好德科技股份有限公司
2026 年度資通安全風險管理報告

一、資通安全風險管理架構

資訊部為本公司資安專職單位，資訊主管為資安主管，由資安主管成立跨單位資訊安全推行小組，負責推動、協調及督導公司資訊安全各項事宜，並直接向總經理或其指定代理人報告，以確保資訊安全管理制度有效運作，持續強化公司整體資安防護能力。

二、具體管理方案

（一）落實公司端點裝置資安防護機制

為落實本公司資訊安全管理，資訊部門已建置防火牆，以阻擋外部惡意攻擊及未經授權之網路存取，並於端點設備安裝防毒軟體，加強使用者端之惡意程式偵測與防護能力，降低病毒及駭客攻擊所造成之資安風險。

（二）落實公司網路資安防護機制

透過 Security Agent 提供入侵偵測與防禦、行為監控、惡意程式防護、網頁信譽評等、未知安全威脅偵測及周邊設備存取控管等功能，以確保重要主機及資訊系統安全。並透過其具備之防火牆功能，縮小實體、虛擬及雲端伺服器之攻擊面，藉由精細化過濾規則與網路安全政策，降低系統漏洞遭惡意利用之風險。

（三）落實公司資訊安全管理原則

持續強化資訊安全管理制度，相關措施包括：

1. 提升密碼安全等級，強化帳號與身分驗證管理。
2. 帳號管理規則參照政府組態基準（GCB, Government Configuration Baseline）之安全設定原則。
3. 落實帳號權限區隔及最小權限原則（PoLP, Principle of Least Privilege），降低未經授權存取之風險。
4. 建置重要文件及檔案保護機制，強化機密資訊與重要資料之安全管理。
5. 建置伺服器網路存取紀錄平台，持續監控異常事件及可疑存取行為。

（四）評估資安保險機制

資訊部將視公司實際營運需求、資安風險及成本效益，評估未來投保資安保險之可行性，以降低重大資安事件可能造成之營運損失。

（五）定期執行資安風險評估

定期進行資訊安全風險再評估，檢視現行資安防護措施之適切性與有效性，並依評估結果持續更新相關控管措施。

（六）落實資安稽核、測試與演練

持續實施資訊安全稽核、系統安全測試及緊急應變演練，透過定期檢視與持續改善機制，提升公司資安防護及事件應變能力。

（七）持續強化資安管理制度與未來目標

資訊安全推行小組將持續完善資訊安全相關管理規範，並以取得國際資訊安全認證為長期目標，逐步強化資安管理制度與技術防護機制。同時持續推動員工資訊安全教育訓練與宣導，提升全體員工對資訊安全風險之認知，建立良好之資訊安全文化。

三、投入資通安全管理之內容和資源

資訊安全已成為公司營運的重要議題。為確保資訊系統穩定運作、維護公司及客戶資料安全，並降低潛在資安風險，本公司持續投入相關管理資源，強化資訊安全防護機制。2026 年度資通安全管理執行情形如下：

（一）專責人力

設置「資安專職單位」，負責公司資訊安全規劃、技術導入及相關稽核事項，以維護並持續強化資訊安全管理與防護能力。

（二）資訊安全教育訓練

所有新進員工均於到職前接受資訊安全教育訓練，全體員工每年至少完成一次實體資訊安全教育訓練，藉此提升員工資訊安全意識及資安風險辨識能力。

（三）資訊安全宣導公告

本年度共發布六份資訊安全宣導公告，內容涵蓋釣魚郵件辨識、詐騙郵件防範及資訊安全注意事項，透過實際案例提醒員工留意各類資安威脅，持續強化全體員工之資訊安全防護意識。

（四）資訊安全管理制度與文件維護

為完善資訊安全管理制度、強化內部作業規範及提升營運持續管理能力，本年度新增及修訂以下三份管理文件：

1. 新增「生成式人工智慧（AI）應用管理辦法」：規範員工使用生成式人工智慧工具之原則及注意事項，強化機密資訊與敏感資料保護，降低人工智慧應用所衍生之資訊安全風險。

2. 新增「用印申請與文件管理標準作業程序」：建立用印申請、文件管理及追蹤作業之標準程序，強化文件保存、作業紀錄與管理追溯機制，降低文件遺失及管理疏漏風險。
3. 修訂「好德科技緊急復原計畫」：檢視並更新緊急事件應變與系統復原相關作業程序，以強化資訊系統異常或重大事件發生時之應變及復原能力。

（五）資訊安全基礎建設與防護措施

1. 網路安全防護：持續更新防火牆韌體，並完成 SPAM 郵件安全防護設備及四台防火牆之維護合約（MA）續約，確保網路安全防護機制持續有效運作。
2. 郵件伺服器安全維護：執行 Mail Server 作業系統更新，強化郵件伺服器之系統安全性與穩定性，降低已知漏洞所造成之資安風險。
3. 端點安全管理：持續執行作業系統及相關軟體安全性更新，降低系統漏洞及惡意程式所造成之資安風險。
4. 防毒軟體維護：持續辦理防毒軟體授權續約，維持端點設備之惡意程式偵測與防護能力。
5. 進階資安防護規劃：評估未來導入託管式偵測與回應服務（MDR）之可行性，以提升資安威脅監控、異常偵測及事件應變能力。
6. 資安事件與客戶資料保護：本年度無重大資訊安全事件，亦無因客戶資料遺失而產生之客戶投訴案件，持續維護公司資訊安全及客戶資料保護品質。

（六）資安成效

為強化公司資訊安全治理與監督機制，本年度持續透過管理階層參與、資安專職單位定期會議及內部稽核審查，檢視資訊安全管理措施之執行情形與改善成效。具體成果如下：

1. 董事及獨立董事資安監督：董事及獨立董事參與資安健檢及評核會議共三次，持續關注公司資訊安全管理及風險控管情形。
2. 資安專職單位內部管理：資安專職單位內部成員召開資安會議超過十次，定期檢討資安管理措施、資訊系統防護及相關改善事項。
3. 內部稽核與董事會報告：稽核主管執行資訊安全專案審查，並向董事會提出報告共三次，強化資訊安全管理之監督與查核機制。

（七）第三方資安曝險評級

委託第三方專業資安廠商進行資安曝險評級，針對公司對外資訊服務、網路環境、網域及郵件安全等八大面向進行評估，以客觀檢視外部資安曝險情形。評級結果如下：

評估項目	評級結果	狀態
網站服務安全	96（A）	通過

IP 信譽	99（A）	通過
網路服務安全	98（A）	通過
網域系統安全	99（A）	通過
郵件安全	99（A）	通過
外洩憑證	94（A）	通過
可疑偽冒網域	99（A）	通過
連線安全	99（A）	通過

評級成果：本次八項資安曝險評估均達 A 級標準，全部通過評級要求，平均得分為 97.9 分，顯示公司於本次評估範圍內具備良好的外部資安防護水準。後續將持續關注各項資安曝險指標，並依評估結果強化相關防護措施。