PING AN
Finance · Technology

Expertise Makes Life Simple

Policy Statement on Information Security of Ping An Group

Jan, 2022

This policy applies to all member companies and functional departments of Ping An Insurance (Group) Company of China, Ltd.

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 standards based on regulatory changes and technology updates. The latest version of the Company's Information Security Management Regulations contains 22 specification documents in 6 categories, namely Information Security Policy, Information Security Standards, Information Security Procedures, Information Security Baseline (usually applicable to IT systems), and Guidelines and Codes. The Regulations apply to employees of all departments of Ping An Group and its member companies, and third-party personnel who have access to information assets. The information security system is evaluted by external consuting companies every two years. 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 to strengthen employees' online operation management.

With more than ten years of continuous improvement of practices, Ping An has implemented the Regulations to the highest standards to support information business development.

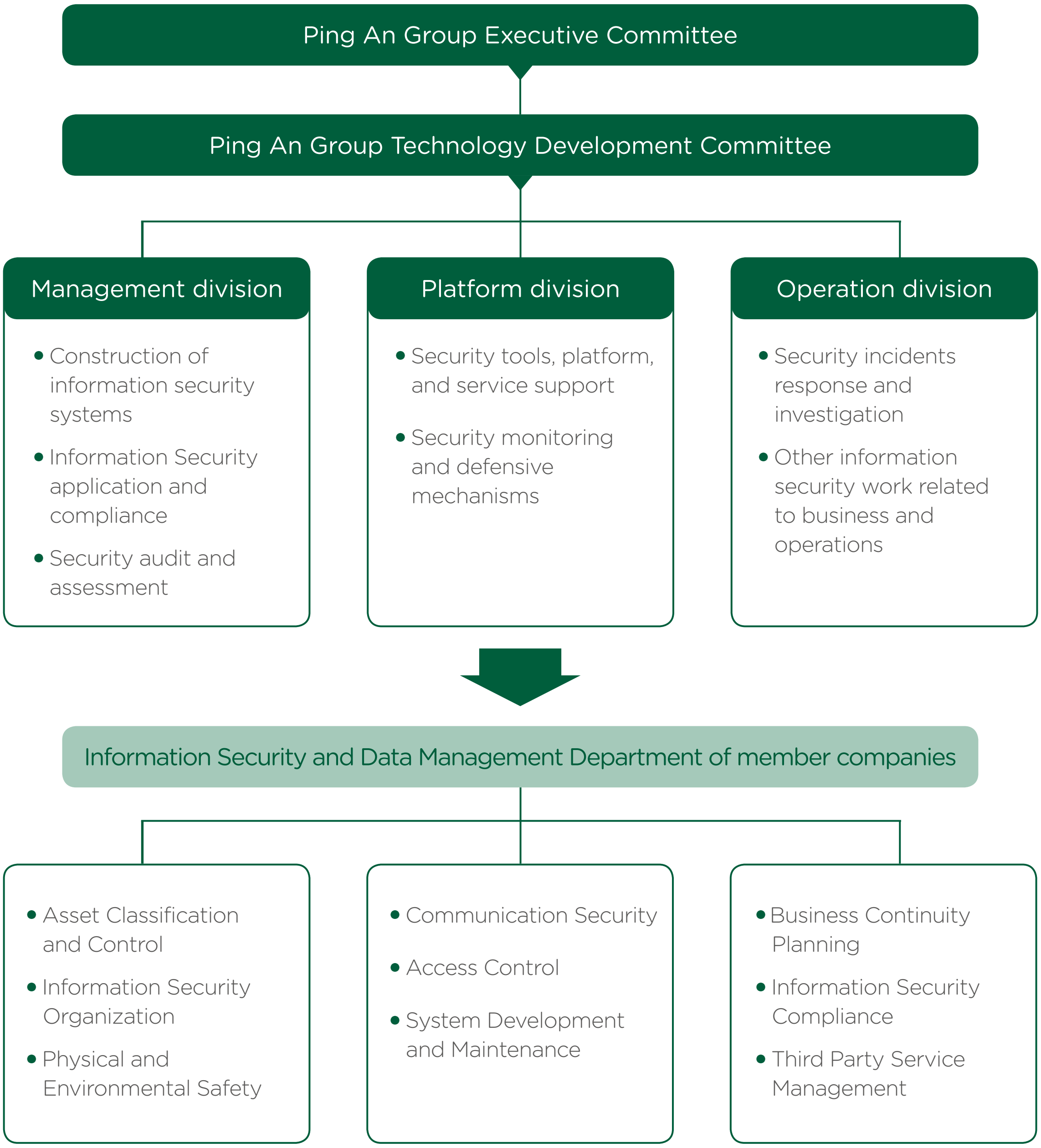
Commitment

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

- Abide by the highest information security standards in accordance with respective laws, regulations, and industry standards and codes;
- Provide sound information protection to ensure information confidentiality, integrity and accessibility;
- Build information and information security controls systems based on Defense in Depth (DiD) and Secure by Default standards;
- Protect information and information systems according to its sensitivity, value and importance.

Management

Ping An's Information Security Department under the Group's Technology Development Committee 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 (CBIRC), China Securities Regulatory Commission (CSRC), Cyberspace Administration of China (CAC) and the Ministry of Public Security. The following structure demonstrates the Ping An information security management framework, work scope and nine key catogories.



Ping An Group Executive Committee

Ping An Group Technology Development Committee

Management division

- Construction of information security systems
- Information Security application and compliance
- Security audit and assessment

Platform division

- Security tools, platform, and service support
- Security monitoring and defensive mechanisms

Operation division

- Security incidents response and investigation
- Other information security work related to business and operations

Information Security and Data Management Department of member companies

- Asset Classification and Control
- Information Security Organization
- Physical and Environmental Safety

- Communication Security
- Access Control
- System Development and Maintenance

- Business Continuity Planning
- Information Security Compliance
- Third Party Service Management

Ping An has established a Group Information Security Response Center and built business security and risk management platforms to detect threats to information security, execute rapid response actions and provide users with secure guarantees regarding information security. Ping An's Information Security Management System has been certified with ISO 27001. We regularly conduct internal and external audits of our information security management and data privacy protection. Those audit results are reported to the Board of Directors, the Executive Committee, and the Risk Management Committee of the Group.

Information Security Principles and Measures

Ping An has formulated information security management principles and measures covering nine key categories based on laws,regulations and industry standards.

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.

Information Security Organization

- All jobs descriptions must include a description of information safety responsibilities and indicate the sensitivity of the information involved.

- Employees must pass ethical integrity assessment 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 and outsourced personnel on topics such as data security and customer privacy to further enhance their awareness and ability in protecting information and data security. Meanwhile, all member companies provide targeted business information security training in line with business practices under the Group's guidance.

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.

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 (Data loss prevention), Access Gateway and other security measures to mitigate security threats and block data leakage.

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 process splitting, process rotation, enforcement checks and other approval procedures.

System Development and Maintenance

- Implementation of 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 grant access strictly on a need-to-know basis to prevent internal data theft. At the same time, advanced technology is used to strengthen system log auditing, and track and identify data leakage.

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.

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.

Third Party Service Management

- Ping An has cooperation with partners in the area of information. For the 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 information age, 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, Ping An will upgrade relevant systems and technologies continuously, and strengthen management and training to achieve our commitments on information security.

This policy is interpreted and revised by Ping An Group, and will be updated in due course according to national policies, regulatory requirements and industry development.