弘裕企業股份有限公司

資通安全風險管理政策與執行情形

一、 本公司為強化資通安全管理，確保資料、系統、設備及網路安全，特訂定資通安全管理政策，達到資通安全風險管控之目的。

二、 為統籌資通安全管理等事項之推動及運作之有效性，成立跨部門之資通安全風險管理委員會，各業務相關單位配合執行，其幕僚作業由資管中心負責。

三、 資通安全政策訂定相關管理規範或實施計畫之風險管控事項如下，並定期評估實施成效：

3.1 人員管理及資通安全教育訓練。

3.1.1 對資通相關職務及工作，應進行安全評估，並於人員進用、工作及任務指派時，審慎評估人員之適任性，並進行必要的考核。

3.1.2 針對管理、業務及資通等不同工作類別之需求，應定期辦理資通安全教育訓練及宣導，建立員工資通安全認知，提升資通安全水準。

3.2 電腦系統安全管理。

3.2.1 辦理資通業務委外作業，應於事前研提資通安全需求，明訂供應商之資通安全責任及保密規定，並列入契約，要求遵守並定期考核。

3.2.2 對系統變更作業，應建立控管制度，並建立紀錄，以備查考。

3.2.3 複製及使用軟體應依相關法規或契約規定，並建立軟體使用管理制度。

3.2.4 為確保系統正常運作，應採行必要的事前預防及保護措施，偵測及防制電腦病毒及其他惡意軟體。

3.3 網路安全管理。

3.3.1 開放外界連線作業之資通系統，應視資料及系統之重要性及價值，採用資料加密、身分鑑別、電子簽章、防火牆及安全漏洞偵測等不同安全等級之技術或措施，防止資料及系統被侵入、破壞、竄改、刪除及未經授權之存取。必要時應以代理伺服器等方式提供外界存取資料，避免外界直接進入資通系統或資料庫存取資料。

3.3.2 與外界網路連接之網點，應以防火牆及其他必要安全設施，控管外界與內部網路之資料傳輸與資源存取。

3.3.3 利用網際網路及全球資通網公布及流通資訊，應實施資料安全等級評估，機密性、敏感性及未經當事人同意之個人隱私資料及文件，不得上網公布。

3.3.4 訂定電子郵件使用規定，機密性資料及文件不得以電子郵件或其他電子方式傳送。機密性資料以外之其他具敏感性資料及文件，如有電子傳送之需要，應視需要以適當的加密或電子簽章等安全技術處理。

3.4 系統存取控制。

3.4.1 系統存取政策及各級人員之存取權限應予明確規定，並以書面、電子或其他方式告知員工及使用者之相關權限及責任。

3.4.2 離（退）職人員，應立即取消各項資通資源之所有權限，並列入離（退）職之必要手續。人員職務調整及調動，應依系統存取授權規定，限期調整其權限。

3.4.3 為加強作業系統之安全管理，應建立系統使用者註冊管理制度，並落實使用者通行密碼管理，使用者通行密碼之更新周期，最長以不超過六個月為原則。

3.4.5 開放外界連線作業，應事前簽訂契約或協定，明定其應遵守之資通安全規定、標準、程序及應負之責任。

3.4.6 對系統服務廠商以遠端登入方式進行系統維修者，應加強安全控管，並建立人員名冊，課其相關安全保密責任。

3.4.7 重要資料委外建檔，不論在機關內外執行，均應採取適當及足夠之安全管制措施，防止資料被竊取、竄改、販售、洩漏及不當備份等情形發生。

3.4.8 為維護資通安全，應建立資通安全稽核制度，定期或不定期進行資通安全稽核作業。

3.5 系統發展及維護安全管理。

3.5.1 自行開發或委外發展系統，應在系統生命週期之初始階段，即將資通安全需求納入考量；系統之維護、更新、上線執行及版本異動作業，應予安全管制，避免不當軟體、暗門及電腦病毒等危害系統安全。

3.5.2 對廠商之軟硬體系統建置及維護人員，應規範及限制其可接觸之系統與資料範圍，並嚴禁核發長期性之系統辨識碼及通行密碼。如基於實際作業需要，得核發短期性及臨時性之系統辨識及通行密碼供廠商使用，但使用完畢後應立即取消其使用權限。

3.5.3 委託廠商建置及維護重要之軟硬體設施，應在本公司相關人員監

督及陪同下始得為之。

3.6 資通資產安全管理。

3.6.1 資通資產應建立目錄，訂定資通資產的項目、擁有者及安全等級分類等。

3.6.2 建立資通安全等級之分類標準，以及相對應的保護措施。

3.6.3 已列入安全等級分類的資通及系統之輸出資料，應標示適當的安全等級以利使用者遵循。

3.7 實體及環境安全管理。

就資通相關設備安置、周邊環境及人員進出管制等，應訂定實體及環境安全管理措施。

3.8 業務永續運作計畫之規劃與管理。

3.8.1 訂定業務永續運作計畫，評估各種人為及天然災害對業務運作之影響，訂定緊急應變及回復作業程序及相關人員之權責，並定期演練及至少每年一次調整評估更新計畫。

3.8.2 為維業務正常運作，對資通安全事件應建立緊急處理機制，在發生資通安全事件時，應依規定之處理程序，立即向資管中心或資安防護組通報，採取反應措施，並聯繫檢警調單位協助偵查。

四、 114 年執行情形：

4.1 員工資通安全教育訓練，(於 114/6 月, 11 月週會講習及電子郵件宣導)。

4.2 使用者電腦權限查核。(每月自動查核)。

4.3 網頁應用程式主機安全弱點掃瞄（結果：風險低）114/10。

4.4 雲端異地備份：10T 空間採用 AES-256 加密備份 114/6。

4.5 導入 NOC 與 SOC 網路維運與資安監控收集分析 114/4。

4.6 郵件系統執行兩階段認證 114/4。

4.7 完成上市櫃公司資安教育訓練課程與資訊安全大會 114/5 月。

4.8 社交工程演練。114/9 月。