# 賢研發股份有限公司

## 資訊安全管理

隨著 AI 技術的快速演進，資訊攻擊模式已發生根本性轉變。駭客利用 AI 大幅壓縮攻擊籌備期，預測至 2026 年，資安攻擊窗口恐將從數天驟減至 24 至 48 小時內，防禦時效性面臨嚴峻挑戰。

面對此一趨勢，我們採取多層次防護策略，涵蓋數據加密、存取控制、即時監控及災難復原計畫，確保資訊在傳輸與儲存過程中的絕對安全。除持續優化內部教育培訓、更新資安政策與硬體設備外，更積極導入先進軟體工具偵測系統弱點，並由專業資安人員進行精準判讀與即時修補，全面構築堅實的資安防線。

| **重大主題** | **資訊安全與客戶隱私管理** |
|---|---|
| **重大主題意義** | 為了保障聚賢員工、客戶、供應商或承包商，本公司秉持著符合法規相關要求，並於每年度提供教育訓練，有效將低人為疏失，天然災害、等導致資訊外洩、盜竊、竄改、破壞，透過嚴格的維護資料安全，有效降低風險與損失。 |
| **政策／承諾** | 除擁有多項的資安管理措施之外，聚賢依循法規，建立資料保護機制、定期更新防毒軟體、風險評估、資安教育訓練等。並每年度檢視設備狀況適時的汰換老舊或無法更新設備，以防潛在風險並維持資訊系統效能及穩定性。 |
| **目標** | **短期（2026 年）：**<br>• 每年至少一次落實公司內部同仁對於資訊安全的認知<br>• 2026 年重大資安事件數：0 件<br>• 客戶隱私外洩事件數：0 件<br>• 持續推動資訊安全教育訓練與內部宣導，提高全員資訊安全意識<br>• 持續透過年度資訊安全稽核，持續檢視並防範潛在違規風險 |

**中長期（2027-2030 年）：**

- 每年持續宣導，確保同仁具有資訊安全意識。
- 加強公司資訊安全管理並符合法規的資訊安全協定
- 維持 2030 重大資安事件數：0 件

**行動辦法**

公司每年度進行線上或線下資訊安全宣導，並每年度 7 月和 12 月會有資訊安全抽查，並將於 2026 年度後改為每季度抽核一次，確保同仁具備防範意識。在年度資訊安全稽核中，會檢視員工的權限是否符合當前職務需求，並遵循最小權限原則，同時檢查是否有員工瀏覽不良網站或下載含有威脅的檔案，以確保公司資料不會外洩。

**2025 年實際績效**

- 完善資安治理與合規制度
  透過完善「電腦化資訊系統作業辦法」與「個人資料保護作業辦法」，明確規範員工及客戶隱私保護標準；嚴格執行機密資訊保護，2025年度員工入職簽署「保密暨競業禁止契約書」100%
- 深化技術防禦與監控機制

| | |
|---|---|
| 主動檢測 | 全面評估資安風險，定期執行系統弱點掃描、網站安全檢測、滲透測試及防火牆規則檢視，主動發掘並修補潛在漏洞。 |
| 存取控制 | 維護 Active Directory（AD）網域服務，落實終端設備權限控管；導入單一登入（SSO）機制，集中管理帳號與密碼策略，降低閒置帳號遭入侵風險。 |
| 資料防護 | 強化資料備份機制，針對重要資料庫欄位實施加密處理；嚴格控管業務電腦之USB及藍牙端口使用權限，降低資料外洩風險。 |
| 設備維護 | 定期維護防火牆與備份裝置，確保資安基礎設施運作正常。 |

| **2025 年的目標** | **達成進度及說明** |
|---|---|
| 客戶隱私零外洩 | 2025 年聚賢無侵犯客戶隱私的情事發生，亦無接獲隱私遭侵犯之投訴案件。 |
| 持續推動資訊安全教育訓練與內部宣 | 2025 年 7 月共識營向全體員工進行資安議題宣導 |

| | | | |
|---|---|---|---|
| | 導，提高全員資訊安全意識 | 及灌輸資安防範概念，並導入 SSO 系統，以統一管理員工身分，提升資訊安全防護層級與管理效率 | |
| | 持續透過年度資訊安全稽核，持續檢視並防範潛在違規風險 | 2025 年度無發生資訊安全稽核缺失 | |
| **申訴機制/溝通管道** | • Email、員工意見回饋平台、電話、勞資會議<br>• 於本公司官方網站設置聯絡信箱，提供利害關係人溝通 | | |

**資訊安全管理政策**

聚賢始終秉持誠信原則，致力於高標準的客戶隱私保護。我們制定了「內部重大資訊保密作業程序」與「個人資料保護作業辦法」，並要求全體員工於入職時簽署保密協議，定期接受資安宣導，嚴格禁止洩漏個人或客戶隱私，全面落實資訊安全責任。

為建構全方位的資安防護網，公司從制度、技術與管理三大面向同步推進，依據營運需求與風險評估動態調整控管措施，確保資安管理深入日常營運的每一環節。針對科技廠區之高規格規範，我們嚴格禁止攜帶具備拍攝、錄影及錄音功能之電子設備進入廠區。

在兼顧資安合規與溝通效率的前提下，公司統一配發無拍攝功能之公務手機供現場同仁聯繫使用；同時，為強化網域防護，嚴禁以非公務設備（如個人電腦）連接內部網路。各廠區亦設有專屬辦公空間，供工務及行政人員處理庶務，確保資料安全無虞並維持高效作業。

2025 年度，聚賢未發生任何違反資安規範之事件，亦無資安威脅或系統弱點通報紀錄，具體展現了我們對客戶隱私及資訊安全管理的高度重視與嚴謹執行力。

- **資訊安全管理政策**

| 策略 | 目的 | 因應方式 |
|---|---|---|
| 資安管控 | 強化設備維運與資訊資產安全 | 定期檢測弱點、限縮連線來源<br>門禁管制、環境監測、定時巡檢<br>資訊資產盤點、異動變更管理 |
| 網路及資安管理 | 提升網路使用安全並防範外部威脅 | 密碼強度要求<br>網段區塊隔離、網路流量監測管控<br>防火牆更新、入侵防禦偵測、惡意郵件攔阻 |
| 資訊存取控制 | 確保資訊存取權限分工與控管落實 | 權限分級與分工管理<br>員工異動即時調整權限<br>委外廠商簽署保密協議與資訊使用規範 |

| | | |
|---|---|---|
| 資料備份與復原 | 確保資訊可用性與災後復原能力 | 建置資料備份計畫與監控機制<br>定期備份與還原演練 |
| 資安宣導與稽核 | 提升資安意識與制度有效落實 | 定期辦理資安講習與宣導活動<br>新進人員簽署保密協定<br>實施內部資安稽核作業 |

更多資訊安全管理政策內容可參考公司 114 年股東會年報

- **資訊安全管理規範**

| 管理機制 | 目的 | 方法 |
|---|---|---|
| 網路威脅控管 | 主動防禦,即時封鎖網路異常行為 | 設置適當防火牆防範惡意網路攻擊，並定期測試 |
| 本地備份與異地備份 | 預防重要資訊因外部天災或人禍而遭遺失或破壞 | 重要資訊系統或設備已建置適當的備份或監控機制並定期演練,以維持其可用性 |
| 網路弱點評估 | 針對上網行為管控及威脅偵測，以防止威脅入侵 | 個人電腦均已安裝防毒軟體且定期確認病毒碼之更新,並禁止使用未經授權的軟體 |
| | | 持續評估內外部威脅可能造成之資通安全風險，透過系統弱點掃描、網站安全檢測、滲透測試、防火牆規則檢視等作業。並定期評估網路基礎架構環境,持續修補內部系統潛在弱點，及導入資訊安全設備及資安技術應用，強化資安基礎防禦力 |
| 資安意識 | 增強資訊安全意識,減少資安風險 | 不定期辦理資訊安全及個人資料保護之宣導作業 |
| 權限管理 | 防範員工任意移動或存取機密資訊 | 依據文件與職權設定存取權限、保管、加密、解密流程之管理措施 |
| 商業機密安全 | 防範員工使用可移動儲存裝置洩漏機敏資訊 | 針對本公司以外之機構或人員因參與本公司併購、重要備忘錄、策略聯盟、其他業務合作計畫或重要契約之簽訂，應簽署保密協定，並不得洩露所知悉之本公司內部重大資訊予他人 |
| 郵件安全 | 防範員工遭受釣魚信件等社交工程作業威脅 | 為提升郵件安全與資安意識,故不定期向員工宣導定期更改電子郵件信箱密碼（符合複雜密碼規則）與不隨意點擊信件內之連結的重要性 |
| 網路存取控管 | 增強資訊安全意識,強化網路憑證 | 要求同仁帳號、密碼與權限應有保管與使用之責任，並定期更換密碼 |
| 防火牆升級計畫 | 全面提升資訊安全防護韌性 | 汰換各辦公據點之舊型防火牆 |

| | | |
|---|---|---|
| | 與風險控管能力，降低設備老化與設定異質所造成的安全缺口與故障風險 | |

- **資訊安全教育訓練**

聚賢於每年度 7 月份之大型活動期間，借助公司大型活動的機會定期為全公司同仁進行資訊安全教育訓練。本年度訓練主要聚焦於社交網路詐騙，跟同仁宣導最新的詐騙手法，提供公司對於社交網路工程犯罪的認知。2025 年度亦舉辦一次資訊安全宣導活動加強其資訊安全防護觀念，持續強化全體員工的資安意識與應對能力。

**資訊安全處理流程**

除本公司內稽內控每年度至少一次資訊安全及個資保護控制作業之稽核外，每年度也會有外部稽核稽查，同時若發生重大資訊洩漏情事，依上市公司管理辦法中，進行向上呈報，並啟動緊急應變程序。倘若需要外部協助，將請協力廠商或尋求國內資安組織協助，最後應邀集內部稽核等部門商討處理對策，並於結案後將結果做成紀錄，以供內外部稽核進行查核。

