倚天酷碁股份有限公司

資訊安全管理運作及執行情形

本公司為了落實公司資通安全風險管理，建立安全及可信賴之資訊系統，確保資料、系統、設備及網路安全，提升同仁對資訊安全之認知，保障權益，符合資訊安全相關規定，於內部控制訂定「資訊安全檢查」等相關政策；另為強化公司資訊安全管理機制，業已依「公開發行公司建立內部控制制度處理準則」規定，於本年度成立資訊安全專責單位，設置有 1 名資訊安全專責主管及 1 名資訊安全專責人員，以負責推動、協調監督及審查資通安全管理事項，定期檢討資安政策，並於 2025 年 3 月 11 月董事會報告**資安管理運作及執行情形**。

本公司為落實資通安全風險管理，建立安全且可信賴之資訊系統，以確保資料、系統、設備及網路之安全，並提升同仁對資訊安全之認知、保障公司與利害關係人之權益，於內部控制制度中訂定「資訊安全檢查」等相關政策與規範。另為強化公司資訊安全管理機制，已依《公開發行公司建立內部控制制度處理準則》之規定，於本年度成立資訊安全專責單位，設置 1 名資訊安全專責主管及 1 名資訊安全專責人員，負責推動、協調、監督及審查資通安全相關管理事項，並定期檢討及精進資安政策。

本公司並依循總部之資通安全政策，完成伺服器盤點、資安自評、建立外部網域清單及對外網站與服務清單，並執行伺服器作業系統弱點掃描、對外網站及網路弱點掃描及滲透測試，同時持續進行弱點修復作業。此外，亦持續辦理內部資安教育訓練與釣魚郵件演練，以強化員工之資安意識與防護能力。相關資安管理運作與執行情形，已於 2025 年 3 月 11 日向董事會報告。

管理機制：

1. 於內部控制制度中，訂定「資通安全檢查」，並定期檢視此規範之有效性。
2. 本公司因向關係人宏碁公司租用辦公用地，享有其提供的網路佈建及運作維護等服務，另本公司現有營運支援處編制有 4 位資訊管理人員，由本公司資安主管偕同出租人宏碁公司辦理年度資安檢查。
3. 加強員工資訊安全概念，定期宣導資訊安全之重要性，嚴格管理資料之利用與安全維護。
4. 為使資訊系統損害發生時能儘速順利恢復業務，降低可能的損失與風險，本公司制定「資料備份機制」及「災難復原計劃」，以確保資訊系統之正常運作及資料保全，並降低無預警天災及人為疏失造成之系統中斷風險。
5. 為確保資訊系統安全，資料的存取需經適當的授權，並定期檢查授權是否允當，以防範

機密資料外流之風險。

運作及執行情形：

1. 定時備份各資訊系統及異地備援，並於每年定期進行資訊系統復原演練測試，以確保資訊系統之正常運 作及資料保全，降低無預警天災及人為疏失造成之系統中斷風險 。
   (2025.05.02 完成資料庫系統復原演練)
2. 建置各種資安技術控管方案，包括網路防火牆、防毒系統、防垃圾郵件等系統，並每月定期檢視防火牆政策設定，確保各項 allow/deny 規則正確有效。
3. 增加資訊資料保護保險(CYBER EDGE)，以分散可能的風險損失，並調整資料庫網段區隔，避免非授權主機存取系統資源。
4. 定期執行社交工程演練，宣導同仁最新詐騙釣魚郵件型態，避免同事誤觸；每年上下半年各執行一次釣魚郵件演練，另於 2025 年 4 月完成紅隊演練，並依演練結果進行弱點修補。
5. 強化各系統密碼複雜度及安全性設定，以降低遭駭客入侵之風險，並配合總部規範導入單一登入機制（Single Sign-On）、雙重驗證（2FA）及限制特定 inbound IP 等控管措施。
6. 定期檢視並整理各資訊系統使用帳號，停用未使用或不必要之帳號，以確保無未經授權之存取；每月定期檢視機房 VPN 使用帳號，並不定期檢視 ERP 系統帳號權限。
7. 本年度全面更新同仁使用設備為公司配發之公務設備，以提升整體資訊安全防護能力；非公司配發設備不得連線公司內網或 VPN，新購辦公設備均須由 IT 完成安全設定後始得交付使用。
8. 不定期辦理資訊安全宣導，以提升同仁資安意識並降低資安事件發生風險，內容包括員工電子郵件資安教育、社交工程防範宣導及軟體使用規範說明。
9. 導入防火牆入侵防禦系統（Firewall IPS）及入侵偵測系統（IDP），以強化網路監控及防護能力，提升整體網路使用之安全性。
10. 將網站連線機制由 HTTP 升級為 HTTPS，並落實 HSTS（HTTP Strict Transport Security）機制，以確保資料傳輸安全並強制導向加密連線。
11. 導入 NAC（Network Access Control）系統以強化設備存取控管能力，並由宏碁公司提供 UEM、CrowdStrike 及 Forescout 等工具進行設備合規性與安全性管理。
12. 定期執行軟體資產盤點，以確保軟體合法授權及版本控管，每年至少盤點一次，未具授權證明之軟體須強制移除，以維持軟體使用之合規性。

13. 透過定期參與內外部資訊安全教育訓練及宣導課程，持續提升資安人員對資安風險型態