大學光學科技股份有限公司
Universal Vision Biotechnology Co., Ltd.

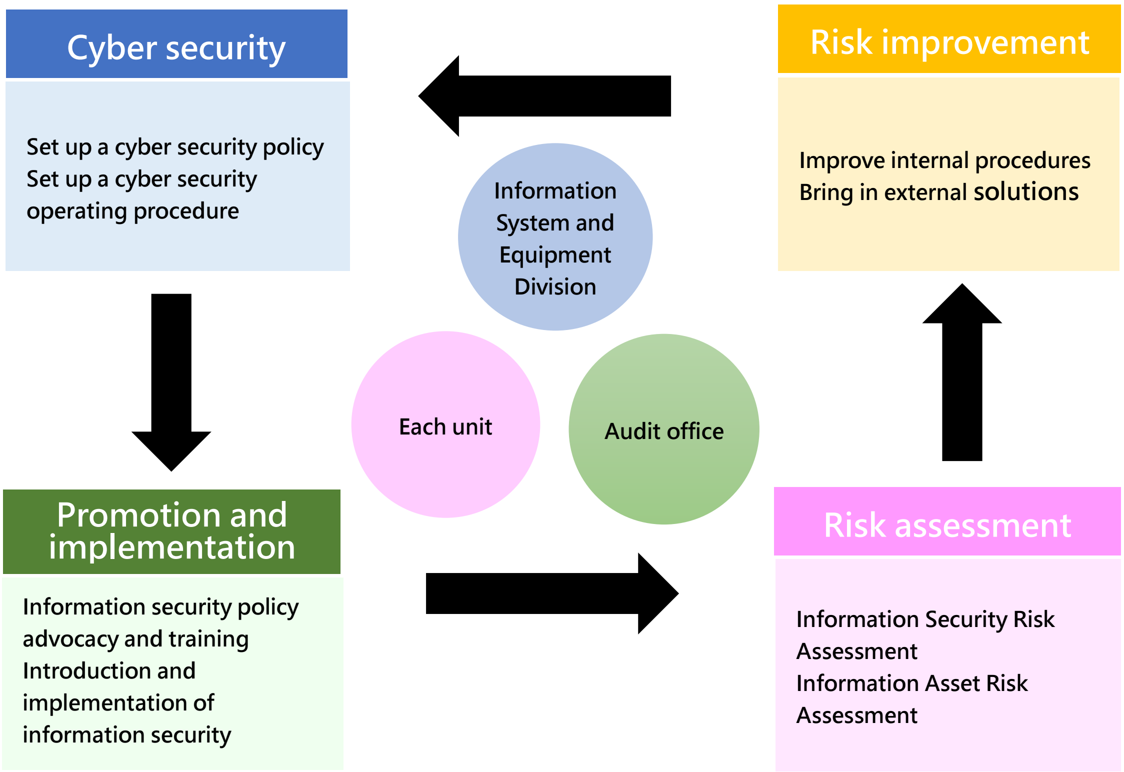
Cyber Security

1. Cyber security management strategy and structure

The unit in charge of information security of the Company is the Information System and Equipment Division, which is staffed with one director and several professional information personnel, is responsible for formulating internal information security policies, planning and implementing information security operations, and the promotion and implementation of information security policies, reports the Company's information security governance overview to the Audit Committee.

The Company's information security supervision and inspection unit is the Audit Office, which is staffed with one audit director and several dedicated auditors, is responsible for supervising and inspecting the implementation of internal information security matters. If relevant deficiencies are found in the inspection, the inspected unit will be required to submit relevant improvement plans and specific actions, which will be tracked for the improvement results so as to reduce internal information security risks.

Organizational operation mode - The PDCA cycle management is adopted to ensure the achievement of reliability goals and continuous improvement.



Cyber security

Set up a cyber security policy
Set up a cyber security operating procedure

Risk improvement

Improve internal procedures
Bring in external solutions

Information System and Equipment Division

Each unit

Audit office

Promotion and implementation

Information security policy advocacy and training
Introduction and implementation of information security

Risk assessment

Information Security Risk Assessment
Information Asset Risk Assessment

2. Cyber security policy

In order to implement the effective operation and implementation of UVB's various information management systems, we maintain the confidentiality, integrity, and availability of important information systems so as to ensure the safe operations of information systems, equipment, and networks.

UVB has established an information security management mechanism, including the following three major items:

(1) System norms: Formulate the Company's information security management systems and guidelines, and standardize the information-related operation behavior of colleagues.

(2) Application of new technology: Import and build information security management related software and hardware, and implement information security management measures.

(3) Personnel training: Regularly conduct information security education and training to enhance the information security concept of all colleagues and implement various information security measures.

Described as follows:

- System norms: The Company has formulated a number of information security management guidelines and systems to regulate the information security behavior of the Company's personnel. It regularly inspects whether the relevant systems conform to the changes in the operating environment every year, and makes adjustments in a timely manner according to needs.
- Application of new technology: In order to prevent various internal and external information security threats, in addition to adopting a multi-layer network architecture design, the Company also builds various information security protection systems and mechanisms, such as high reliability architecture (HA) of high availability, host environment backup, data backup (transaction records, differential backup, and full backup), off-site backup mechanism to improve the security of the overall information environment. In addition, in order to ensure that the operation behavior of internal personnel conforms to the Company's system norms, asset management system tools are also introduced to implement equipment and personnel information security management measures.
- Personnel training: The Company regularly organizes information security education and training courses and establishes an online learning (E-Learning) system to enhance internal personnel information security knowledge and professional skills.

3. Specific management plan:

Information Security Management Measures		
Type	Description	Relevant operations
Authority management	Management measures for personnel account, authority management, and system operation behavior	Personnel account permission application management and review Regular personnel account permissions inventory
Access control	Control measures for personnel access to internal and external systems and data transmission channels	Internal / external access control measures Operation behavior tracking record
External threat	Internal potential weaknesses, poisoning channels, and protective measures	Host / computer vulnerability inspection and update measures Virus protection and malware detection Malicious attacks prevention equipment
System availability	System availability status and handling measures when service is interrupted	Routine inspection of computer room System / network availability monitoring and reporting mechanism Response measures to service interruption Information backup, local / remote backup mechanism, regular data restoration test Host restore test Regular disaster recovery drills

4. Resources invested in cyber security management

Two part-time staff are in place to be in charge of information security development. A budget in the amount of 6 million and more is prepared for information security software and hardware updates.

The loss and possible impact (for example, the impact on the operation or goodwill) due to major cyber security incidents in the most recent year and as of the publication date of the annual report, and the countermeasures. If it cannot be reasonably estimated, the fact that it is impossible to reasonably estimated should be explained: None.