資通安全管理

(一) 資通安全風險管理架構、資通安全政策、具體管理方案及投入資通安全管理之資源

1. 資安管理架構：

2. 本公司資通安全之權責單位為資訊課，統籌公司資訊安全政策，宣導資訊安全相關訊息，並符合現行法律、法規需求適時調整，以確保本公司資通安全、系統符合機密性、完整性、可用性之要求。

(二) 資通安全政策

1. 目標為「確保永續發展及保護公司相關業務資訊之機密性、完整性及可用性，避免遭受外洩、破壞及遺失等任何形式的威脅。
   (1) 資訊資產之機密性、完整性、可用性。
   (2) 確保系統存取的管制。
   (3) 避免未經授權修改或使用資料與系統。
   (4) 定期執行查核。
2. 員工應遵守相關規定
   (1) 若收到來路不明的電子郵件，不宜隨意打開電子郵件，以免啟動惡意執行檔，使個人電腦遭到破壞，並請立即告知資訊人員處理。
   (2) 員工個人帳號皆須先填寫帳號申請單，資訊人員收到後才會建立其帳號。
   (3) 員工不得將帳號及密碼交由他人使用。
   (4) 員工應遵守本公司訂定的網路規範，如有違反相關規定，則依規定處理。

(三) 具體管理方案

1. 網路資安管控

   建立防火牆、安全網路架構等網路資安措施，加強對外網路的監控與管控，並建置 VPN 以確保資料傳遞的保密性與安全性；並同時針對公司內部網路建立存取控制機制，限制非授權人員存取公司機密資料，且使用者調整職務或離職（退休）時，立即註銷其系統存取權限。

   (1) 防火牆、防毒軟體：自動更新防火牆及防毒軟體，降低病毒感染機會。
   (2) 郵件過濾機制：保護郵件系統免受垃圾郵件、惡意連結和惡意附件的影響，有效地過濾和阻止垃圾郵件的傳遞，減少用戶的郵件信箱中的垃圾郵件量，並能夠檢測和隔離含有病毒的郵件附件，避免病毒在內部傳播，以防止用戶被引導到惡意網站或受到釣魚攻擊。
   (3) 機房進出管制:機房進出須填寫機房進出登記簿,必要時需要進行追蹤與調查，也需經過授權才能進入機房，未經授權者禁止進入。
   (4) 每月定期 E-MAIL 資安郵件宣導，提高同仁對於資訊安全風險的認識。

2. 資料存取管控

   本公司針對各部門之資料權限進行評估，依據資訊分類與等級將資料進行分級管控，依執行業務之需求,賦予使用者系統存取權限,以確保重要機密資料得到適當保護。

本公司落實員工存取資料之審核流程，掌握資料存取紀錄，且本公司採用最小權限原則管理公司內部系統及資料的存取權限，非經授權亦無法檢視。

確保只有授權人員才能夠訪問和管理硬體設備，系統管理員必須定期審查和管理訪問權限，以確保授權人員能夠適當地訪問和管理硬體設備。

3. 資料備份機制

本公司使用 16 卷磁帶來進行備份，磁帶備份的具體分配如下：

（1）系統備份：

使用 2 卷磁帶，用於「每半年一次」，這些磁帶將用於對系統進行完整備份，包括作業系統、應用程式及核心配置，確保在重大故障或災難發生時能夠迅速恢復整個系統。

（2）軟體備份：

使用 4 卷磁帶，用於 「每三個月一次」，專門用來定期備份公司使用的軟體及其配置，保護公司應用程式資料，防止丟失或損壞。

（3）資料庫備份：

使用 10 卷磁帶，用於「每天備份」，每天進行資料庫的增量或差異備份備份，確保資料的最新性與完整性，並最大程度減少資料丟失風險。

（4）災難復原機制：

資料備份也和災害復原機制結合，以確保遇到災害時，備份資料可以即時供應並快速復原。

(四) 投入資通安全管理之資源

1. 資安團隊建置：

公司投入 2 名資安人員，負責資訊安全政策執行、資安事件調查與處理及回應、威脅分析、資安內部意識訓練，以及軟硬體及資安架構評估及導入。

2. 資安設備與授權投入：

投入資安相關防毒授權、垃圾郵件過濾更新、維護合約及設備等投入共計新台幣 150 萬元。

3. 資安風險檢視：

每月定期內部召開資安會議，檢視資安風險並進行矯正。

4. 災害復原演練：

年度內共執行 1 次災害演練，驗證備份與還原機制之適行性。

5. 防毒防護：

透過防毒端點防護機制(Kaspersky Endpoint)，114 年 12 月成功攔截 135 次惡意攻擊。

6. 垃圾郵件防護：

透過郵件防護，114 年度成功攔截 151,020 封垃圾郵件及隔離 8,249 封威脅郵件。

7. 資安健檢：

透過弱點掃描、網站滲透測試與釣魚信件等方式進行年度資安健檢，共執行 2 次、複查 1 次。測試人數共 430 人、複查人數 100 人。

8. 資安宣導：

透過內部通報與郵件定期進行資安宣導，年度累計 12 則。

9. 專業訓練與證照：

年度內相關資訊人員共取得 1 張資安相關(稽核)證照，並累計 40 小時資安專業訓練時數。

(五) 列明最近年度及截至年報刊印日止，因重大資通安全事件所遭受之損失、可能影響及因應措施，如無法合理估計者，應說明其無法合理估計之事實：無。