Delta Information Security Policy

1 Information Security Goals

1.1 Ensure the confidentiality of Delta Group's information assets, implement information access control, and ensure that information can be accessed only by authorized personnel.

1.2 Ensure the integrity of Delta Group's information operations and management and avoid unauthorized modification.

1.3 Ensure the continuity of information operations for Delta Group.

1.4 Ensure that the information operations of Delta Group comply with relevant laws and regulations.

2 Information Security Control Measures

2.1 Establish the Information Security Committee to govern the operations of the information security management system and identify relevant internal and external issues as well as the requirements and expectations from the stakeholders regarding information security.

2.2 Management shall be committed to maintaining information security, continuously improving the quality of information security, and reducing the occurrence of information security incidents so as to protect customers' business and interests.

2.3 Documents of the information security management system shall be updated at appropriate intervals and well-defined management mechanisms shall be established for data protection .

2.4 Information asset classification and risk assessments shall be conducted regularly.

2.5 All employees of the Group shall be responsible for protecting information assets they own, keep, or use.

2.6 Work assignments shall be considered based on employee skills. The separation of duties shall be implemented to prevent unauthorized modification or misuse of information or services.

2.7 When the suppliers, their employees, or contractors have a need to access the Delta Group's information assets, performing proper review is required.

All personnel shall be responsible for protecting Delta Group's information assets they own, keep, or use.

2.8 Business continuity plan should be formulated according to business operations and tested regularly.

2.9 Information security indicators shall be inspected on a regular basis to ensure the effectiveness of the implementation of the information security management system and control procedures.

2.10 All employees shall ensure environmental security of workplace and prevent information assets from theft or damage.

2.11 The management of communication security shall be implemented.

2.12 The development, modification, and installation of information operations or procedures must be in line with information security policies and regulations.

2.13 The parties to which this policy is applicable shall pay close attention at all times to information security incidents, security vulnerabilities, and violations of the security policies and regulations, and shall also file reports in accordance with defined procedures.

2.14 The parties to which this policy is applicable shall abide by relevant internal and external regulations and establish necessary management and control procedures, and conduct regular information security audits.

2.15 The mobile device security measures shall be implemented to manage the potential risks caused by using a mobile device.

2.16 The processes of project management shall include the issues related to information security.