金財通商務科技服務股份有限公司

資訊安全管理制度

ISMS-101 資訊安全政策

注意：任何個人、組織或團體在使用、複製、散播本文件之部分或全部內容前，應取得金財通商務科技服務股份有限公司合法授權，任何未經事前授權者，將依法追究其責任。

文件版本：V1.0

目 錄

壹、 目的 1

貳、 範圍 1

參、 權責 1

肆、 名詞定義 1

伍、 作業內容 2

陸、 援引文件 6

柒、 附件 6

捌、 修訂紀錄 7

壹、目的

定義金財通商務科技服務股份有限公司（以下簡稱本公司）的資訊安全政策，使全體同仁能遵守並有所依循，使各項業務作業順利運行，並確保各項資訊媒體之安全，以達成本公司資訊安全之目標。

貳、範圍

本文件適用於本公司及所屬各部處規劃、實作、審查與改善資訊安全管理制度。

參、權責

一、全體同仁

遵守資訊安全政策與相關管理規範。

二、管理階層

(一) 確立資訊安全方向、目標與制度架構，確保與公司策略一致。

(二) 提供必要資源，明確分配角色與責任，保障制度運作。

(三) 監督制度執行與風險管理，持續評估、審查及改善資訊安全管理制度。

肆、名詞定義

一、資訊安全

保護資訊的機密性、完整性與可用性；另外，也能涉及如鑑別性、可歸責性、不可否認性及可靠性等特性。

二、資訊安全管理制度（Information Security Management System, ISMS）

基於業務風險作法，以建立、實作、運作、監視、審查、維護與改善資訊安全，即為保護資訊安全而建立的管理規範和流程。

三、機密性（Confidentiality）

使資訊不可用或不揭露給未經授權之個人、個體或過程的性質，即為

只有獲授權者才能存取或知悉資訊。

四、完整性（Integrity）

保護資產之準確度和完全性的性質，即為資訊保持正確與完整，不被未經授權修改或破壞。

五、可用性（Availability）

在獲授權個體要求時， 可取得及使用之性質，即為獲授權者在需要時能取得並使用資訊資產。

六、鑑別性（Authenticity）

個體為其所宣稱具有之性質，即為個體確實擁有其宣稱的身分或特性，而非假冒或偽造。

七、可歸責性（Accountability）

個體對其行動與決策之職責，即為能夠明確確認行為人，並由其對所作行動與決策負責。

八、不可否認性（Non-repudiation）

可證明所宣稱事件（或動作）之發生及其發起個體的能力，即為能夠證明某項行為或事件確實發生，且可確認實際執行該行為的人。

九、可靠性（Reliability）

預期行為與結果一致之性質，即為資訊或行動與原本的計畫或決策一致，且不被未經授權的更動或破壞。

十、管理階層

指組織內負責制訂策略與方向，且具有決策與資源分配權限的高階主管。

伍、作業內容

一、資訊安全管理制度

(一) 概述

本公司為展現貫徹資訊安全管理的決心，確保所有資訊資產獲得適當保護，依照 ISO/IEC 27001 採用「Plan-Do-Check-Act」（PDCA）之循環運作模式，建立與實施資訊安全管理制度，並維繫其有效運作與持續改進。

(二) 規劃（Plan）：依據本公司整體策略與目標，藉由成立資訊安全管理組織，控制潛在之威脅及弱點，規劃風險評鑑、建置控管機制，以建立資訊安全管理制度。

(三) 實作（Do）：依據評估規劃之結果，建立或修正應有之管控機制。

(四) 審查（Check）：監督資訊安全管理制度各項作業之落實執行，並評估及稽核其有效性。

(五) 改善（Act）：根據審查之結果與建議，執行矯正措施，改善並執行應有之控管機制，以持續維護資訊安全管理制度運作

二、資訊安全目標

透過對人員、作業及資訊資產之管理，確保本公司資訊處理作業能安全有效運作、保障客戶各項權益，並提升客戶對本公司資訊服務之信心，由全體同仁共同努力達成下列目標：

(一) 資訊系統之正常運作。

(二) 客戶資料與隱私權之保護完全符合法令要求。

(三) 客戶資料處理過程與結果之完整正確。

(四) 確保本公司資料之機密性（Confidentiality）、完整性（Integrity）及可用性（Availability）。

三、管理階層之責任與承諾

管理階層應建立資訊安全管理組織，並透過明確之領導與承諾，確保資訊安全管理制度得以有效規劃、實作、審查與改善，其管理責任如

下：

(一) 最終核定並宣導資訊安全政策與目標，確保其與本公司策略方向相容，並持續督導其落實情形。

(二) 明確分配與協調資訊安全管理相關之角色、權責與責任，並確保全體同仁瞭解其應遵循之法令法規、合約及制度要求。

(三) 確保資訊安全管理制度需求與本公司既有流程妥善整合，並溝通符合制度要求及持續改善之重要性。

(四) 充分提供資源以規劃、實作、審查與改善資訊安全管理制度。

(五) 制訂資訊安全風險評估原則，包括可接受風險等級之準則，並確保相關風險經評估與適切管理。

(六) 施行資訊安全管理制度之管理審查，確保制度達成預期結果。

(七) 鑑別資訊安全管理制度之內外部利害關係人，考量其對本公司之資訊安全需求與期望，並決定內外部所需之溝通。

(八) 監督與檢討資訊安全事件，並考量可能影響資訊安全管理制度之內、外部議題。

(九) 每年實施資訊安全教育訓練與宣導，評估所提供資訊安全教育訓練之有效性。

(十) 其他資訊安全事項之審核與最終核定。

四、資訊安全管理

(一) 為利本公司推行資訊安全工作，應建立資訊安全組織，督導資訊安全管理制度之運作，識別資訊安全管理制度之各項議題，以符合本公司資訊安全之目標，即利害關係人之期待。

(二) 本公司應建立風險管理及資訊資產控管措施，降低整體資訊安全風險。

(三) 本公司應建立資訊安全事件之監控、通報與應變機制，並結合營

運持續管理，以降低資訊安全事件之衝擊，確保資訊服務之持續運作。

(四) 本公司應建立資訊安全管理制度之文件與紀錄管制機制，確保相關文件與紀錄之制訂、核發、變更、保存及使用均受適當控管。

(五) 本公司應辦理資訊安全教育訓練及宣導，建立全體同仁之資訊安全意識，以提升本公司資訊安全治理能力。

五、資訊安全管理制度之改善

(一) 持續改善

本公司應透過內外部稽核結果、資訊安全事件分析、矯正措施及管理審查等機制，持續增進資訊安全管理制度之有效性。

(二) 矯正措施

本公司應採取適當的控管措施，以減少資訊安全管理制度建置與運作過程中所發現之不符合事項，並防止再度發生。矯正措施之作業程序如下：

1. 識別各項不符合事項。

2. 判定各項不符合之原因。

3. 評估所需採取之措施，以確保各項不符合事項不再重複發生。

4. 決定及實作所需之矯正措施。

5. 及審查所採取之矯正措施的有效性。

六、資訊安全政策指導與覆核

本資訊安全政策每年至少評估內容一次，檢討、審核與修訂以符合內外部利害關係人的需求與期望，確保資訊安全實務作業之有效性。

七、實施規範與法令之遵循

全體同仁均須遵循此資訊安全政策，違反者須依本公司相關規定予以處分，如涉有相關刑責或法律責任者，將衡酌情節追訴其法律責任。

陸、援引文件

無。

柒、附件

無。

捌、修訂紀錄

版次	公告日期	修訂頁次	文件負責人	修訂內容摘要
V1.0	2026/03/31	NA	陳暐浩	2026/03/20 遵循 ISO/IEC 27001:2022 標準與組織需求，制訂本政策，建立基準，公佈發行。