



EirGenix, Inc.

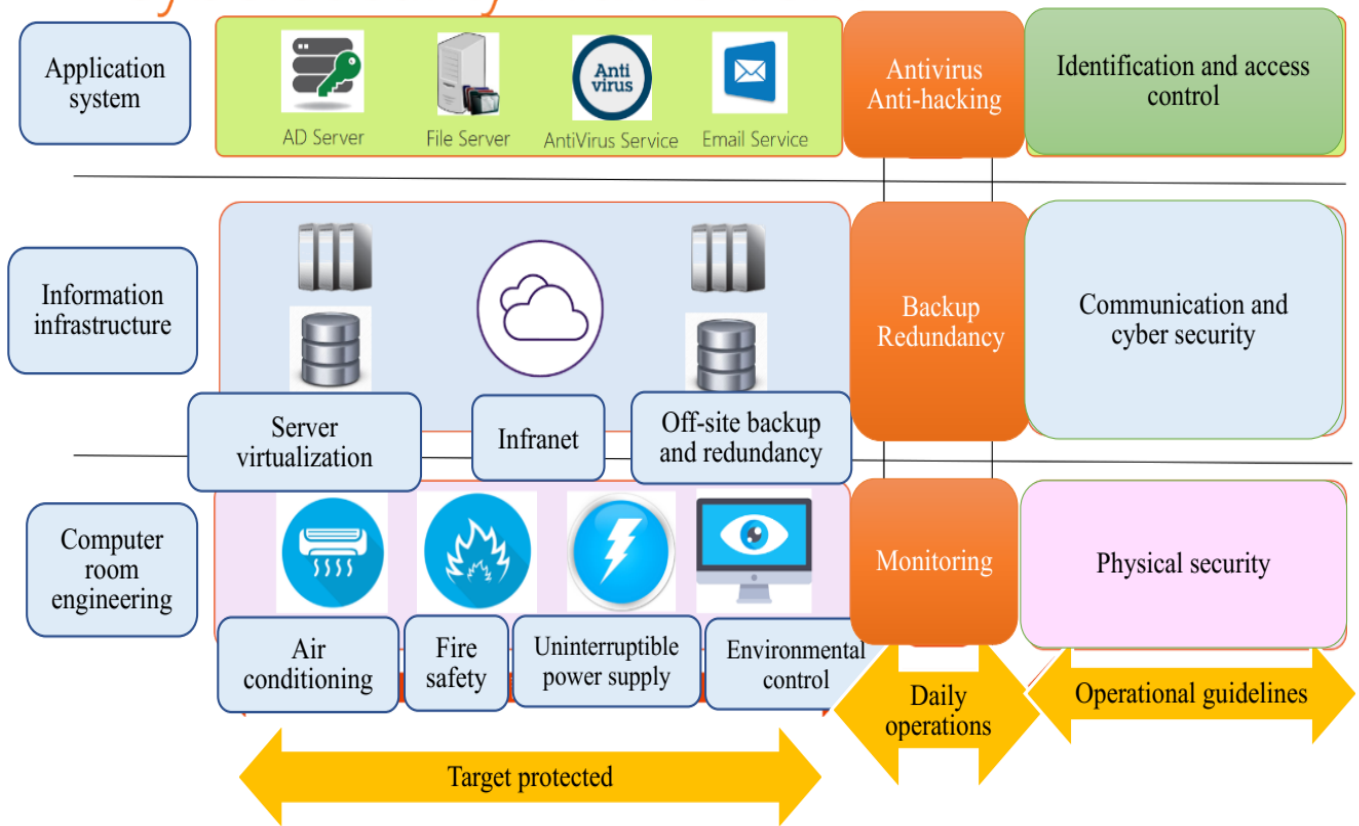
Cyber Security Management

Cyber security risk management framework, cyber security policies, concrete management programs, and investments in resources for cyber security management.

The Company has included information security in the annual audit project, regularly reviewed and evaluated security measures, and regularly changed various security settings, while updating the system and working with professional vendors to ensure information and network security. Furthermore, to ensure that our information system can continue to provide stable services, we have established various redundancy mechanisms and backup systems and improved relevant processes as appropriate and upgraded computer software and hardware in response. The Information Technology Department often sends information security information to employees via emails and reported information security issues to the Board on March 22, 2022.

We have also established an information security risk management framework to reduce the risk of unknown information security threats caused by changes in the internal and external information environment. To reduce the unknown information security risks caused by new information technologies adopted and changes in the external environment, the Information Technology Department is responsible for coordinating information security and relevant matters and formulating internal information security plans. After such plans are approved, the department should conduct information security risk management as per the standard operating procedures, regularly examine internal information security, raise personnel' s awareness of information security, and perform information security drills. The Company's information security framework is designed in a layered manner, and the structure is as follows:

Cybersecurity Framework



It aims to achieve the purpose of corporate sustainable development, ensure the effective operations of the Company's information systems to support the normal operations of various business activities, and ensure continuous operations to minimize operating losses. When all employees of the Company use information-related systems, this information security management policy is used as the basis for management and compliance.


The information system security policy is divided into the aspects below:

- A. System and regulations: Update relevant information security management regulations, infrastructure, systems, and information security protection technologies in line with relevant laws and regulations and changes in the Company's business and information technologies, to maintain the confidentiality, integrity, and availability of our important information systems, and continuously protect information from various threats. The permissions

management and changes of the important information systems should be recorded as a basis for auditing.

- B. Information technology management: Update and evaluate information systems in real time and execute necessary control measures to ensure the security of data, systems, networks, and information infrastructure.
- C. Personnel and organization: The Information Technology Department should offer information security education and training to raise internal personnel' s awareness of information security and improve their relevant professional skills.

The Company actively strengthens the security of the overall information system. Relevant matters, from the information security regulations to the design of information infrastructure, system maintenance and upgrading, professional personnel' s training, and raising of employees' awareness of information security, are all included in the scope of information security. We self-examine information security every year to see if relevant systems are aligned with the changes in the environment and make timely adjustments according to needs. We adopted the Taiwan Intellectual Property Management System (TIPS) in 2021 to strengthen the management of the Company's confidential information. Our specific information security management measures implemented are as follows:

Category	Description	Operating method
Permissions management	Personnel and group accounts and verification methods management, permissions management, and system management	 Personnel accounts management operations should proceed or be changed after an application is filed and approved by responsible managers in accordance with the operating procedures. Each user's use permissions should be immediately revoked after resignation or job change to prevent unauthorized access.

Category	Description	Operating method
	permissions management	<ul style="list-style-type: none"> ✚ Regularly review system-related permissions. ✚ Manage system account life cycle and permissions accounts. ✚ Adopt multi-factor authentication and designated login to manage important systems.
Access management	Data flow control and auditing, physical equipment access management, audit records, and incident investigation	<ul style="list-style-type: none"> ✚ Revise data flows into and out of important information systems and keep records of the access for auditing. ✚ Conduct physical security protection of the information system console. ✚ Analyze audit records and issue automatic warnings of abnormalities. ✚ Identify the information security level according to the importance and the degree of risk. ✚ Adopt digital rights management technology for important files to control the data flow to avoid unauthorized access.
Threat and risk management	Rate the information risks that may be caused by internal employees, external personnel, and potential vulnerabilities in	<ul style="list-style-type: none"> ✚ Standardize the user's computer preset. ✚ Launch operating regulations for external vendors to access the Company's information systems. ✚ Launch risk assessment procedures for adoption of new technologies. ✚ Deploy multiple brands' multi-layer firewalls and cloud email

Category	Description	Operating method
	<p>the systems and take measures to reduce risks</p>	<p>filtering to reduce the chance of external cyber attacks and intrusion of phishing emails.</p> <ul style="list-style-type: none"> ✚ Strengthen endpoint security, regularly update users' computers, and install antivirus software. ✚ Regularly offer information security education and training to improve personnel's awareness of information security .
<p>System integrity and availability management</p>	<p>Maintain the availability and integrity of data and systems to resume normal operations in the event of a disaster or damage</p>	<ul style="list-style-type: none"> ✚ The host has been virtualized in a cluster to improve the availability of systems. ✚ Adopt large storage devices, regularly automate on-site and off-site backups, and perform recovery tests as planned to ensure the integrity and availability of systems. ✚ Adopt multiple redundancy mechanisms for infrastructure, multiple UPS systems with automatic generators, N+1 and 1+1 fan coil units, as well as multiple redundancy measures for internal and external network wires and equipment to reduce the chance of information service interruption.