Cathay Financial Holdings (Cathay FHC)
Information Security Policy

Established on April 27, 2007
Amended on February 6, 2013
Amended on March 15, 2018
Amended on March 21, 2019
Amended on August 19, 2021
Amended on May 13, 2022
Amended on May 11, 2023
Amended on April 23, 2025
Amended on August 15, 2025
Responsible Unit: Information Security Division

Article 1 Objective

To enhance the information security management of Cathay Financial Holdings ("Cathay FHC"), establish a secure and reliable information and operations environment, ensure the confidentiality, integrity, and accessibility of information assets, and raise employees' awareness of information security, thereby protecting the rights and interests of employees, customers, and Cathay FHC, Cathay FHC hereby establishes this Information Security Policy ("the Policy").

Article 2 Policy Statement

Cathay FHC's policy statement on information security management is as follows:

I. Cathay FHC's information security management shall comply with the Personal Data Protection Act, Financial Holding Company Act, Implementation Rules of Internal Audit and Internal Control System of Financial Holding Companies and Banking Industries, related regulations and guidelines established by Cathay FHC and subsidiaries, rules from competent authorities, and the Policy herein.

II. Cathay FHC strictly prohibits any unauthorized access to, disclosure of, or destruction of its information assets. To safeguard information security, appropriate controls shall be maintained throughout the

information-asset lifecycle to prevent any information-security incident.

III. Effective information security measures shall be considered when developing information systems and using third-party cloud services to mitigate the risk of network and computer system attacks or unauthorized access by hackers or internal personnel.

IV. All employees of Cathay FHC (including contractors, interns, and temporary workers) have the responsibility and obligation to protect Cathay FHC's information assets that they obtain or use, preventing unauthorized access, alteration, destruction, or improper disclosure.

V. Cathay FHC has the right to manage information assets belonging to Cathay FHC, including but not limited to information processed, stored, or transmitted on Cathay FHC's information assets or using online resources on behalf of Cathay FHC.

VI. Information services contracts shall regulate the following items:

i. The scope of the entrusted tasks and the rights and responsibilities of the entrusted organization.

ii. Entrusted persons are obligated to protect Cathay FHC's information assets and shall not disclose, access, alter, or destroy Cathay FHC's information assets without prior authorization.

iii. Entrusted persons shall comply with the Policy herein and related management guidelines. Entrusted persons shall also remain alert for any information security incidents, vulnerabilities, and violations of Cathay FHC's Information Security Policy and related management guidelines. In the event of any aforementioned circumstances, entrusted persons shall immediately report to Cathay FHC's responsible unit and Information Security Division.

iv. Confidentiality clause and audit clause.

v. Contract termination and cancellation clause.

vi. Penalty clause and indemnification clause.

vii. Other mandatory items.

Article 3 Applicability & Scope

The Policy applies to all employees of Cathay FHC as well as partners and contractors (including advisors and cloud service providers) who may have access to information related to Cathay FHC’s business.

The scope of the Policy covers the following (hereinafter collectively referred to as "Information Assets"):

I. All information and documents owned by Cathay FHC.

II. All hardware assets, including Cathay FHC’s mainframes, servers, personal computers, terminal equipment, communication lines, and any equipment related to the preceding assets or connected with Cathay FHC's information systems.

III. All physical spaces where Cathay FHC’s hardware assets are stored.

IV. All software assets, including application systems, cloud services, and any items related to the preceding assets or connected with Cathay FHC's information systems.

V. Other information assets owned by Cathay FHC or any information assets under Cathay FHC's management in compliance with contracts, laws, or regulations.

Article 4 Terms and Conditions

Terms used in the Policy are defined below:

I. Information: Refers to raw data, processed information, and derivative knowledge that is displayed in any form and recorded or stored in any media (including paper).

II. Information Security: Aims to ensure the confidentiality, integrity, accessibility, privacy, and compliance of information so that information can be safely, accurately, appropriately, and reliably applied to any planning, execution, management, and related efforts toward Cathay FHC's business objectives.

III. Cloud Services: Any services leased from cloud service providers for computation, storage, and backups; including but not limited to network equipment, servers, storage space, information security equipment, system software, applications, analytics, computing resources, and other services. Any services not leased from third-party cloud service providers shall be governed by other provisions herein.

IV. Cloud Service Providers: Third-party vendors that provide network, server, storage space, infrastructure, security equipment, system software, applications, analytics, computing resources, and other services to individuals or enterprises through leases.

Article 5 Information Security Management Units & Responsibilities:

To balance business development and information security control and to underscore the importance of information security, appropriate human resources and equipment should be allocated for planning, monitoring, and executing information security management operations. Cathay FHC shall appoint an Executive VP or equivalent position to serve as (or concurrently hold the position of) Chief Information Security Officer (CISO) to oversee the rollout of information security policies and resource allocation. An independent information security unit, separate from the information department, shall be established, and a Senior VP or equivalent level employee shall be appointed (or concurrently serve) to head this unit, with no overlapping responsibilities in information or other conflicting roles. Dedicated information security personnel should also be assigned accordingly.

The dedicated information security unit is responsible for planning, monitoring, and executing information security management and shall report the information security performance of the previous year to the board of directors each year.

Article 6 To ensure the effectiveness of information security management and operations, Cathay FHC's information management units and information security units shall be responsible for the first and second lines of defense, respectively.

The Information Division and any units related to information development and maintenance (hereinafter referred to as "Information Management Units") are responsible for the first line of information security defense. Information development includes the planning and design of information systems or security mechanisms during the development or introduction stages. Information maintenance includes the setup, maintenance, monitoring, incident reporting, and handling of information systems or security mechanisms during the management stage. These tasks can also be delegated by Information Management Units to subsidiaries when necessary.

The Information Security Division is responsible for the second line of information security defense, which is planning information security strategies and blueprints, promoting information security policies, monitoring the execution of information security, tracking remediation efforts for security deficiencies and incidents, and conducting information security training and awareness training. Information security operations entrusted to a subsidiary with stricter information security controls than Cathay FHC shall be governed by the subsidiary's policies.

If an employee holds concurrent positions in both Cathay FHC and a subsidiary, the information security control standards of the stricter entity should be applied to the information assets used by the employee.

Article 7 Information Security Governance Framework

To effectively roll out information security across Cathay FHC and oversee information security management across subsidiaries, Cathay FHC shall establish an Information Security Committee:

I. Convenor & Members:

The highest-ranking information security officer of Cathay FHC shall serve as the convener, and a deputy convener may be appointed. The President shall be invited to attend and advise. The head of the Information Security Division shall serve as the executive secretary. Committee members shall include the highest-ranking information security and IT officers from Cathay FHC and subsidiaries. Subsidiaries without IT or information security departments shall appoint dedicated personnel and may invite related management from Cathay FHC to attend.

II. Meeting Frequency:

The committee shall convene once every six months and shall convene ad hoc meetings when necessary.

III. Committee Tasks:

i. Formulate Cathay FHC's information security policies.

ii. Roll out Cathay FHC and subsidiaries' information security management policies.

iii. Formulate Cathay FHC and subsidiaries' education and training plans for information security awareness.

iv. Oversee Cathay FHC and subsidiaries' information security practices.

v. Deliberate and decide on major group-wide information security projects.

Article 8 To roll out information security, maintain effective group-wide communication, and achieve consistent information security management across Cathay FHC and its subsidiaries, Cathay FHC shall establish an Information Security Communication Committee:

I. Convenor & Members:

The highest-ranking information security officer of Cathay FHC shall serve as the convener, and a deputy convener may be appointed. The management of the Information Security Division shall serve as the executive secretary. Committee members shall include the highest-ranking information security officers, information security managers, and information security personnel from Cathay FHC and subsidiaries. IT or business management may be invited to attend as well.

II. Meeting Frequency:

The committee shall convene once every month and shall convene ad hoc meetings when necessary.

III. Committee Tasks:

i. Plan and discuss Cathay FHC and subsidiaries' information security blueprint and fundamental management requirements.

ii. Review and discuss the compliance and suitability of Cathay FHC and its subsidiaries' information security management systems.

iii. Compile reports on Cathay FHC and subsidiaries' information security practices.

iv. Discuss and plan group-wide information security projects.

v. Communicate and coordinate information security affairs across the group.

Article 9 Information Security Incident Management Principles

All employees who discover or receive reports from external parties of suspected information-security incidents, any potential violation of the information-security policy or related regulations, or any external threat, must remain vigilant and report the matter in accordance with established procedures.

In the event of a major information-security incident, Cathay will maintain transparent communication with potentially affected stakeholders explaining the response actions taken and the preventive measures implemented to minimize the risk of recurrence.

Article 10 Policy Assessment

This policy shall be amended as necessary in light of the latest developments in governmental regulations, technology, and business operations, and its adequacy shall be reviewed at least annually.

The results of these reviews will serve as the basis for continuously improving the information-security management system, ensuring it effectively protects the Company’s assets against evolving risks.

Article 11 Date of Effectiveness

The Policy shall take effect upon approval by the board of directors and shall be similarly amended or abolished.