CHANG HWA COMMERCIAL BANK LTD.

Information Security Policy

V8.5

Version	Revision Date	Reviser	Approval Date	Approver	Remarks
V1.0	2004/05	IT Division	2004/05	CEO	
V2.0	2005/01	IT Division	2005/01	CEO	
V3.0	2006/01	IT Division	2006/01	CEO	
V3.1	2006/04	IT Division	2006/04	CEO	
V3.2	2006/12	IT Division	2006/12	CEO	
V4.0	2008/12	IT Division	2008/12	CEO	
V5.0	2009/12	IT Division	2009/12/29	The 8th meeting of the 22nd term board of directors.	
V6.0	2013/05	IT Division	2013/05/14	The 20th meeting of the 23rd term board of directors.	
V7.0	2018/01	IT Division	2018/01/19	The 8th meeting of the 25th term board of directors.	
V7.1	2018/09	Information Security Center	2018/09/28	The 16th meeting of the 25th term board of directors.	
V8.0	2020/05	Information Security Center	2020/05/07	The 37th meeting of the 25th term board of directors.	
V8.1	2021/07	Information Security Center	2021/07/22	The 15th meeting of the 26th term board of directors.	
V8.2	2022/03	Information Security Division	2022/03/29	The 24th meeting of the 26th term board of directors.	
V8.3	2023/05	Information Security Division	2023/06/07	The 40th meeting of the 26th term board of directors.	
V8.4	2025/03	Information Security Division	2025/03/20	The 24th meeting of the 27th term board of directors.	

Version	Revision Date	Reviser	Approval Date	Approver	Remarks
V8.5	2026/05	Information Security Division	2026/09/24	The 5th meeting of the 28th term board of directors.	

Contents

Article 1	Purpose	1
Article 2	Compliance	1
Article 3	Goal	1
Article 4	Scope	1
Article 5	Information Security Organization Structure	2
Article 6	Responsibility	3
Article 7	Chief Information Security Officer	3
Article 8	Head of Information Security	4
Article 9	Foreign Branches	4
Article 10	Policy Promotion	4
Article 11	Information Security Incident Report	4
Article 12	Violation of Information Security Guidelines	5
Article 13	Addendum	5
Article 14	Implementation and amendments	5

Article 1 Purpose

The Chang Hwa Commercial Bank Co., Ltd. (the Bank) has the policy to enhance information security management, ensure the confidentiality, integrity, and availability of information, safeguard the reliability of information equipment (including hardware, software, and related facilities) and the network system, and make all the staff to understand information security, and also prevent from any factor of obstructing, damaging, invading, or any unfavorable behavior or attempt to the resources mentioned above.

Article 2 Compliance

1. Personal Information Protection Act.
2. ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection - Information security management systems – Requirements.

Article 3 Goal

The objective of information security is to safeguard the legal and authorized access to the Bank's information and to provide complete and reliable information system operations when there are internal and external security threats. While happening any incident, there shall have necessary actions to reduce the damage from the incident. The Bank continues to invest the necessary resources in the information security protection systems to achieve information security objective.

Article 4 Scope

The scope of the Information Security Policy includes all information software, hardware, and related facilities. Related departments and personnel should follow the items below having management guidelines to execute information security plans and support the Bank's goals.

1. Information security responsibility.
2. Personnel management and information security training.
3. Computer system security management.
4. Network security management.

5. System access management.
6. System construction, development, and maintenance management.
7. Information asset security management.
8. Data protection management.
9. Physical and environmental security management.
10. Vendor and third-party information security requirements and management.
11. Information security risk assessment management.
12. Information security auditing management.
13. Monitoring and responsiveness to information security threats.
14. Other information security management.

Article 5 Information Security Organization Structure

In order to effectively promote information security, the Bank has implements three lines model for the information security structure. The first line includes all departments and the IT Division being responsible for executing information security operations. The second line is the Information Security Division monitoring the executing status of the Information Security Policy and the deriving security risks. The third line is the Internal Auditing Division, which checks the operations.

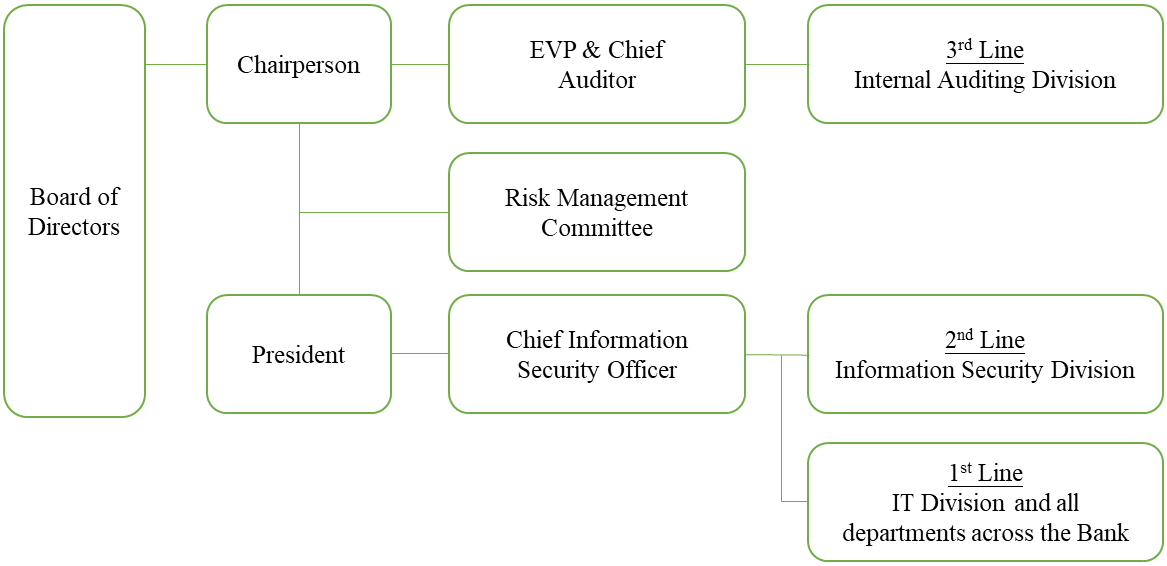


Figure 1: Information Security Organization Structure

Article 6 Responsibility

To ensure that information security management can be promoted effectively, responsibility is clearly stated. To promote and maintain information security execution, management, and auditing, there should be assigned responsibility to appropriate personnel based on the guidelines below:

1. The main responsibility of the IT Division is to promote the management system, monitor the information security system, track and execute the inspections and drills as required by the law, report information security related incidents, and audit the IT Division's information security operations.
2. The main responsibility of the Information Security Division including:
   (1) Taking charge of the planning, management, and execution of the information security system to manage information security risks.
   (2) Supervising each unit in implementing the information security system, and ensuring the confidentiality, integrity, and availability of communication systems, services, and information.
   (3) Establishing mechanisms related to cyber security protection, assessment and response to cyber security intelligence, and reporting of and response to cyber security incidents.
   (4) Incorporating the overall implementation of information security from the preceding year into the assessment of the implementation of the internal control system annually.
   (5) Handling matters related to information security education and training.
3. The main responsibility of the Internal Auditing Division is to audit information security operations.

Article 7 Chief Information Security Officer

The Chief Information Security Officer (CISO) to oversee the promotion of information security policies and the allocation of resources. The CISO shall report the overall implementation of information security from the preceding year to the Board of Directors each year, and report material information security issues in a timely manner.

Article 8 Head of Information Security

The Head of Information Security Division, with a background in information security, is responsible for the implementation of information security policies. The head of Information Security Division shall coordinate and promote information security management operations.

Article 9 Foreign Branches

In addition to complying with the Bank's Information Security Policy, Business Processing Procedures for Information, and related documents, the Bank's overseas branches should formulate information security standards in accordance with local laws and regulations. If the two have different requirements, the higher standard should be selected as the basis for compliance, and it will be reviewed by the Information Security Division before being submitted to the Risk Management Committee.

Article 10 Policy Promotion

The Bank shall promote its Information Security Policy to all the staff and information service providers through policy announcements, keynote speeches, educational training or electronic media. In doing so, the Bank's information security benchmarks can be better promoted and complied with.

Article 11 Information Security Incident Report

In the event of an information security incident, all units shall follow the Bank's “Information Security Event Reporting Procedure”. In the case of a major incident, it shall be handled in

accordance with the “Chang Hwa Bank Material Contingency Handling Procedure”.

If happening the material emergency event, the Information Security Division and IT Division should report to the CISO and the division's Deputy Director of Supervision, take appropriate measures to reduce the damage caused by the accident, and safeguard the ongoing business operations.

Article 12 Violation of Information Security Guidelines

Employees in CHB must comply with the Information Security Policy, Business Processing Procedures for Information, and related correspondence. If any violations are found, they will be dealt with as appropriate, such as education and training, preparing a review report, and further evaluation by Personnel Review Committee, etc.

Article 13 Addendum

If the Bank's Information Security Policy has any addendum, it should still follow the spirit and principles of competent authority regulations and information security management to ensure the confidentiality, integrity and availability of the Bank's information assets.

Article 14 Implementation and amendments

The policy should be evaluated at least once a year, or re-evaluated when major changes occur, to comply with the latest developments in relevant laws, organizations, and businesses, and to ensure the effectiveness of information security practices.

The policy and any amendments to the articles shall only take effect upon approval by Board of Directors.