

### 3-6 資訊安全及隱私

為強化資通安全之風險管理，成立資通安全執行小組、建置資通安全風險管理架構、訂定資通安全政策及具體管理方案及投入資通安全管理之資源等，並定期檢討資通安全政策，以確保資通安全。

#### 3-6-1 資通安全風險管理架構

資通安全執行小組定期檢討資通安全管理政策及相關辦法。各單位成員皆依相關辦法確實執行。日常營運時定期進行防火牆、網路設備、伺服器設備之檢核，以即時發現問題。進行資通安全風險評估，配合稽核單位查核以確保作業之正確性及有效性。遇有錯誤、漏洞與風險立即進行改善，以建構資通安全之持續改善管理循環。

#### 3-6-2 資通安全政策

本公司資通安全政策為「維護公司資通之機密性、完整性、可用性與適法性，避免發生人為疏失、蓄意破壞與自然災害時，遭致資通與資產遭致不當使用、洩漏、竄改、毀損、消失等，影響本公司作業，並導致公司權益損害」。本公司已於113年導入ISO 27001資通管理系統，並定期取得ISO27001認證，目前證書之有效期為113年11月21日至116年11月20日。透過ISO27001資通安全管理系統之導入，強化資通安全事件之應變處理能力，保護公司與客戶之資產安全。

2025年公司除了安排新人報到後之新人資通安全課程外，並舉辦全廠性「資通安全」教育訓練課程，透過教育訓練強化全員對於資訊安全及個資保護之認知與實務能力。說明如下：

1. 泰金累積上課人次達 223 人、總訓練時數 63 小時，受訓率約 41 %。
2. 廣金累積上課人次達 638 人、總訓練時數 78 小時，受訓率約 65 %。
3. 台金累積上課人次達 109 人、總訓練時數 2 小時，受訓率約 90 %。

## 目的

為強化資通安全之風險管理，確保資料、系統、設備及網路安全，特訂定本政策

## 資通 安全目標

確保本公司資通作業之正確性、可用性、完整性與機密性。避免內、外部資安事件之威脅。於事故發生時，亦能迅速應變，在最短時間內回復正常運作，降低事故帶來的損害。

## 資通安全管理措施

成立資通安全執行小組，訂定資通安全政策及具體管理方案，落實資通安全作業循環以確保資通安全。

### A. 落實資訊安全，強化服務品質

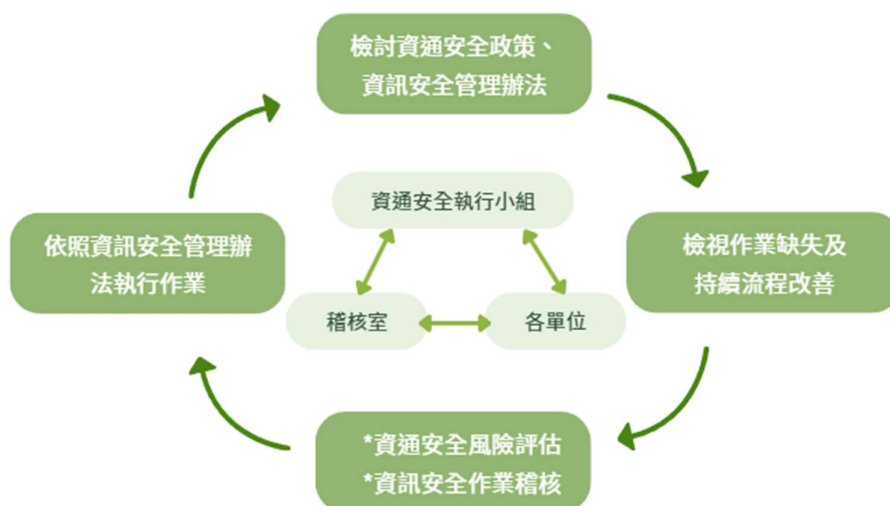
- 由全體同仁貫徹執行ISMS，所有資訊作業相關措施，應確保業務資料之機密性、完整性及可用性，免於因外在之威脅或內部人員不當的管理，遭受洩密、破壞或遺失等風險，選擇適切的保護措施，將風險降至可接受程度持續進行監控、審查及稽核資訊安全制度的工作，強化服務品質，提升服務水準。

### B. 加強資安訓練，確保營運永續

- 督導全體同仁落實資訊安全管理工作，每年持續進行適當的資訊安全教育訓練，建立「資訊安全，人人有責」的觀念，促使同仁瞭解資訊安全之重要性，促其遵守資訊安全規定，藉此提高資訊安全智能及緊急應變能力，降低資訊安全風險，達持續營運之目標。

### C. 即時緊急應變，迅速災害復原

- 訂定重要資訊資產及關鍵性業務之緊急應變計畫及災害復原計畫，並定期執行各項緊急應變流程的演練，以確保資訊系統失效或重大災害事件發生時，能迅速復原，確保關鍵性業務持續運作，並將損失降至最低。



### 具體管理方案

資通安全具體管理方案，由資通安全事件發生時間點區分，可分為事前預防、日常營運維持、資安事件處理。具體管理方案內容如下：

類別	說明	內容
預防外部入侵	安裝防火牆與防毒軟體	<ul style="list-style-type: none"><li>● 設置網路防火牆</li><li>● 伺服器與電腦主機安裝防毒軟體防毒軟體病毒碼自動更新</li><li>● 每週執行防毒軟體電腦掃描</li></ul>
預防資料外洩	帳號、權限管理	<ul style="list-style-type: none"><li>● 人員帳號審核及管理</li><li>● 定期進行系統權限設定檢核</li></ul>
日常營運維持	資料備份與相關檢核	<ul style="list-style-type: none"><li>● 依資料性質進行資料備份、異質備份與異地存放定期進行資料還原測試</li><li>● 每日執行伺服器主機檢核暨系統測試</li><li>● 定期電腦檢核</li></ul>
資安事件處理	災害復原計畫	<ul style="list-style-type: none"><li>● 訂定災害復原計畫</li><li>● 若無事件發生時定期模擬演練</li><li>● 事後撰寫災害復原計畫執行報告進行檢討改善</li></ul>

## 投入資通安全管理之資源



- 建置防火牆，加強公司網路之防護和管控功能



- 以VPN連線方式進行安全性的外部連線管控



- 建置SPAM SQR 進行郵件過濾，減少垃圾信件及抵禦各式郵件攻擊



- 訂定資訊安全風險管理辦法，加強公司內部管控功能



- 公司電腦均需安裝公司指定之防毒軟體，並自動更新病毒碼



- 建置離線式備份系統，完善備份系統機制



- 相關資訊系統的權限設



- 導入ISO 27001並取得認證

投入經費彙總如下：

2025 年項目	臺金山 (NTD)	廣州金日及廣 州金立 (CNY)	泰國金山 (THB)
WIFI 設備	78,000	54,110	92,020
防火牆設備	72,030	33,000	361,767
防毒軟體	23,100	13,650	40,098
監控設備	N/A	98,055	86,892
SPAM	87,675	N/A	N/A
微軟軟體授權(Win、 Office)	69,867	N/A	322,938
備份軟體	104,000	N/A	120,521
合計	434,672	198,815	1024,236

本案已列入 114 年 11 月 12 日日第 19 屆第 19 次董事會報告事項。