台中銀行
TAICHUNG BANK

台中商業銀行資訊安全政策
Taichung Commercial Bank Information Security Policy

第一條　目的

Article 1　Purpose

為確保台中商業銀行(以下簡稱「本行」）所屬之資訊資產的機密性、完整性及可用性，以符合相關法令規章之要求，使其免於遭受內、外部蓄意或意外之威脅，並衡酌本行之業務需求，訂定本政策。

This Policy is established to ensure the confidentiality, integrity and availability of the information assets of Taichung Commercial Bank (hereinafter referred to as "the Bank"), to meet the requirements of relevant laws and regulations, and to protect the Bank from internal and external intentional or accidental threats, and to consider the business needs of the Bank.

資訊資產之定義：為維持本行資訊業務正常運作之硬體、軟體、資料、文件及人員。

Definition of information assets: hardware, software, data, documents and personnel to maintain the normal operation of the Bank's information business.

第二條　目標

Article 2　Objectives

為保護本行資訊資產免遭不當使用、洩漏、竄改、破壞等情事，確保資訊蒐集、處理、傳送、儲存及流通之安全，目標如下：

To protect the Bank's information assets from improper use, leakage, tampering, damage, etc., to ensure the security of information collection, processing, transmission, storage and circulation, the objectives are as follows:

一、機密性：保護敏感資訊免於未經授權公開或被他人恣意取得。

Confidentiality: To protect sensitive information from unauthorized disclosure or being inadvertently obtained by others.

二、可用性：確保資訊及重要服務在使用者需要時可以取得。

Availability: To ensure that information and important services can be obtained when users need it.

三、完整性：適當之安全防護措施以防止資料不當之修改或增刪，確保資料能完整提供，未有遺漏的情形發生。

Integrity: Appropriate security measures to prevent improper modification or addition or deletion of data to ensure that the information can be provided in full and no omissions have occurred.

四、適法性：確保本行各項業務服務之執行須符合相關法令規章之要求。

Legality: To ensure that the implementation of various business services of the Bank is subject to the requirements of relevant laws and regulations.

第三條　適用範圍

Article 3　Applicability

資訊安全管理範疇涵蓋十四項領域，避免因人為疏失、蓄意或天然災害等因素，導致資料不當使用、洩漏、竄改、破壞等情事發生，對本行造成各種可能之風險及危害，各領域分述如下：

The information security management scope covers 14 areas to avoid improper use of data, leakage, tampering, damage, etc. due to factors such as human error, deliberate or natural disasters, and caused various possible risks and hazards to the Bank. They are as follows:

一、資訊安全政策訂定與評估。

Information Security Policy establishment and evaluation.

二、資訊安全組織。

Organizations of information security.

三、人員安全管理與教育訓練。

Personnel security management and educational training.

四、資訊資產分類與管制。

Classification and control of information assets.

五、存取控制安全。

Access control security.

六、加密控制措施。

Encryption control measures.

七、實體與環境安全。

Physical and environmental security.

八、作業安全管理。

Operation security management.

九、通訊安全管理。

Communication security management.

十、系統開發與維護之安全。

Security of system development and maintenance.

十一、供應商安全管理。

Supplier security management.

十二、資訊安全事件之反應及處理。

Response and handling of information security incidents.

十三、營運持續運作管理。

Business continuity operation management.

十四、相關法規與施行單位政策之符合性。

Compliance with relevant laws and regulations and the policies of the implementing unit.

第四條　權責及分工

Article 4　Rights and obligations and division of work

應成立資訊安全組織統籌資訊安全事項推動，並定期舉辦管理審查會議。

An information security organization shall be set up to coordinate the promotion of information security matters, and regularly hold

management review meetings.

資訊安全之稽核事項，由稽核室查核。

The Auditing Office shall audit the information security audit matters.

資訊安全事件通報管理，由風險管理部會同各業務相關單位辦理。

Information security incident reporting and management shall be handled by the Risk Management Department in conjunction with relevant business units.

資訊安全教育訓練，由資訊維運部統籌規劃，會同人力資源部辦理。

Information security education and training shall be coordinated and planned by the Information Operation Department in conjunction with the Human Resources Department.

第五條　責任

Article 5　Responsibility

管理階層應積極參與及支持資訊安全管理制度，並提供適當之資源實施本政策。

The senior management should actively participate in and support the information security management system and, provide appropriate resources to implement this policy.

本行承諾將持續強化事件應變處理能力並建立適當營運持續管理系統，達成持續提供產品及服務之目標。

The Bank promises to continuously strengthen its ability to handle incidents and establish an appropriate business continuity management system to achieve the goal of continuously providing products and services.

本行及子公司全體人員、派遣人員、委外服務廠商與訪客等皆應遵守本政策。

All staff, dispatched personnel, outsourcing service providers and visitors of the Bank and its subsidiaries shall abide by this policy.

本行及子公司全體人員、派遣人員與委外服務廠商均有責任透過

適當通報機制，通報資訊安全事件或弱點。

All staff, dispatched personnel and outsourcing service providers of the Bank and its subsidiaries have the responsibility to notify information security incidents or vulnerabilities through appropriate notification mechanisms.

任何危及資訊安全之行為依本行之相關規定進行議處，必要時得視情節輕重追究其民事及刑事責任。

Any behavior that jeopardizes information security shall be conducted in accordance with the relevant provisions of the Bank, and if necessary, the civil and criminal liability shall be investigated according to the circumstances.

第六條　管理指標

Article 6　Management indicators

為評量資訊安全管理目標達成情形，應以定量化指標和定性化指標來評估實施成效。

Assessment of information security management objectives completion rate should be based on quantitative and qualitative indicators to assess the effectiveness of the implementation.

一、定量化指標:

Quantitative indicators

可透過準確數據定義、精確衡量並能設定績效目標的量測指標。

Metrics that can be defined with accurate data, accurately measured, and capable of setting performance goals.

二、定性化指標:

Qualitative indicators

無法直接透過數據、數量計算衡量內容，需對量測目標進行客觀描述和分析來反映量測結果的指標。

The event impossible to directly measure the content through data and quantity calculations, needing necessary objectively describe

and analyze to the measurement targets in order to reflect the measurement results.

第七條　審查

Article 7　Review

本政策應至少每年檢視一次並留存相關紀錄，以反映相關法令規章、技術及資訊業務等最新發展現況，確保資訊安全實務作業之有效性。

This policy should be reviewed at least once a year and relevant records should be kept to reflect the latest developments in relevant laws and regulations, technology and information services to ensure the effectiveness of information security practices.

第八條　核定層級

Article 8　Level of Approval

本政策經董事會通過後頒布實施，修正時亦同。

This policy shall be implemented after approval and promulgation by the Board of Directors and the same also applies to any amendments made.

.