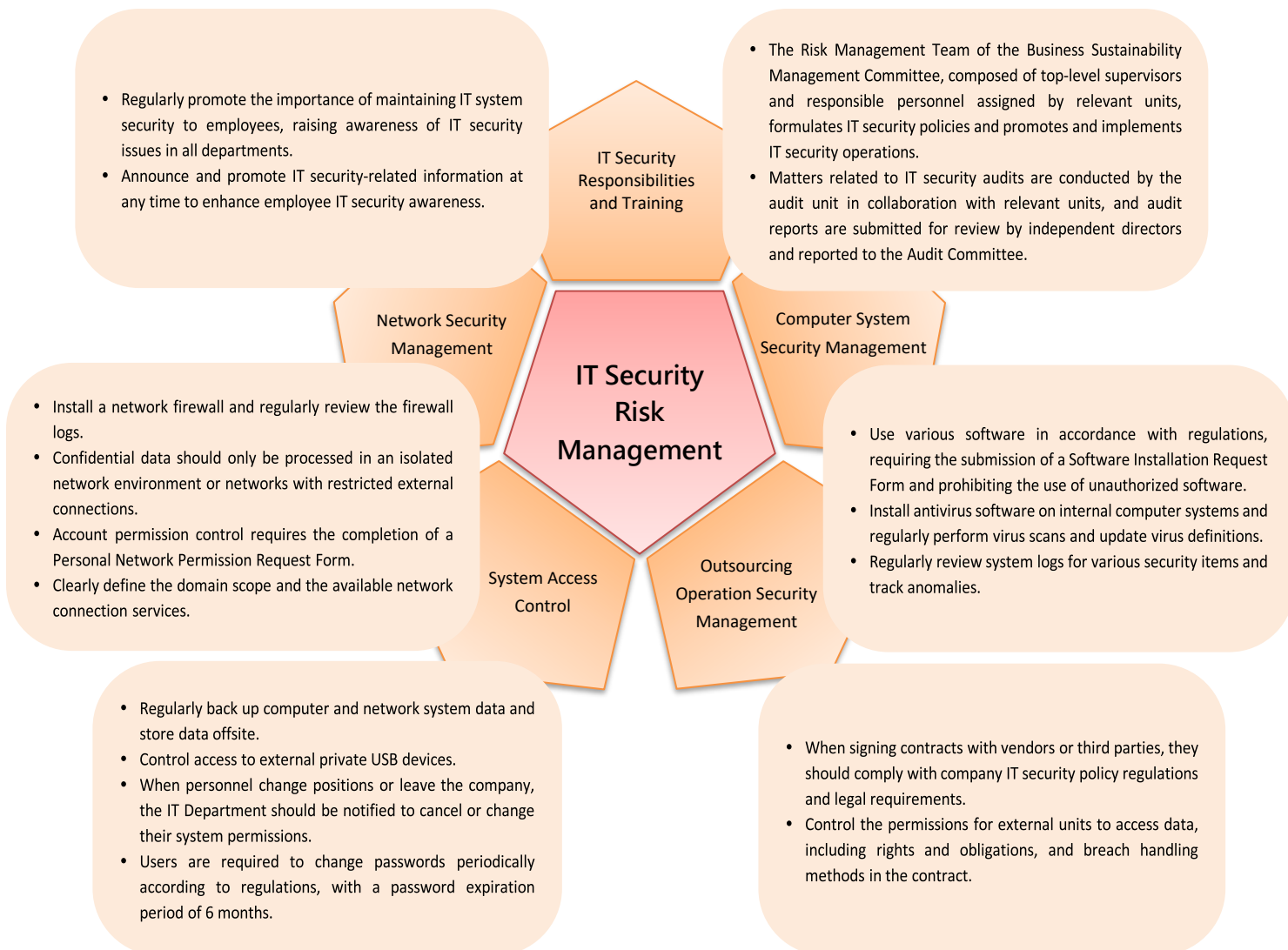# IT Security Risk Management

IT Security

To strengthen IT security management and uphold the confidentiality, integrity, and availability of our company's critical IT systems, we have internally established multiple IT security regulations and policies to govern the IT security practices of our company personnel. We conduct annual reviews to ensure that these regulations align with the evolving operational environment and make necessary adjustments as required to establish a secure and dependable technology industry.

Management regulations related to IT security policies include:

Access control for programs and data	Control of data input and output operations	Control of data processing operations	Security control of files and equipment
Procurement, usage, and maintenance control of hardware and system software	Procedure control of system recovery planning and testing	Control of IT security inspections	Control of public data

IT Security Risk Management Framework

- Regularly promote the importance of maintaining IT system security to employees, raising awareness of IT security issues in all departments.
- Announce and promote IT security-related information at any time to enhance employee IT security awareness.

IT Security Responsibilities and Training

- The Risk Management Team of the Business Sustainability Management Committee, composed of top-level supervisors and responsible personnel assigned by relevant units, formulates IT security policies and promotes and implements IT security operations.
- Matters related to IT security audits are conducted by the audit unit in collaboration with relevant units, and audit reports are submitted for review by independent directors and reported to the Audit Committee.

Network Security Management

Computer System Security Management

IT Security Risk Management

- Install a network firewall and regularly review the firewall logs.
- Confidential data should only be processed in an isolated network environment or networks with restricted external connections.
- Account permission control requires the completion of a Personal Network Permission Request Form.
- Clearly define the domain scope and the available network connection services.

- Use various software in accordance with regulations, requiring the submission of a Software Installation Request Form and prohibiting the use of unauthorized software.
- Install antivirus software on internal computer systems and regularly perform virus scans and update virus definitions.
- Regularly review system logs for various security items and track anomalies.

System Access Control

Outsourcing Operation Security Management

- Regularly back up computer and network system data and store data offsite.
- Control access to external private USB devices.
- When personnel change positions or leave the company, the IT Department should be notified to cancel or change their system permissions.
- Users are required to change passwords periodically according to regulations, with a password expiration period of 6 months.

- When signing contracts with vendors or third parties, they should comply with company IT security policy regulations and legal requirements.
- Control the permissions for external units to access data, including rights and obligations, and breach handling methods in the contract.

IT Security Incident Reporting SOP