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，並規畫於年度屆滿首次董事會報告執行情形。

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。
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。
3. 增加資訊資料保護保險(CYBER EDGE)，以分散可能的風險損失。
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。
5. 提高及改善各系統的密碼複雜度及安全性設定，降低被駭客攻擊的風險。
6. 定期檢視整理各系統使用帳號，停用無用的帳號確保無未經授權的存取。
7. 本公司於今年度全面更新同仁設備為公發設備，以提高資安防護效能。
8. 不定期進行資通安全宣導，提高同仁資安相關意識。以減少資通安全事件的發生。
9. 導入 FIREWALLIPS（入侵防禦系統）、IDP(入侵偵測系統)功能。提升網路使用的安全性。
10. 網站連線由 http 轉換成 https。提升資料傳遞的安全性。
11. NAC 系統導入，提升設備控管的能力，確保設備的合規性。
12. 進行軟體相關盤點工作，確保軟體的合法性及版本相關控管工作。
13. 藉由定期內、外部資通安全教育訓練課程與宣導會的參與，達到資安人員對資安風險型態的知識、防範與法令資訊的更新。