Maintenance Plan

(II) Intrusion Attack Intelligence

If the content of information security intelligence includes clear evidence of attacks on specific webpages, inappropriate content on specific pages, personal data leakage on specific webpages, or network attack activities conducted on specific systems, it constitutes intrusion attack intelligence.

(III) Sensitive intelligence

If the content of information security intelligence includes personal data that may directly or indirectly identify an individual, such as name, date of birth, national identification card number, passport number, characteristics, fingerprints, marital status, family, education, occupation, medical records and healthcare data, medical treatment, genes, sexual life, health examinations, criminal record, contact information, financial status, social activities, and other personal data, or if public disclosure of the intelligence would infringe the rights of the Company, individuals, or other groups, or involve Company confidential information, sensitive information, or national secrets, it constitutes sensitive intelligence.

(IV) Intelligence involving core business, core information systems, and the operation of core business and core information systems involving critical infrastructure operations constitutes involvement of core business.

2. Information Security Intelligence Response Measures

After conducting classification and assessment of information security intelligence, the Company shall take corresponding measures based on the nature of the intelligence, and may adjust the control measures of the information security maintenance plan where necessary.

(I) Information security-related information intelligence

Risk assessments are conducted after consolidating intelligence, and corresponding risk prevention mechanisms are implemented based on the control measures of the information security maintenance plan.

(II) Intrusion Attack Intelligence

The dedicated (part-time) information security personnel shall determine whether there is any immediate danger and, where necessary, take immediate notification and response measures, adopt corresponding risk protection measures in accordance with the information security maintenance plan, and notify each unit to carry out relevant prevention.

(III) Sensitive intelligence

For content involving personal data, trade secrets, general official secrets, sensitive information, or national secrets, masking or deletion shall be adopted for exclusion. For example, personal data and trade secrets shall be excluded by masking or deleting the specific section or text, or by de-identification.

(IV) Intelligence involving core business and core information systems shall be assessed as to whether it affects the Company's operations, and corresponding risk management mechanisms shall be adopted in accordance with the information security maintenance plan.

(V) Join information security intelligence sharing organizations to obtain information security early warning intelligence and information on information security threats and

A Plus Biotechnology Co., Ltd.

Information Security Maintenance Plan

vulnerabilities

(1) National Information Security Information Sharing and Analysis Center
(<https://www.nics.nat.gov.tw/>)

(2) Taiwan Computer Emergency Response Team/Coordination Center
(<https://www.twcert.org.tw/>)

(VI) The method for notifying other affected agencies, reporting contact windows, and contact information may refer to the “Enterprise Information Security Incident Response Guide” of the Taiwan Computer Emergency Response Team/Coordination Center (TWCERT/CC).

XII. Management of Outsourcing of Information Systems or Services

If the Company currently has a need to outsource the establishment, maintenance and operation of information systems, or information services, it shall, after considering the other party's professional capabilities and experience, the nature of the outsourced items, and information security and other items, select appropriate vendors and supervise their information security implementation status.

1. Matters to Note When Soliciting Outsourced Information Services

- (I) The procedures and environment for the trustee's performance of entrusted business shall involve sound information security management measures or pass third-party certification.
- (II) The entrusted party shall assign sufficient information security professionals who have received appropriate qualification training, hold information security professional certificates, or have similar business experience.
- (III) The entrusted party shall have relevant information security maintenance measures.
- (IV) When the entrusted party accepts entrusted business involving national secrets, it shall consider the classified content level of the national secrets involved in the entrusted business, and specify in relevant announcements or contract documents that the personnel handling such business and personnel who may come into contact with such national secrets shall undergo suitability screening, and their departure from the country shall be Classified National Security Information Protection Act.
- (V) The suitability screening referred to in the preceding paragraph may, within the necessary scope, examine the following matters, and the written consent of the person concerned shall be obtained before the examination:
 - (1) Persons who have committed the offense of disclosure of secrets, or after the termination of the Period of Mobilization for Suppression of Communist Rebellion, have committed the offense of internal disorder or the offense of foreign aggression, and have received a final and binding criminal judgment, or are wanted and whose case has not yet been closed.
 - (2) Former civil servants who, for violating relevant security and confidentiality regulations, have been subject to disciplinary sanctions or administrative sanctions of demerit or above.
 - (3) Persons who have been lured or coerced by foreign governments, the Mainland Area, or the official authorities of Hong Kong or Macau to engage in matters detrimental to national security or major interests.

A Plus Biotechnology Co., Ltd.

Information Security Maintenance Plan

- (4) Other specific items related to the protection of national secrets.
- 2. Matters to Note When Supervising the Entrusted Party's Information Security Maintenance Status
 - (I) Where the entrusted business of the information system includes custom information system development, the trustee shall provide a third-party security testing certificate for said information system. If the services involve the use of systems or resources not developed by the trustee, the trustee shall specify the non-self-developed content and its source, and provide a proof of authorization.
 - (II) If, in performing entrusted business, the entrusted party violates information security-related laws and regulations or becomes aware of an information security incident, it shall notify the entrusting Company and the remedial measures taken within 1 hour.
 - (1) Information systems are tampered with.
 - (2) Operation of the system is affected or suspended.
 - (III) Upon termination or rescission of the entrustment relationship, it shall be confirmed that the entrusted party returns, transfers, deletes, or destroys the data held for performing the entrustment contract.
 - (IV) Other information security-related maintenance measures to be taken by the entrusted party.
 - (V) The Company shall periodically, or when it becomes aware that the entrusted party has experienced an information security incident that may affect the entrusted business, verify the implementation status of the entrusted business through audits or other appropriate means.

XIII. Information Security Education and Training

- 1. Information Security Education and Training Requirements
 - (I) Information security personnel with concurrent duties or information personnel shall each receive at least 6 hours of professional information security course training every year.
 - (II) The Company's employees shall each receive at least 3 hours of general information security education and training every year.
- 2. Methods for Conducting Information Security Education and Training
 - (I) At the beginning of each year, the Information Security Protection Group shall, taking into account the needs of different job categories such as management, business, and information, formulate information security awareness promotion and education and training plans, so as to establish employees' information security awareness and enhance the Company's information security level, and shall retain relevant records of information security awareness promotion and education and training.
 - (II) The content of the Company's information security awareness promotion and education and training may include:
 - (1) Information Security Policy.
 - (2) Information security laws and regulations.
 - (3) Information security operations.
 - (4) Information security technical training.
 - (III) When employees report for duty, they shall be fully informed of the Company's

A Plus Biotechnology Co., Ltd.

Information Security Maintenance Plan

relevant information security operating standards and their importance.

(IV) The policy on information security education and training shall apply not only to employees, but also uniformly to external users of the Company.

XIV. Assessment Mechanism for Information Security Matters Involving Company Employees
The Company's employees' information security awareness shall be included in assessments and implemented in accordance with the employee performance appraisal management regulations and employee reward and punishment management regulations.

XV. Continuous Improvement and Performance Management Mechanisms for the Information Security Maintenance Plan and its Implementation

1. Implementation of the Information Security Maintenance Plan

In order to implement this security maintenance plan and enable information security management to operate effectively, relevant units shall ensure that, when formulating documents, processes, procedures, or control measures at various levels, they are consistent with the Company's information security policy, objectives, and the content of this security maintenance plan, and shall retain relevant records of implementation results.

2. Audit Mechanism for the Implementation of the Information Security Maintenance Plan

(I) Implementation of the Audit Mechanism

- (1) The dedicated information security supervisor shall carry out internal audit operations regularly (at least once every 2 years) or once after major system changes or organizational restructuring.
- (2) The audit plan shall include the basis and purpose of the audit, period, key areas, composition method of the audit team, confidentiality obligations, audit methods, criteria and items, and assistance matters for the audited unit, and shall include the results of the previous audit in the scope of the audit.
- (3) When conducting an audit, the dedicated information security supervisor shall notify the audited unit before carrying out the audit, and clearly provide the audited unit with audit information (including the audit period, sample data interval, audit items, and sample information).
- (4) The Company's auditors shall receive appropriate training and have audit capabilities, and shall not audit the business they handle themselves, so as to ensure the objectivity and fairness of the audit process. The contents of the audit checklist shall be compiled into the audit report and improvement tracking report, and submitted to relevant responsible supervisors for approval.
- (5) Audit results shall be reported to the General Manager, and relevant records of the audit process shall be retained as evidence of the information security audit plan and audit events.
- (6) When conducting an audit, auditors shall perform at least one specific audit item (for example: whether they understand the information security policy and the information security responsibilities to be borne, whether information security operating procedures and powers and responsibilities for personnel have been established, and whether passwords are changed regularly).

(II) Audit Improvement Report

- (1) If the audited unit identifies deficiencies or items pending improvement after the implementation of the audit, it shall formulate improvement measures and

A Plus Biotechnology Co., Ltd.

Information Security Maintenance Plan

- improvement progress planning for the deficiencies or items pending improvement, and implement them.
- (2) If the audited unit identifies deficiencies or items pending improvement after the implementation of the audit, it shall determine the causes thereof and assess whether similar deficiencies or items pending improvement exist.
 - (3) After determining the causes of deficiencies or items pending improvement, the audited unit shall propose and implement relevant improvement measures and improvement progress planning, and may consider changes to the current information security management system or related documents where necessary.
 - (4) The Company shall periodically review the effectiveness of the improvement measures, improvement progress planning, and supporting documents adopted by the audited unit for deficiencies or items pending improvement.
 - (5) When the audited unit implements improvement measures, it shall retain relevant implementation records, and fill in an improvement report with the improvement methods and results.
3. Continuous Improvement and Performance Management of the Information Security Maintenance Plan
- (I) The Company's dedicated information security supervisor shall regularly convene an information security management review meeting every year to confirm the implementation status of the information security maintenance plan.
 - (II) Management review topics shall include the following discussion items:
 - (1) Status of handling past management review agenda items.
 - (2) Changes in internal and external issues related to information security management operations, such as changes in laws and regulations, requirements of the parent company, and resolutions of the dedicated information security supervisor.
 - (3) Appropriateness of the content of the information security maintenance plan.
 - (4) Feedback on information security performance.
 - (5) Implementation status of the information security policy and objectives.
 - (6) Implementation status of the allocation of information security manpower and resources.
 - (7) Implementation status of information security protection and control measures.
 - (8) Internal and external audit results.
 - (9) Non-conformities and corrective measures.
 - (10) Risk assessment results and progress of implementation of risk treatment plans.
 - (11) Handling and improvement status of major information security incidents.
 - (12) Feedback from stakeholders.
 - (13) Opportunities for continual improvement.
 - (III) Follow-up reports shall be prepared for the management review of the continual improvement mechanism, and relevant records shall also be retained as evidence of the implementation of the management review.
 - (IV) The annual report shall state information such as cybersecurity policies, specific management plans, resources invested in cybersecurity management, losses and

A Plus Biotechnology Co., Ltd.

Information Security Maintenance Plan

possible impacts of material cybersecurity incidents, and response measures.

XVI. Implementation

1. This Plan shall be implemented upon approval by the General Manager, and the same shall apply when amended.
2. This Plan was established on August 1, 2024.
The 1st amendment was made on September 20, 2024.