Chailease Holding Company Limited.

Guidelines for Information Security Management

Date: _____/_____/_____ Approved by Chairman of the board

I. Purpose

1. The Company sets forth these Guidelines in order to strengthen the information security management and establish a reliable information operating environment to ensure the Company's rights and interests.

II. General Rule

2. The “Company” in the Guidelines, is referring to Chailease Holding and its affiliates.
3. The Company may conduct information security risk assessment in accordance with relevant laws and regulations to determine the level of information security requirements, and adopt appropriate measures to ensure the security of the Company's data operation.
4. Regarding the “appropriate measures” in the Guidelines, the risk level of each information asset and the degree of impact or harm to the Company's operation shall be comprehensively considered, and adopt commensurate and cost-effective information security measures.
5. The Company shall set relevant regulations and regularly evaluate the implementation results for the following information security measures:
   (1) The formulation of information security policy.
   (2) The responsibility division of information security.
   (3) The security management of computer system.
   (4) The security management of network.
   (5) The management of system access control.
   (6) The security management of system development and maintenance.
   (7) The security management of information assets.
   (8) Physical and environmental security management.
   (9) Sustainable business operation program.
   (10) Laws and operations compliance.

III. The Formulation of the Information Security Policy

6. The Company shall set relevant information security policy in accordance with actual business needs, and notify relevant personnel to comply with the policy in writing, electronically or otherwise. Also the Company shall regularly review the content to reflect the latest laws, technologies and

business development to ensure the effectiveness of the policy.

IV. The Responsibility Division of Information Security

7. The Company shall delegate responsibilities to related departments and personnel based on the following principals:
   (1) The information department shall be responsible for the formulation of information safety policy. Related information positions and works shall be divided appropriately, and the responsibilities shall be clear.
   (2) The auditing department shall conduct at least once information security auditing operation each year.
   (3) The human resource department shall arrange new employees' education training and to proclaim relevant information security issues.
   (4) The marketing department shall correctly classify various business information within the Company.
   (5) The general affairs department shall properly establish and maintain the Company's inventory of assets, and set the information assets, owners and security levels of each unit.
   (6) The legal department shall review the information contracts and provide appropriate advisements.
   (7) The heads of all departments shall strengthen the employees' awareness of information security and supervise their underlings to implement information operation security.
8. The Company may instruct a cross-unit team based on the needs of information security management, to coordinate information security operations management and resource scheduling matters.

V. The security Management of Computer System

9. Information department shall adopt necessary preventive and protective measures to ensure that the computer system is functioning properly.

VI. The Security Management of Network

10. The Company shall apply firewalls and other facilities to control the transmission and access of data between internal and external networks.
11. The Company should properly control the wires, network equipment and data exchange interfaces that transmit information or conduct transactions through the public network.
12. The Company website shall strengthen the protection of customer information and sensitive files in order to prevent data leakage.

VII. The Management of System Access Control

13. The Company only grants the necessary authority for personnel at all level to execute the system. The authority adjust with the position of the personnel is adjusted or transferred.
14. The system authority of the Company's resigned employees should be immediately canceled and the cancellation should be included in the requirements for the personnel leaving procedure.
15. In the event that the Company opens an external vendor connection, the linker should be abided by the Company's information security regulations, procedures, and is responsible for information security.

VIII. The Security Management of System Development and Maintenance

16. The Company shall take information security needs into account in the initial stage of the system life cycle when developing system. When handling outsourcing information operations, the Company shall specify the information security and confidentiality responsibilities to the vendors.
17. System maintenance, update, online implementation and version change operations shall be subject to appropriate security controls.
18. When the Company entrusts the manufacturer to build and maintain important hardware and software facilities, it should be supervised and accompanied by the Company's relevant personnel.

IX. The Security Management of Information Assets

19. The Company shall adopt appropriate and adequate information security measures based on different security levels.

X. Physical and Environmental Security Management

20. The Company shall establish appropriate physical and environmental security management measures based on the equipment placement, surrounding environment and personnel access control, assets value and safety risk level. Also the Company should regularly review the appropriateness of the security management measures.

XI. Sustainable Business Operation Program

21. The Company shall assess the impact of various artificial and natural disasters on the Company's operations and establish emergency response and recovery procedures, also to conduct regular exercise.
22. The Company shall establish an emergency handling mechanism for information security incidents. In the event of a security incident, it shall adopt

response measures in accordance with the prescribed procedures.

XII. Laws and Operations Compliance

23. The Company shall establish appropriate protection measures for all information fields within the Company in accordance with relevant internal and external laws and regulations, and regularly review the appropriateness of the measures.
24. The Company's information content and storage period should be determined by the requirements of domestic laws or regulations.

XIII. Appendix

25. In the event that there is special nature of the Company's business, the Company may refer to the Guideline to determine alternative regulations.
26. In the event that the Company does not have an information security management policy, it may refer to the Guidelines.