PING AN
Expertise Creates Value

Expertise Makes Life Simple

Policy Statement on Information Security of Ping An Group

September, 2025

This policy statement applies to the Ping An Insurance (Group) Company of China, Ltd.

As Ping An Group advances its comprehensive digital transformation, the digital business landscape becomes increasingly diverse. With this evolving landscape, information security has become a crucial cornerstone for Ping An to achieve sustainable development. Ping An commits to managing information security risks with high standards to ensure the secure and reliable operation of the information systems across the entire Group. This commitment provides a solid foundation for offering diverse products and convenient services to customers in all business sectors.

Scope of Application

This policy statement applies to Ping An Insurance (Group) Company of China, Ltd. (hereinafter referred to as “the Group”, "the company"). Each member company may establish its own policy statement in conjunction with this policy statement.

Commitment

Ping An commits to conducting information security management at high standards, which includes:

- 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 control systems based on Defense in Depth (DiD) and Secure by Default standards;
- Protect information and information systems according to its sensitivity, value, and importance.

Information Security Management Framework

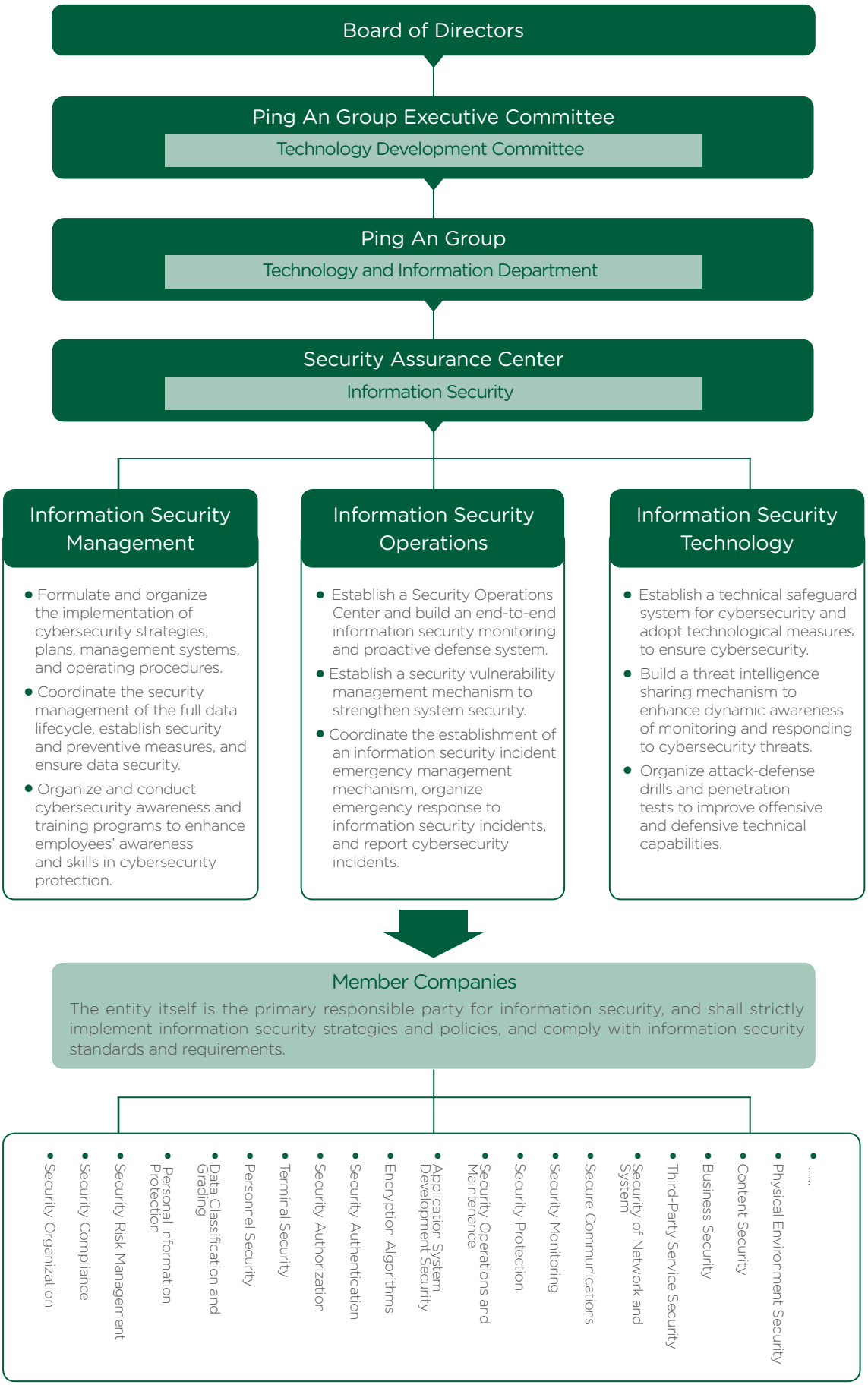
The Group has established a network and data security accountability system, under which the Board of Directors assumes primary responsibility for network and data security. The Board of Directors implements national laws, regulations, and policy requirements on cybersecurity, defines the Group's cybersecurity objectives, reviews cybersecurity strategies and plans, and supervises their implementation.

The Group Executive Committee has established a Technology Development Committee, which undertakes the overall functions of coordinating the Group's technology development strategy and major initiatives in the field of technology. It is responsible for formulating major strategies and key systems in the field of technology, and, upon approval by the Executive Committee, leading, supervising, monitoring, and guiding the implementation of relevant work by the Group and its member companies.

The Group Technology and Information Department serves as the Group's competent authority for information security. It is responsible for overall planning, organization, and coordination of information security at the Group level, and for reporting significant information security matters to the Board of Directors or its authorized committee, as well as to senior management.

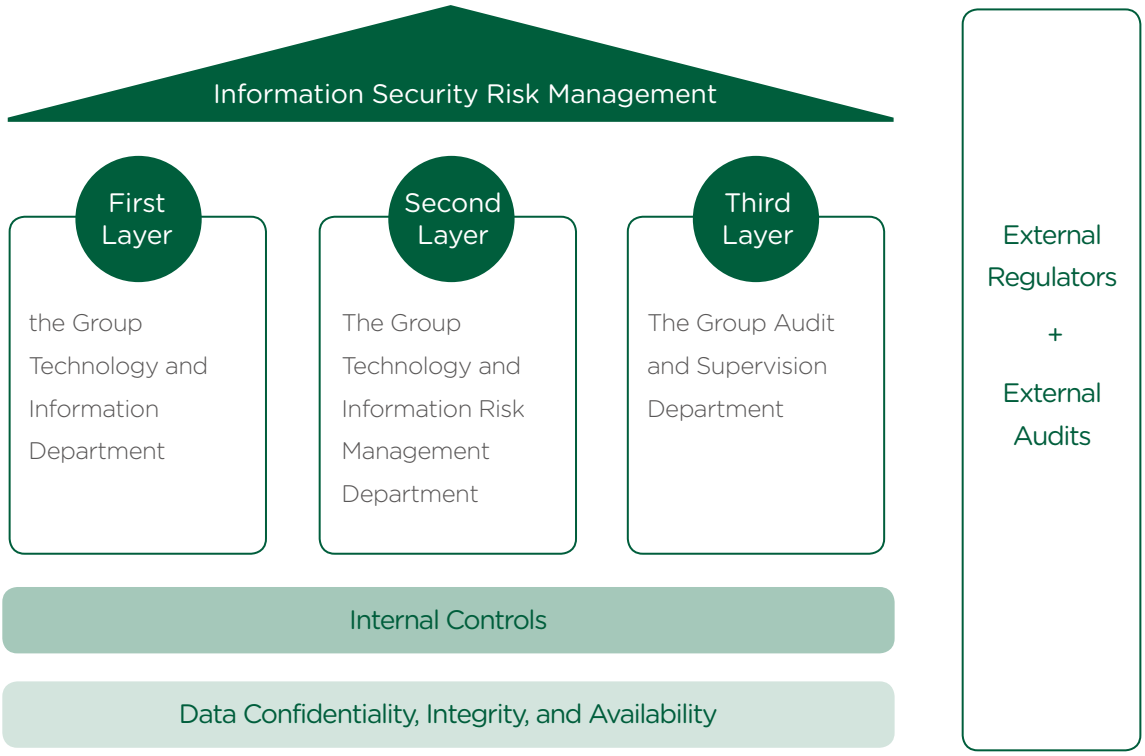
Each member company is the primary responsible entity for information security within its own organization. Member companies shall strictly implement information security strategies and policies, and comply with information security standards and requirements. Each member company has designated personnel responsible for network security, data security, and personal information protection, and ensure accountability in these areas. Member companies shall fulfill their obligations on information security, implement specific control strategies, and ensure data confidentiality, integrity, and availability.

The Ping An information security management framework and its main scope of work are outlined as follows.


Board of Directors
Ping An Group Executive Committee
Technology Development Committee
Ping An Group
Technology and Information Department
Security Assurance Center
Information Security
Information Security Management
Formulate and organize the implementation of cybersecurity strategies, plans, management systems, and operating procedures.
Coordinate the security management of the full data lifecycle, establish security and preventive measures, and ensure data security.
Organize and conduct cybersecurity awareness and training programs to enhance employees' awareness and skills in cybersecurity protection.
Information Security Operations
Establish a Security Operations Center and build an end-to-end information security monitoring and proactive defense system.
Establish a security vulnerability management mechanism to strengthen system security.
Coordinate the establishment of an information security incident emergency management mechanism, organize emergency response to information security incidents, and report cybersecurity incidents.
Information Security Technology
Establish a technical safeguard system for cybersecurity and adopt technological measures to ensure cybersecurity.
Build a threat intelligence sharing mechanism to enhance dynamic awareness of monitoring and responding to cybersecurity threats.
Organize attack-defense drills and penetration tests to improve offensive and defensive technical capabilities.
Member Companies
The entity itself is the primary responsible party for information security, and shall strictly implement information security strategies and policies, and comply with information security standards and requirements.
Security Organization
Security Compliance
Security Risk Management
Personal Information Protection
Data Classification and Grading
Personnel Security
Terminal Security
Security Authorization
Security Authentication
Encryption Algorithms
Application System Development Security
Security Operations and Maintenance
Security Protection
Security Monitoring
Secure Communications
Security of Network and System
Third-Party Service Security
Business Security
Content Security
Physical Environment Security
.....

Information Security Risk Management

Ping An's information security management system consists of three layers of defense, each with different information security roles and responsibilities. Every individual of Ping An takes a collective responsibility to protect information assets.



First Layer

The first layer of defense consists of the Group Technology and Information Department and other departments of the Group. The Group Technology and Information Department is responsible for formulating and organizing the implementation of network and data security plans, management systems, and operating procedures.

Second Layer

The second layer of defense is the Group Technology and Information Risk Management Department, which is primarily responsible for establishing mechanisms for the identification, assessment, and monitoring of network and data security risks, and for organizing their implementation.

Third Layer

The third layer of defense is the Group Audit and Supervision Department, which is responsible for organizing and carrying out specialized security audits and supervising the rectification of identified issues.

Information Security Principles and Measures

Ping An has formulated information security management principles and measures based on laws, regulations, and industry standards. These are focused on security management, security operations, and security technology and consist of 12 key categories.

01. Security Organization and Personnel

- Establish a clear network and data security execution team, set up dedicated positions for network and data security management and technology, and ensure that relevant personnel have the necessary professional knowledge and skills.
- Implement corresponding cybersecurity controls before, during, and upon employment changes or termination to reduce the harm to information assets caused by human fraud, theft, and incorrect operations.
- Conduct at least one cyber security education and training session per year for all staff (including full-time employees and third-party personnel), to enhance employee awareness and level of cyber security protection. The company requires employees to actively identify cyber security risks, report cyber security incidents promptly for escalation, creating an environment where everyone works together to maintain cyber security.
- All employees must comply with this policy statement and other information security regulations, and hold the responsibility for maintaining information security and data protection. Any person who violates the company's information security system will be punished in accordance with the latest *"Red, Yellow, and Blue" card punishment system*, and for particularly serious behaviors, legal responsibility will be pursued.

02. Information Security Compliance

- Protect customer information and privacy, and strictly follow information security requirements to protect the legitimate rights and interests of the state, citizens, legal persons, and other organizations.
- Comply with obligations such as cyber security classification protection, protection of critical information infrastructure, security evaluations of commercial cryptography applications, and network security reviews.

03. Security Risk Assessment and Certification

- Conduct at least one cybersecurity risk assessment annually to identify and evaluate the effectiveness of existing risk control measures, and address any issues promptly.
- Carry out data security risk assessment, monitoring, and handle in conjunction with data processing scenarios, conducting a comprehensive data security risk assessment on annual basis to ensure the safe and stable development of data utilization activities.
- Actively promote certification for information security management system standards applicable to business operations, including but not limited to ISO/IEC 27001, ISO/IEC 27017, ISO/IEC 27018 and others.

04. Full Lifecycle Protection of Data Security

- Build cybersecurity controls at each stage of the full lifecycle, including data collection, transmission, storage, use, exchange, and destruction, to ensure that data-related activities are legal and compliant, necessary, auditable, and traceable.

05. Security of Third-Party Services

- Implement procurement management, classification and grading, contract terms, monitoring and evaluation, risk management, regulatory reporting, etc., to ensure the information security and controllability of third-party services. At the same time, clearly define information security-related clauses in contracts with third parties, including but not limited to data protection, access control, security incident response, reporting and escalation, etc.
- Conduct regular information security assessments of third parties, which include but are not limited to security management systems, personnel security, data security, security protection, emergency response and handling, etc.; conduct annual due diligence on suppliers through questionnaires and other means, and perform on-site audits for key suppliers.

06. Security Authentication and Authorization Management

- Users need to be authenticated before accessing information and information systems. The authentication method is compatible with the sensitivity and risk of the information. Passwords have a validity period and must be changed at least every 90 days. Weak passwords are prohibited.

For high-risk systems such as centralized systems and business systems accessible from the external network, measures such as whitelist access mechanisms and two-factor authentication are adopted to enhance security protection.

- Follow the minimization and need-to-know principles in terms of permission management, and only permit to access necessary information. No individual is allowed to handle the entire business transaction or operating procedure alone.

07. System Development Security and Maintenance

- Establish application security standards and control processes covering the software development lifecycle to strengthen security management. Conduct requirement analysis, security plan reviews, source code security checks, component risk assessments, and security testing. Systems will not be put into production if they fail the security tests.
- In terms of vulnerability management, establish a closed-loop mechanism for handling vulnerabilities at different levels, clearly defining the timeframes for addressing vulnerabilities of various levels. Set up mechanisms for monitoring and proactively identifying vulnerabilities through penetration testing and red-blue confrontations to promptly discover and fix cybersecurity vulnerabilities, improving system security.
- Establish security baselines for servers, network devices, operating systems, databases, middleware, etc., and strengthen their management and maintenance. Verify and update the effectiveness of security baselines and security configuration policies.

08. Regional Boundaries and Communication Security

- Use isolation techniques to divide the network into external networks, DMZ, and internal networks. Deploy appropriate access control mechanisms at network boundaries and set access control rules to prevent network intrusion attacks.
- Implement different security communication rules for different network regions. All connections to the company network must incorporate appropriate security measures to protect internal networks, information, and information systems. Sensitive information must be encrypted using recognized encryption technology before it can be transmitted over the Internet.

09. Security Monitoring and Protection

- Implement a 7x24 cybersecurity monitoring and operations mechanism, employ a combination of proactive and passive defense measures to maintain system information security. It monitors and records information activities and manages the entire process of information security incidents, ensuring that all significant accesses and operations within Ping An's information systems are recorded. This guarantees traceability of sensitive activities within the system, allowing for precise attribution to responsible individuals.
- Develop a comprehensive cybersecurity incident emergency management system along with contingency plans that cover various cybersecurity emergency scenarios. Clearly define the organizational structure and mechanisms for emergency responses and implement specific requirements for incident handling. Specify the procedures for employees incidents reporting and escalation, adopting a one-click reporting feature via email. Regularly review and update contingency plans, and conduct at least one cybersecurity emergency drill annually to enhance the capability to respond to various cybersecurity incidents. In the event of a cybersecurity incident, report it according to regulatory requirements and notify relevant parties as necessary.
- In terms of network intrusion, deploy network security devices such as DDoS, IPS, and WAF according to the network security risk situation. It also deploys security platforms/tools like APT situational awareness defense systems and honeypot systems to provide comprehensive security monitoring, analysis, warning, and response.
- Regarding threat intelligence, establish a security emergency response platform and implement threat intelligence systems. It collects information related to threats to information security, conducts analysis and investigation, issues security warnings, and tracks the progress of remediation.

10. Terminal Security

- Implement terminal security control measures and strategies to enhance monitoring, blocking, and tracing of various non-compliant activities.

11. Business and Content Security

- Establish security controls for high-risk operations such as user registration, password reset, and device binding, ensuring the authenticity and non-repudiation of transaction identities and device information, and continuously strengthen monitoring and response to unusual transaction behaviors.

- Establish an information content security review management mechanism, following the principle of "review before publication". This involves actively filtering and monitoring content to identify and proactively block illegal and undesirable content to ensure the legality, accuracy, and authenticity of information and maintain a healthy online environment.

12. Physical and Environmental Safety

- Adopt 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, such as fire, flood damage, riots, and more, implement corresponding physical environmental protection measures.

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.