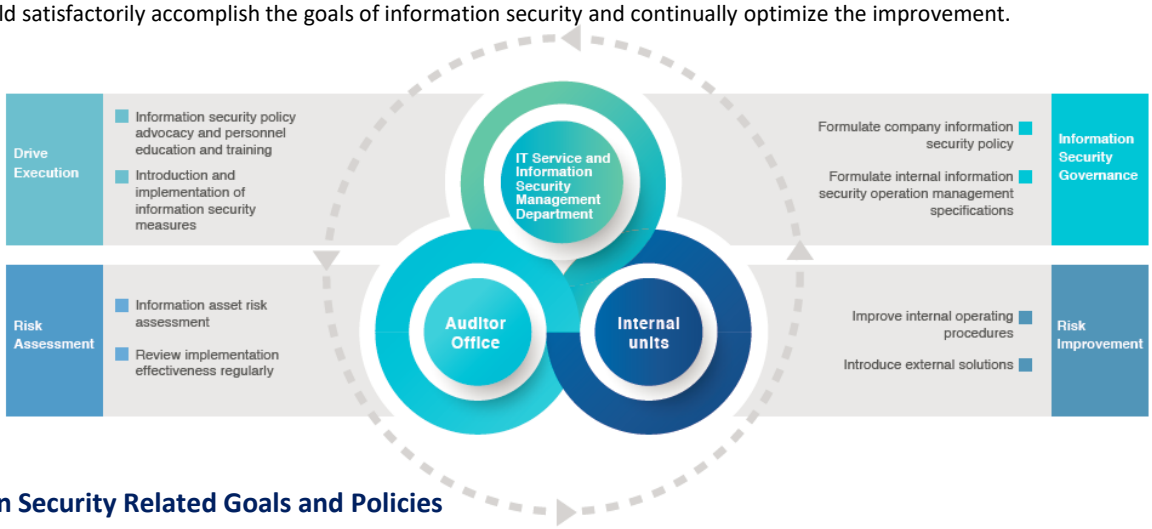
Information Security Policy and Management Programs

Information Security Related Risk and Management Framework

In Sinyi Reality (hereinafter referred to as the "Company"), the information security issues are under charge by the Information Service & Information Security Management Department which assumes the responsibility for internal information security policies to map out and implement information security operations, execute and implement thoroughly the information security policies.
In terms of organizational operation, the Company adopts Plan-Do-Check-Act (PDCA) circulatory management, set up integral information security management systems to effectively prevent information security related problem from occurrence. In turn through such efforts, the Company could satisfactorily accomplish the goals of information security and continually optimize the improvement.



Information Security Related Goals and Policies

Information Security Related Goals

The Company duly works out the information security policies well oriented to the Sinyi Group and invests appropriate resources to completely ensure confidentiality, integrity and availability.

1. With adequate efforts to ensure confidentiality, implement thoroughly the information access control. Only such personnel having been adequate authorized with the required power are entitled to access to information.
2. The Company puts forth maximum possible efforts to ensure accurate and integral contents of the information and shall prevent a potential unauthorized amendment to the information.
3. The Company assures the availability of the information system and provides such system to meet the need of business operation.
4. The Company assures that all information operation would satisfy the requirements by laws and regulations.

The Information Security Policies

1. The Company enhances the security of the Sinyi Group's information system and network environment to prevent potential disclosure of electronic confidential information.
2. The Company duly sets up the sound countermeasure procedures to deal with an information security incident to prevent the impairment from worsening.
3. The Company carries out information security related educational & training programs, strengthens the consensus and awareness of entire Sinyi Group staff about information security.
4. The Company promotes the information security management system, implements thoroughly the Sinyi Group's information security management operation and further reassesses the performance of the implementation to accomplish the goals of panoramic information security.

Concrete Management Programs

In the information security enhancement part, in addition to ensuring the normal operation of backup and remote storage operations, using firewalls, intrusion detection systems, data leakage prevention (DLP), anti-virus walls and anti-virus software and other information security measures, it also introduces a network attack defense system. To detect advanced threats and targeted attacks entering and exiting the network, such as malicious programs, behind-the-scenes manipulation (C&C) communications, and hidden hacking activities that cannot be detected by standard information security protection to improve the level of information security. In addition, the load balancing system and high availability architecture design are adopted to ensure the system availability.

Information Security Related Management Measures		
Categories	**Descriptions**	**Relevant operations**
Privilege management	The management systems over User ID, privilege management and behaviors of system operations	• Privilege management and review over User ID • Periodical inventory check over the privilege of User ID
Access control	The control measures for the entire personnel in access to internal and external systems and information transmission channels.	• The control measures over the access to internal and external systems • Control over sensitive information from being divulged • Operation behavior track record
External threats	Potential internal vulnerability, virus channels and protective measures thereof	• Host/computer vulnerability protection and update measures • Protection against virus and malware detection • Source code inspection/penetration testing • Cyber threat monitoring
System availability	System availability status and countermeasures against an event of service interruption	• Use high-availability architecture for important systems. • System/network availability monitoring and reporting mechanism • Contingency countermeasures against interruption of services • Information backup measures, principal site/offsite backup mechanism • Disaster restoration drills or exercises on a regular basis