Taishin Financial Holding
Information Security Policy

June 20, 2007 -Approved by Presidentof Taishin Holdings

July 8, 2009 -Approved by Presidentof Taishin Holdings

December 23, 2010 -Approved during the 12th meeting of the 4th board

May 18, 2023 -Approved during the 27th meeting of the 8th board

I. Purpose:

This policy has been established to enforce information security management within the Company, and to ensure that information assets obtained, processed, transmitted, stored, and circulated in ways that comply with security principles of confidentiality, integrity, and availability. This policy shall serve as reference to subsidiaries for the establishment of their respective security policies.

II. Scope:

This Information Security Policy describes ways of processing and protecting different forms of information assets, and outlines rules that are relevant to enhancing reliability of data processing hardware/software and maintenance of the physical security of computer facilities. All departments shall convey the duty of protecting sensitive and confidential information to employees and service vendors.

III. Information security responsibilities

(I) All employees: It is the responsibility of every employee to protect computer data from accidental or intentional corruption, modification and dissemination. Employees have their duty to notify line manager or administration department immediately upon learning any act of violation.

(II) Personnel in charge:

The personnel in charge msut confirm the security requirements of data and reports, utilization management, protection and maintenance of confidentiality.

(III) The users of information assets: Use of the Company's computer systems and resources must be authorized by the authorized manager and are subject to the following responsibilities.

1. Information shall be used only for the specified purpose in a manner that complies with computer resource and system access rules.
2. Unauthorized distribution of information must be avoided.

(IV) Information management personnel: Information management personnel shall ensure that appropriate procedures are implemented to manage development activities at various stages of system development, management and maintenance.

(V) Security management personnel: Each subsidiary shall have information security personnel or team available to oversee, promote, review and improve information security management practices.

IV. The Company should inspect characteristics of its own IT processes and include all or part of the following information security management items in the scope of management and implement corresponding operating standards and procedures.

(I) Roles and responsibilities in information security
(II) Management of personal security and information security awareness
(III) Management of computer security
(IV) Management of network security
(V) System access control
(VI) Security management for system development and maintenance
(VII) Management of physical and environmental security
(VIII) Management of supplier information security risk
(IX) Management of information security incidents
(X) Management of IT business continuity
(XI) Management of privacy protection
(XII) Other areas of information security management

V. When developing or modifying important information systems and structures, the Company should pay attention to relevant information security controls and strengthen resilience of system operations.

VI. The Company must have in place reporting and response measures for information security incidents in order to enable better response to information security incidents and reduce impacts and losses to the company.

VII. The internal audit unit should act in an objective, impartial, and professional manner and audit information security controls, and propose appropriate improvements to reasonably ensure effective information security management.

VIII. All employees of the Company and its subsidiaries shall comply with the information security regulations and self regulatory guidelines established by the competent authority or respective trade associations, including but not limited to "The Rules Implementation of Internal Audit and Internal Control System of Financial Holding Companies and Banking Industries", "The Financial Institutions Information Security Protection Benchmarks", "The Self Regulatory Guidelines for Information Security Protection for Insurance Companies", and" The Establishing Information Security Inspection Mechanisms for Securities Firms".

IX. Any employee of the Company or any of its subsidiaries who fails to comply with the information security guidelines or whose conduct violates the information security requirements shall be subject to the applicable disciplinary action.

X. This policy shall be assessed regularly or re-assessed after a major change in order to stay aligned with the current regulatory, technological and organizational, and operational circumstances.

XI. This policy shall be implemented with the approval of the board of directors. The same applies to subsequent amendments.

台新金控股份有限公司

資訊安全政策

民國 96 年 6 月 20 日金控總經理核定
民國 98 年 7 月 8 日金控總經理核定
民國 99 年 12 月 23 日第四屆第十二次董事會核定
民國 112 年 5 月 18 日第八屆第 27 次董事會核定

一、 目的：

為強化本公司各單位資訊安全管理，確保各項資訊資產取得、處理、傳送、儲存及流通的流程均能符合機密性、完整性及可用性之安全原則，特訂定本政策，並供各子公司遵循與訂定資安政策之參考。

二、 範圍：

本資訊安全政策說明如何處理及保護各種形式的資訊資產，同時也制定規則，以提升資訊處理硬體與軟體的可靠度，及電腦設施的實體安全維護。各部門應將保護敏感或機密資訊之義務廣為宣導全體員工及提供資訊服務之委外廠商共同遵守。

三、資訊安全職責分工

(一). 全體同仁：

保護電腦資料免於遭受意外或蓄意破壞、修改或散佈，是每位員工的責任；當察覺任何違犯規範之情況，應有責任立即告知主管或管理部門知悉。

(二). 業務權責人員：

須確認資料及報表之安全需求研議、使用管理、保護及資訊機密維護。

(三). 資訊資產使用者：

使用公司電腦系統及資源，必須先經權責主管授權核可，並具備下列責任。

1. 按指定用途使用資訊，並遵循電腦資源存取及系統執行之控管。
2. 避免未經授權的資訊散佈。

(四). 資訊管理人員：
從事資訊處理系統開發、管理及維運者，應確保各系統發展及維運階段皆有合適的處理程序來管理各階段工作。

(五). 安控管理人員：
為能適切實施資訊安全管理，各子公司應有資訊安全推動人員或小組，以辦理資訊安全計劃推動、查核及改善。

四、本公司應審視本身資訊作業特性，將下列資訊安全管理項目全部或部分納入管理，建立相對應之作業標準及程序：

(一). 資訊安全權責分工

(二). 人員安全管理及資訊安全體認

(三). 電腦系統安全管理

(四). 網路安全管理

(五). 系統存取控制

(六). 系統發展及維護之安全管理

(七). 實體及環境安全管理

(八). 供應商資安風險管理

(九). 資訊安全事故管理

(十). 資訊業務持續營運管理

(十一). 隱私資訊保護管理

(十二). 其他資訊安全管理事項

五、本公司於開發或修改重要資訊系統及資訊架構時，應將相關資訊安全控管措施納入重要考量，強化系統營運韌性。

六、本公司須訂有資訊安全事件相關通報及處理措施，以強化遭遇資訊安全事件時的應變能力，降低對公司的影響及損失。

七、內部稽核單位，應以客觀、公正及專業的立場，查核資訊安全控管機　制，並提出合適之改善建議，以合理確保資訊安全管理之落實。

八、本公司及各子公司所有同仁應遵循主管機關或業別同業公會訂定之資訊安全相關法規及自律規範，包含但不限於「金融控股公司及銀行業內部控制及稽核制度實施辦法」、「金融機構資通安全防護基

準」、「保險業辦理資訊安全防護自律規範」及「建立證券商資通安全檢查機制」等。

九、本公司及各子公司所有同仁若未遵循資訊安全相關管理要點或有任何違反資訊安全要求之行為，應依相關規定議處。

十、本政策應定期進行評估，或於發生重大變動時重新評估，以符合相關法規、技術及組織、營運現況。

十一、本政策經本公司董事會核定後實施，修訂時亦同。