Mycenax Biotech Inc.

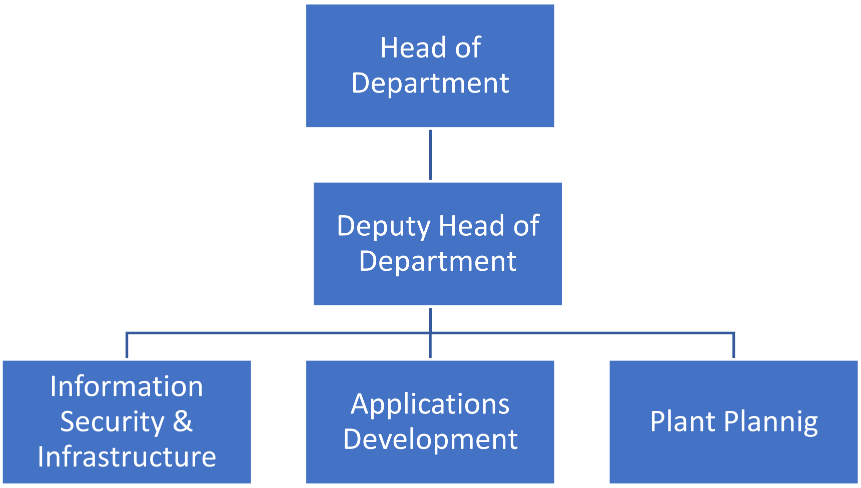
The cyber security risk management

1. The cyber security risk management framework

1.1 Information Security Organization

The Company has an Information Technology Management Department, which is responsible for coordinating information security and protection-related policy formulation, implementation, risk management, and compliance checks. The head of the department reports the effectiveness of information security management, issues and directions related to information security to the board of directors every year.

1.2 Organization of the Information Technology Management Department


Head of Department
Deputy Head of Department
Information Security & Infrastructure
Applications Development
Plant Plannig

2. The information and communication security policy

2.1 Information security management strategy and framework

In order to effectively implement the information security management of the whole plant, the information security organization holds regular meetings every quarter to review the applicability and protection measure of the information security according to the management cycle mechanism of Plan, Do, Check and Action (PDCA), and report the implementation results to the board of directors every year.

2.1.1 Plan: Focus on information security risk management, establish a complete Information Security Management System (ISMS), reduce corporate information security threats from the system, technology, and program, and establish confidential information protection services that meet the Company's needs and meet the highest standards.

2.1.2 Do: Construct multi-layer information security protection, continuously introduce innovative technologies for information security defense, integrate and internalize the information security control mechanism into daily operation processes such as software and hardware maintenance, systematically monitor information security, and maintain the confidentiality, completeness, and availability of the Company's important assets.

2.1.3 Check: Actively monitor the effectiveness of information security management, and conduct information security index measurement and quantitative analysis based on the audit results.

2.1.4 Action: Based on review and continuous improvement, implement supervision and audit to ensure the continuous effectiveness of information security regulations; when employees violate relevant regulations and procedures, personnel sanctions will be taken depending on the circumstances of the violation (including employee performance appraisals for the current year or necessary legal actions). In addition, based on performance indicators and maturity evaluation results, regular review and implementation of improvement measures including information security measures, education and training, and publicity to ensure that the Company's important confidential information is not leaked.

2.2 Management Plan

2.2.1 Network Security

(1) Network security introduces advanced technology to perform computer scanning and system and software updates.

(2) Strengthen the network firewall and network control to prevent the spread of computer viruses across machines and across factories.

2.2.2 Endpoint Security

(1) Establish a computer equipment entry control mechanism to prevent unauthorized or malicious software from entering the Company.

(2) Set endpoint antivirus measures based on computer types to enhance malware behavior detection.

2.2.3 Application Security

(1) Formulate development process application security self-inspection form, evaluation standards and improvement goals.

(2) Continue to strengthen the application control security control mechanism and integrate it into the development process and platform.

2.2.4 Data Security

(1) Control folder access permissions through file confidentiality classification.

(2) The important data are regularly backed up, and the 3-2-1 backup principle is followed.

(3) Regularly communicate the Company's latest information security regulations and precautions.

3. The Resources Invested and Achievements in the Implementation of Information and Communication Security Management for the Fiscal Year 2023:

3.1 Strengthen information security framework:

3.1.1 Completed network architecture enhancements across various plant facilities, ensuring that unauthorized devices are unable to access the Company’s internal network resources.

3.1.2 Implemented a visualized network equipment management platform to provide real-time monitoring of the status of network devices.

3.1.3 Leased cloud backup space, storing the third backup copy in the cloud.

3.2 Staff education and training

3.2.1 Conducted a social engineering black-box exercise for all employees (without prior notification) to enhance awareness of information security, with a total of 377 participants.

3.2.2 Provided information security policy training for new employees, with a total of 16 individuals trained.

3.2.3 IT personnel responsible for information security underwent two external educational training sessions in separate batches.

3.2.4 Selected information security incident cases each quarter for the Company-wide awareness campaigns on the importance of information security.

4. The status of the implementation of Information and Communication Security Management for the year 2023 was reported to the Board of Directors in the 10th meeting (November 13, 2023) of the 15th session.