Ping An Group Information Security Policy

Information security management is crucial to Ping An's business development. As the scale of information systems and data acquisition and management continues to expand, strict information security management has become a critical safeguard for the sustainable development of Ping An.

Ping An strictly follows and implements relevant laws and regulations, and continuously adjusts existing information security management based on market regulatory changes and technology updates. The latest version of the Information Security Management Regulations contains 6 categories of 22 specification documents, including Information Security Policy, Information Security Standards, Information Security Procedures, Information Security Baseline (usually applicable to IT systems), and Guidelines and Codes. The information security system applies to all parties of Ping An, employees of subsidiaries, and third-party personnel who have access to information assets. Ping An has adopted a series of behavior control and security protection methods, including employee online operation management, print control, document and hard disk encryption, and watermark tracking.

After decades of continuous improvement of practices, Ping An has always adhered and implemented to the highest standards to support information business development.

Commitment

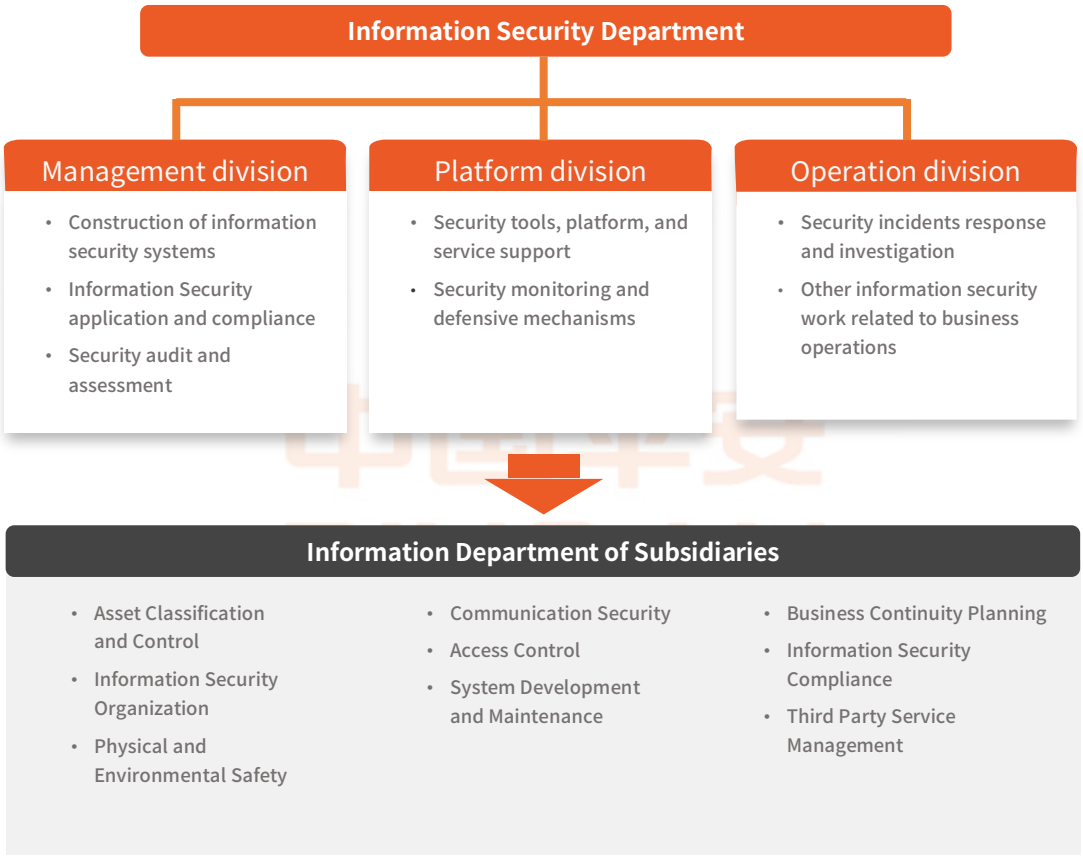
Ping An pledges to establish and implement the highest standards of information security according to industry standards, and:

1. Abide by the highest information security standards in accordance with respective laws, regulations, and industry standards and codes;
2. Provide sound information protection to ensure its confidentiality, integrity and accessibility;
3. Build information and information security controls systems based on in-depth defense and default secured standards;
4. Establish information and information systems according to its sensitivity, value and importance.

Management

Ping An's Information Security Department coordinates all information security related work. It utilizes three sub-departments to ensure effective implementation of the relevant regulations. To

achieve the highest industry standards, the development of information security management strictly abides by national laws, complies with regulations established by authorities, including the China Banking and Insurance Regulatory Commission, China Securities Regulatory Commission and Cyberspace Administration of China and Ministry of Public Security. The following structure demonstrates the Ping An information security management framework scope and 9 focuses.



We have established a Group Information Security Response Center and built several platforms for information security risk management of Group functions and businesses. These resources detect threats to information security, execute rapid response actions and enable us to provide customers with guarantees regarding secure information security. Ping An's Information Security Management System has been certified with ISO 27001 at group level. We regularly conduct internal and external audits of our information security management and data privacy protection. Those audit results are reported to the Audit and Risk Management Committee under the Group's Board of Directors.

Information Security Principles and Measures

Ping An has formulated information security management principles and measures covering 9 categories of information security, based on laws and regulations in the industry, with the highest standards.

1 Asset Classification and Control

- All information assets, including but not limited to written, oral, and electronic information, should be classified and identified based on their sensitivity, importance, and access restrictions.
- Important assets should be marked on the assets list, which is maintained and updated on a timely basis.

2 Information Security Organization

- All jobs or tasks with information security implications define information responsibilities descriptions and indicate the sensitivity of the information involved.
- Employees must pass ethical integrity screening and sign a confidentiality agreement before coming on board. Relevant procedures must be followed to ensure the protection of information assets when staff changes position or leaves the company.
- Employees who violate information security regulations will be subject to penalties.

Every year, we provide training to all employees on topics such as data security and customer privacy to further enhance their awareness and ability in protecting information and data security. All subsidiaries conduct business information security training for all employees under the Group's guidance.

3 Physical and Environmental Safety

- Ping An has adopted strict physical security precautions to prevent information from unauthorized access, destruction and interference. In preparation for possible natural disasters and man-made accidents or incidents, Ping An has implemented corresponding physical environmental protection measures.

4 Communication Network Security

- All networks connected to Ping An have taken appropriate security measures to protect the internal network, information, information systems and ensure the security in data transformation.
- Eliminate illegal intrusion and data leakage through network access authentication, network isolation by security classification, transmission channel encryption and various network security protection technologies.
- Adopt DDoS defense (Distributed Denial of Service), terminal DLP (Data leakage prevention), mail DLP, Access Gateway and other security measures to mitigate security threats and block data leakage.

5 Access Control

- Accountability: All actions must be recorded to be traceable; unauthorized actions are handled according to relevant policies.
- Authentication: Users need to be authenticated before accessing information systems. The authentication method is compatible with the sensitivity and risk of the information.
- Authorization: Users are to follow the minimization principle and are only permitted to

access necessary information.

- Confidentiality: Information assets must be properly protected according to their information classification. The sharing of classified and confidential information must pass necessary authorization.
- Integrity: Information must be protected from unauthorized tampering, damage or destruction.
- Responsibilities: A single person cannot handle the entire business transaction or operating procedure on their own. High-risk functions must take effective monitoring measures, including 'spin-off' process, process rotation, enforcement checks and other approval procedures.

6 System Development and Maintenance

- Implement security regulations should be strictly followed during application development, release and updates. E-commerce applications should be designed to protect the confidentiality and integrity of customer information in the public network environment and ensure the non-repudiation of the transaction.
- The encryption algorithm used must meet the principles of data protection, including: achieving the confidentiality, integrity, authentication and non-repudiation and has been publicly verified. The encryption key must be properly managed throughout the key life cycle.
- Adopt strong identity authentication methods such as two-factor authentication for important systems, and strictly abide by the *knowing its necessity* principle to prevent internal data theft. At the same time, advanced technology is used to strengthen system log auditing, discovery and track data leakage.

7 Business Continuity Planning

Ping An has established appropriate measures to ensure that information is available to authorized users. In the case that the original data is destroyed or lost, the most recent backup information is extracted to achieve continuity of the service.

8 Information Security Compliance

Ping An protects customer information and privacy, and strictly follows information security requirements in accordance with the highest standards in laws, regulations, and contractual requirements.

9 Third Party Service Management

Ping An has cooperation with partners in the area of information. In response to third-party service management, Ping An has established clear regulations to ensure that procurement and partnerships are in compliance with the relevant regulatory authorities.

In the era of information, achieving information security is an important guarantee for Ping An to implement sustainable development strategy. In order to provide safe and reliable products and

services, we will upgrade relevant systems and technologies continuously, and strengthen management and training to achieve the commitments on information security.