Policy Statement on Information Security Management of Lufax Holding Ltd.

This policy is interpreted and revised by Lufax Holding Ltd and will be updated in response to developments in national policies, regulatory requirements and industry practice in due course.

General

Lufax Holding Ltd. (hereinafter referred to as “Lufax” or “the Company”) has rich business scenarios and massive real data, and information security management is the most critical part in its business development. As the information system and the data grow, strict information security management standards become an important guarantee for the stable and sustainable development of Lufax. Lufax establishes an information security risk management system to ensure the secure and reliable operation of the Company’s information system, thus providing a solid guarantee for each business department to deliver diversified products and convenient services to customers.

Applicable Scope

This policy statement applies to all departments and employees of Lufax and its member companies, as well as all third-party personnel who have access to information assets, covering all business segments of Lufax.

Commitment

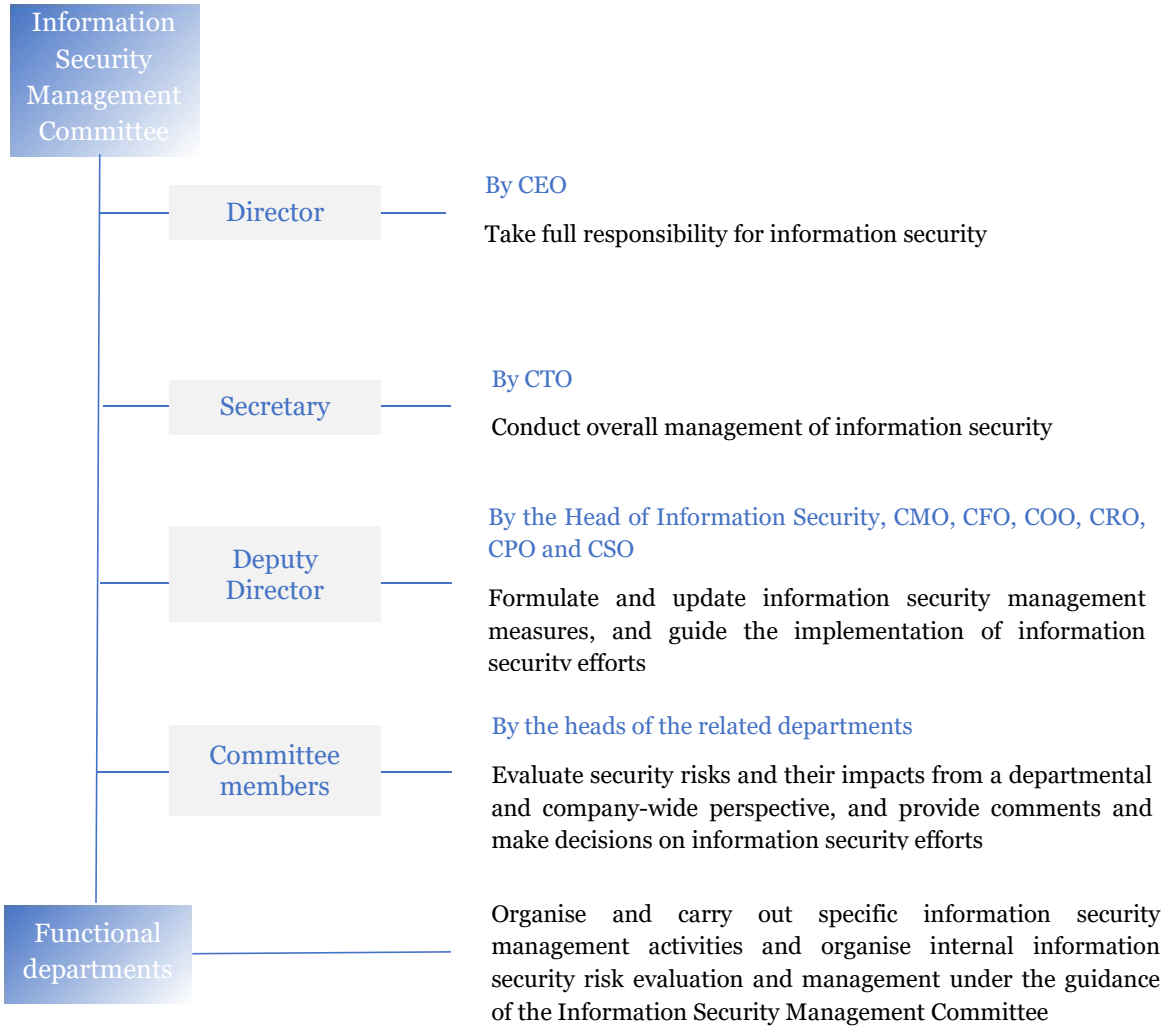
Lufax commits to:

- strictly complying with the information security requirements set out in national laws, regulatory provisions and industry standards and codes;
- ensuring that the information is properly protected to guarantee its confidentiality, integrity and availability;
- adopting defence in depth and security by default as the implementation principles for security controls for the information and the information system; and
- ensuring that the information and the information system are protected in accordance with their sensitivity, value and materiality.

Information security management structure

At Lufax, the Co-CEO is the most senior leader responsible for involving the Information Security Management Committee under the Executive Committee of the Company to ensure and supervise the effective and continuous implementation of information security management measures.

The framework and main work scope for information security management of Lufax are illustrated as follows:



Information Security Principles and Measures

Based on relevant laws and regulations and industry standards, Lufax has clarified the principles and the measures of information protection, and has defined 12 prior tasks with respect to security management, security operation and security technology.

1. Asset Security and Data Classification and Grading

- All information assets, including written, oral and electronic information, should be classified and labelled according to their sensitivity, materiality and the principle of access restriction required by the business;
- All important assets related to information should be marked in the list of assets, and be maintained and updated in time;
- Data should be classified and graded according to the principles and rules of data classification and grading, and different levels of data should be subject to corresponding confidentiality protection.

2. Security Organisation and Personnel Security

- Security responsibilities must be described for all positions, and the sensitivity of the positions should be clarified;
- Employees must pass a character test and sign a confidentiality agreement before joining the Company, and relevant procedures must be implemented when an employee changes position or leaves the Company, to ensure that the protection of information assets is not compromised;
- Any employee who violates the information security system will be punished in accordance with the latest version of the Red, Yellow and Blue Card Punishment Regulations, and Lufax will take legal action against particularly serious behaviours;
- In respect of information security awareness promotion, all new employees are required to complete the orientation training for information security within three months after joining the Company. Besides, Lufax provides training on information security for all employees (including part-time) and contractors every year, covering data security, personal information protection, terminal security and other security areas, so as to comprehensively strengthen employees' information security protection awareness and skills.

3. Authentication and Authorisation

- Authentication

  Before accessing information and the information system, users must pass the identity authentication in a manner appropriate to the sensitivity of the information and the level of risk.

- Authorisation

  Only the necessary authority is granted in accordance with the principle of minimising authority and the need-to-know principle.

- Segregation of duties

  No one is allowed to handle an entire business transaction or a process alone. High-risk functions must be subject to effective monitoring measures, such as splitting process, process rotation, mandatory review and approval procedures.

4. System Development and Maintenance

- Security rules should be followed during the development, releasing and update of application systems. The development of e-commerce application system should ensure the confidentiality and integrity of customer information in public network environment, as well as the non-repudiation of transactions;
- The encryption algorithm applied must comply with the principles of data protection. In particular, the encryption algorithm should meet the requirements for protecting the confidentiality, integrity, authentication and non-repudiation of data; the encryption algorithm selected must be publicly demonstrated; and the encryption key must be properly managed throughout its lifecycle;
- Two-factor authentication and other strong identity authentication means should be applied to important business systems. The authorisation management principle of “minimum authorisation and need-to-know” should be strictly abided by to avoid internal data theft; and advanced technical means should be applied to strengthen the system log audit, as well as to track and identify data leakage behaviours;
- During the operation and maintenance, relevant changing procedures must be implemented to prevent malicious or accidental unauthorised tampering or deletion of information.

5. Security Monitoring and Protection

- By taking proactive and reactive measures to protect the security of the system

and information, Lufax monitors and records information-related activities, and conducts full-process operation management for information security incidents, so as to ensure that all critical access and operations to Lufax information systems are logged and that sensitive actions in the system are traceable and can be accurately traced back to the responsible performers. Meanwhile, the security operation platform developed by Lufax enables the Company to monitor the risk scenarios concerning network, host, terminal, application, data base, employee and public opinion, and to alert and deal with the identified information security incidents in time.

6. Network Boundary and Communications Security

- Configure access control mechanism at the network boundary based on the differences between network zones, and set access control rules;
- Monitor the performance, traffic and illegal access of network, and timely handle or report the exceptions.
- Formulate appropriate preventive measures against malicious or accidental unauthorised tampering with or deletion of information assets;
- It is necessary to take proper security measures for all lines connected to Lufax network to protect the internal network, information and information system of the Company, and it is especially important to control the connection to public network and networks not managed by Lufax;
- Major networks and operating systems must be critically patched in due time; and new operating systems must be configured with the latest patches;
- All servers, workstations and appropriate equipment must be installed with anti-virus and anti-surveillance software, and anti-virus systems must be upgraded and virus databases updated in a timely manner in order to prevent attacks by malicious codes.

7. Business Continuity Plan

- Lufax has developed proper prevention measures. When the original information is lost or corrupted, the latest backup information can be extracted in time to ensure business continuity.

8. Information Security Compliance

- Lufax strictly adheres to the information security requirements specified by laws, regulations, industry practices and codes, with the highest standards as the principle of implementation. The Company protects customer information and privacy in accordance with the requirements of laws, regulations and

contracts;

- Lufax strictly undertakes obligations such as graded protection, critical information infrastructure protection, commercial cryptographic application security assessment and cybersecurity review;
- For websites, APPs, applets, etc., apply for Internet information service domain name registration or licensing procedures with the regulatory authorities in accordance with the law, and display the registration number or telecommunication business license number in a conspicuous position on the homepage of the website or APP.

9. Information Security Audit and Certification

- Lufax conducts an internal audit of the information security management system is performed at least once a year, and the audit results are reported to the Board of Directors and the Information Security Management Committee of the Company;
- Lufax conducts an independent external audit of information security at least once a year, as well as specific audits and reviews in accordance with the management regulations and requirements of regulators;
- Lufax actively promotes the certification of information security management system standards applicable to its business, including but not limited to ISO 27001.

10. Supplier and Third-Party Information Security Management

- Lufax manages information security matters for supplier and third-party services with high standards. Suppliers refer to legal market entities or other organisations that directly or indirectly provide products or service resources to Lufax in the procurement process. Third-party service personnel include, but are not limited to employees of outsourcing companies, agents, vendor engineers, consultants from consulting companies, etc. Based on the core principle of “keeping sensitive data inside Lufax” and in accordance with relevant laws and regulations, Lufax has formulated and implemented management systems such as Information Security Standards - Third-Party Service Management in light of the actual business situation. At the same time, the Company does not rent, sell, or provide personal data to third parties for purposes other than completing transactions/services;
- Lufax regularly conducts information security and privacy protection compliance assessment for suppliers and third parties. The items under

assessment include, but are not limited to data storage, management systems, technical measures, access rights, disaster recovery facilities and emergency management systems. Lufax also conducts supplier due diligence through questionnaires and other means every year, and performs on-site audit of key suppliers.

11. Content Security

- With the establishment of information content security review management mechanism, Lufax follows the principle of "disclosing information after review" and identifies illegal information and misconducts to block the illegal and harmful information, so as to ensure the legality, accuracy and authenticity of information and maintain a good order of network communication.

12. Physical and Environmental Security

- Lufax takes strict physical security precautions against unauthorised physical access, damage or interference to information assets and information systems. Besides, Lufax has designed and implemented appropriate physical environmental protection measures for the impact of natural, accidental or man-made disasters such as fire, flood and riot on information equipment.