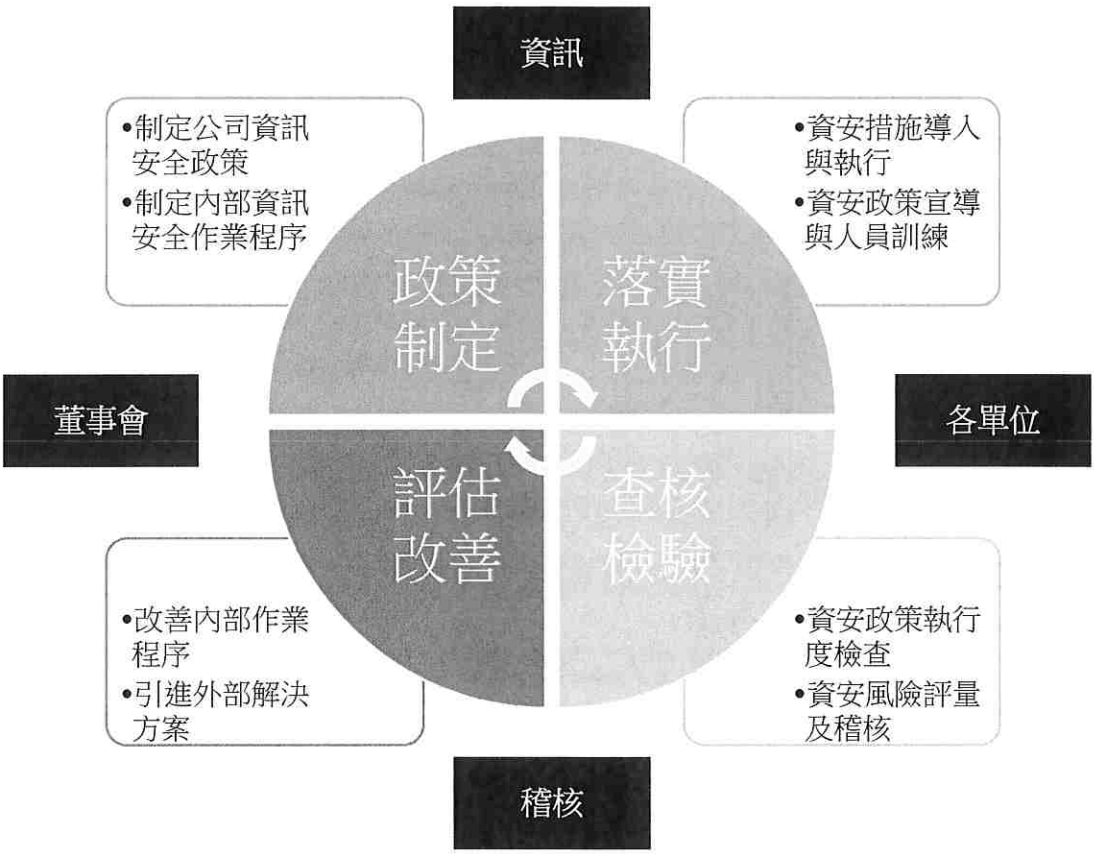
# 資通安全治理暨風險評估報告

一、資通安全管理策略與架構

本公司為配合國家資通安全政策、強化公司內部資訊安全管理，以確保所屬之資訊資產的機密性、完整性及可用性及資訊業務持續運作之資訊環境，並符合相關法規之要求，制定相關資安管理辦法規範。

I. 資通安全風險管理架構

本公司稽核人員每年定期查核，若查核發現缺失，即要求提出改善措施，且追蹤改善結果，以降低內部資安風險。資訊安全管理策略採用 PDCA（Plan-Do-Check-Action）循環流程管理模式，確保可靠度目標之達成且持續改善。




II. 資通安全政策

本公司資訊安全政策，包含制度規範、科技運用、人員訓練三個面向：

1. 制度規範：訂定公司資訊安全管理制度，規範人員作業行為
2. 科技運用：建置資訊安全管理設備，落實資安管理措施
3. 人員訓練：進行資訊安全教育訓練，提昇全體同仁資安意識

III. 具體管理方案

1. 制度規範： 本公司訂有多項資安管理辦法及措施，以規範本公司人員資訊安全行為，並定期執行內部稽核及資安自評，並由會計師進行資訊、資安查核，以檢視相關規定是否符合營運環境變遷，依需求適時調整。
2. 科技運用： 本公司為防範各種外部資安威脅，除採多層式網路架構設計外，更使用中華電信資安艦隊的多項服務，以提昇整體資訊環境之安全性。
3. 人員訓練：本公司定期實施員工的資訊安全教育訓練課程，資訊人員持續參加資安研討會或外部課程，藉以提昇本公司人員資安知識與專業技能。

IV. 投入資通安全管理之資源

本公司每季以時事案例做為資通安全宣導，為加強資訊安全，民國 112 年已編列預算強化資訊安全防護，且每年定期向董事會報告資通安全管理及執行成果。

二、資通安全風險與因應措施

I. 權限管理：人員權限帳號管理與審核及定期盤查與複核

II. 存取控管：File Server 的帳號管控存取、資料傳輸的管道控管，密碼混合編碼及定期變更要求。

III. 外部威脅：中華電信資安艦隊的 UTM 防火牆端點防護、防駭守門員企業版及入侵防護服務

IV. 系統可用性：使用 NAS 資料備份及異地備援措施、定期災害還原演練

三、重大資通安全事件

近年度及截至董事會開會前為止，無發生重大資通安全事件導致任何損失及影響。

以下為本公司資安事件等級說明：重大資安事件為第二、三級

| 等級 | 說明 | 影響範圍 | 通知層級 |
|---|---|---|---|
| 第一級 | 單獨電腦 | 個人電腦、資料 | 資安窗口→資安主管、單位主管 |
| 第二級 | 辦公室區域 | 個人電腦、資料、伺服器、網路設備、資料庫 | 資安窗口→資安主管、部門主管→總經理 |
| 第三級 | 全公司 | | |

四、資通安全風險管控措施

本公司對資安風險之管控以內部控制為基礎，參考外部實例或廠商建議而持續改進，所採取之管控措施(如下表)乃衡量經營管理階層對營運宗旨與企業價值之共識，針對核心業務及重要工作之發展進程，依 ISACA 國際電腦稽核協會台灣分會之"資通安全公司自我檢查表"的 10 個分類於每年定期自我評估及分析後，依據其中風險性較高的部份進行檢討及擬具改善措施，從系統面、技術面、程序面，對已知之威脅採取適當之處理方法，對潛藏之威脅盡可能予以事前分析及鑑別，以保護公司資訊財產的機密性、可用性及完整性，避免遭受各種威脅及降低可能的危害或損失，以提升本公司承受外部攻擊之防護能力及應變彈性，減緩衝擊等級及降低可能造成的損害，妥善因應風險。

| 項次 | 資安管理分類 | 重要管控及防護措施 | 執行頻率 |
|---|---|---|---|
| 1 | 資訊安全政策 | 1.明定資安組織、權責及事件之通報、處理綱要。 | 檢視 1 次/年 |
| | | 2.定期審查、修訂資訊安全政策。 | |
| 2 | 建立資訊安全組織 | 1.設資安管理小組及個人資料保護小組。 | 年 |
| | | 2.訂立資安事件之緊急應變處理及回報程序。 | 次 |
| 3 | 人員安全與管理 | 1.內部控制制度定義資訊人員、使用者之作業權限劃分，及人員異動、離職之作業準則。 | 檢視 1 次/年 |
| | | 2.每半年執行作業權限複核。 | 半年 |
| | | 3.每年定期普查個人電腦，防止公器私用。 | 年 |
| 4 | 資產分類與控管 | 1.資訊類軟、硬體資產列冊管理。 | 年 |
| | | 2.每年定期普查電腦，確認軟、硬體資產。 | 年 |

| 項次 | 資安管理分類 | 重要管控及防護措施 | 執行頻率 |
|---|---|---|---|
| 5 | 實體及環境安全管理 | 1.專用電腦機房具溫度、電力自動控管。 | 日 |
| | | 2.伺服器及個人電腦安裝防毒軟體，重要職務之電腦，每日定時備份，其備份份數至少二代。 | 日 |
| | | 3.異地備份機制。 | 週 |
| | | 4.對重要伺服器或網路設備定期弱點掃瞄。 | 年 |
| 6 | 通訊與操作管理 | 1.電子郵件主機具自我防護及保存稽核之功能。 | 週 |
| | | 2.每日分析防火牆紀錄，並使用趨勢雲端防毒防駭軟體分析、記錄上網行為，即時防堵內、外部異常行為。 | 日 |
| | | 3.即時宣導資安事件、通告或案例，提升防護意識。 | 季 |
| | | 4.使用 Hinet 資安艦隊之防駭守門員、先進網路防禦等服務，擴展防禦的廣、深度，防堵內、外之攻擊。 | 週 |
| 7 | 存取控制 | 1.電子檔資料依部門、個人設定存取權限。 | 不定期 |
| | | 2.對外連線作業申請需經透過電話或 mail 通知。 | 不定期 |
| | | 3.電子郵件區分權限，不須對外連絡者僅能內部寄信。 | 需申請 |
| | | 4.人力資源系統於讀取個資時，自動記錄存取軌跡。 | 不定期 |
| 8 | 系統開發與維護 | 應用系統為套裝軟體，委外開發、維護，在更新程式及系統時，限制連線方式及時間，防範外部的侵入篡改。 | 不定期 |
| 9 | 永續運作之計畫管理 | 1.營運資料庫定期模擬事故演練、測試。 | 季 |
| | | 2.重要設備訂立緊急應變計劃，供發生重大資安事件時遵循及應變。 | 需要時執行 |
| 10 | 內部稽查及其它 | 1.每年電腦普查時告知公司軟體所授權之範圍，規範以外之軟體則要求移除或提供授權證明；軟、硬體普查資料，隨時依資產狀況更新。 | 年 |
| | | 2.資訊單位每年定期自評資訊作業環境安全。 | 年 |
| | | 3.內部稽核人員及會計師每年定期稽查資訊控制作業。 | 年 |

對上列管控措施在執行上的達成度或完整度評量，共分為五級的成熟度：完整、良好、尚可、待加強、差，2023 年度於 2023 年 12 月完成自評為”尚可”，自評報告經資安主管及總經理核閱，並依據風險性較高的部份進行檢討及擬具改善措施

五、資訊安全風險評鑑

針對選定範圍的資訊資產進行全面性的風險評鑑，依據評鑑結果及安全要求選定控管措施，風險評鑑進行方式依據資訊安全風險作業程序，透過系統化的風險評鑑作業，以確定安全要求，且透過評估資產可能的資訊安全弱點與威脅，釐清面臨之風險，以利於日後能清楚識別將面對之處境及需要加強之控制，以確保本公司各資訊資產之機密性、完整性與可用性，同時維持業務正常運作，本公司所提供的人員、服務、資訊紀錄、電腦系統及實體設備等部份，皆屬於本次風險評鑑之範圍。

I. 資訊資產風險辨識評估

綜合本作業於民國 112 年執行風險評鑑作業之資訊資產辨識與價值評估，結果辨識出 43 項資訊資產並依據資產價值及特性，整合為 5 類群組資訊資產，計識別出 64 項風險組合，請參考附錄 6-3 資訊資產清單、6-4 資訊風險值評估表，分析如下：

1. 資訊及資通系統資產價值：取機密性、完整性、可用性中最高值_1=低、2=中、3=高

| 資訊及資通系統資產 | 資產類別 | 機密性 | 完整性 | 可用性 | 資訊及資通系統資產價值 |
|---|---|---|---|---|---|
| 一般使用者 | 人員 | 中 | 中 | 低 | 2 |
| 管理者(各單位主管) | 人員 | 中 | 中 | 中 | 2 |
| 決策者(一級主管) | 人員 | 高 | 高 | 中 | 3 |
| 資訊設備決策者 | 人員 | 高 | 高 | 中 | 3 |
| 資訊設備管理者 | 人員 | 高 | 高 | 中 | 3 |
| 中華電信 60M/20M(台北) | 服務 | 低 | 中 | 中 | 2 |
| 中華電信雙向 100M(彰化) | 服務 | 低 | 中 | 高 | 3 |
| 亞太電信專業型雙向 10M(彰化) | 服務 | 低 | 中 | 中 | 2 |
| 中華電信 100M/40M(宿舍) | 服務 | 低 | 低 | 低 | 1 |
| 交換式集線器 | 服務 | 低 | 中 | 高 | 3 |
| 防火牆 | 服務 | 高 | 中 | 高 | 3 |
| 電腦化資訊管理作業 | 資訊紀錄 | 中 | 中 | 低 | 2 |
| 電腦系統使用權限複核 | 資訊紀錄 | 中 | 低 | 低 | 2 |
| 軟硬體清單 | 資訊紀錄 | 中 | 低 | 低 | 2 |
| 備份紀錄 | 資訊紀錄 | 低 | 低 | 中 | 2 |
| 緊急應變計畫一覽表 | 資訊紀錄 | 中 | 低 | 低 | 2 |
| 年度資訊作業環境安全稽查報告 | 資訊紀錄 | 中 | 中 | 低 | 2 |
| 作業層級內部控制自行檢查表 | 資訊紀錄 | 中 | 中 | 低 | 2 |
| 資訊環境基本資料表 | 資訊紀錄 | 中 | 中 | 低 | 2 |
| 廠商合約書<br>(ERP 系統、租賃印表機、設備維護、網站、防毒) | 資訊紀錄 | 中 | 中 | 低 | 2 |
| ERP 系統資料庫 | 資訊紀錄 | 中 | 中 | 高 | 3 |
| 海鷗系統資料庫 | 資訊紀錄 | 中 | 中 | 高 | 3 |
| Windows AD 伺服器之 User 資料夾 | 資訊紀錄 | 中 | 低 | 中 | 2 |
| Windows AD 伺服器之 Groups 資料夾 | 資訊紀錄 | 中 | 中 | 中 | 2 |
| Windows AD 伺服器之 Sharedoc 資料夾 | 資訊紀錄 | 中 | 中 | 中 | 2 |
| Windows 資料庫伺服器之 MIS 資料夾 | 資訊紀錄 | 中 | 中 | 中 | 2 |
| Windows 資料庫伺服器之海鷗系統資料夾 | 資訊紀錄 | 中 | 中 | 高 | 3 |
| Windows 資料庫伺服器之 ERP 系統資料夾 | 資訊紀錄 | 中 | 中 | 高 | 3 |
| 作業系統(Windows+Linux) | 電腦系統 | 低 | 中 | 高 | 3 |
| 文書軟體(Office) | 電腦系統 | 低 | 中 | 中 | 2 |
| ERP 系統(銷售、採購、庫存、財務、生產) | 電腦系統 | 中 | 中 | 高 | 3 |
| 海鷗系統(客訴、物性) | 電腦系統 | 中 | 中 | 高 | 3 |
| 人事考勤系統(震旦行) | 電腦系統 | 中 | 中 | 中 | 2 |
| 防毒軟體(趨勢科技) | 電腦系統 | 低 | 中 | 中 | 2 |
| 個人電腦(PC、NB) | 實體設備 | 中 | 中 | 低 | 2 |
| 伺服器(Server) | 實體設備 | 中 | 中 | 中 | 2 |

| 資訊及資通系統資產 | 資產類別 | 機密性 | 完整性 | 可用性 | 資訊及資通系統資產價值 |
|---|---|---|---|---|---|
| 儲存設備(NAS) | 實體設備 | 中 | 中 | 中 | 2 |
| 不斷電設備(UPS) | 實體設備 | 低 | 低 | 低 | 1 |
| 考勤刷卡設備 | 實體設備 | 中 | 中 | 中 | 2 |
| 列印設備(印表機、影印機、標籤機) | 實體設備 | 低 | 中 | 中 | 2 |
| 彰化廠-行政大樓 | 實體設備 | 低 | 高 | 高 | 3 |
| 彰化廠-生產大樓 | 實體設備 | 低 | 高 | 高 | 3 |
| 台北總公司 | 實體設備 | 低 | 高 | 高 | 3 |

2. 威脅分析：等級區分 3 級，最低 1 最高 3

平均值 - 威脅等級　　資產類別

| 威脅 | 人員 | 服務 | 資訊紀錄 | 電腦系統 | 實體設備 |
|---|---|---|---|---|---|
| 入侵_CIA | | | | 3 | |
| 中斷_A | | 3 | | | |
| 火災_IA | | | | | 3 |
| 未授權存取資料_CI | 2 | | | | 2 |
| 地震_IA | | | | | 3 |
| 作業人員或使用者錯誤_I | 2 | | 3 | 2 | 1 |
| 作業失能_IA | | | 2 | | |
| 技術失能_IA | | | | 2 | 1 |
| 使用盜版軟體_I | | | | 2 | |
| 委外作業失能_IA | | | 2 | 3 | 2 |
| 破壞_IA | | | | 2 | |
| 軟體程式錯誤_IA | | | | 2 | |
| 通訊服務失能_A | | | | | 2 |
| 惡意破壞資料與設施_IA | | | 2 | | 3 |
| 資料外洩_C | | | 2 | | |
| 電力供給失能_A | | | | | 2 |
| 誤傳_I | 2 | | | | |
| 罷工_A | 3 | | | | |
| 請假_A | 2 | | | | |
| 竄改或任意變更_I | 2 | | | | |
| 離職或更換頻繁_A | 2 | | | | |

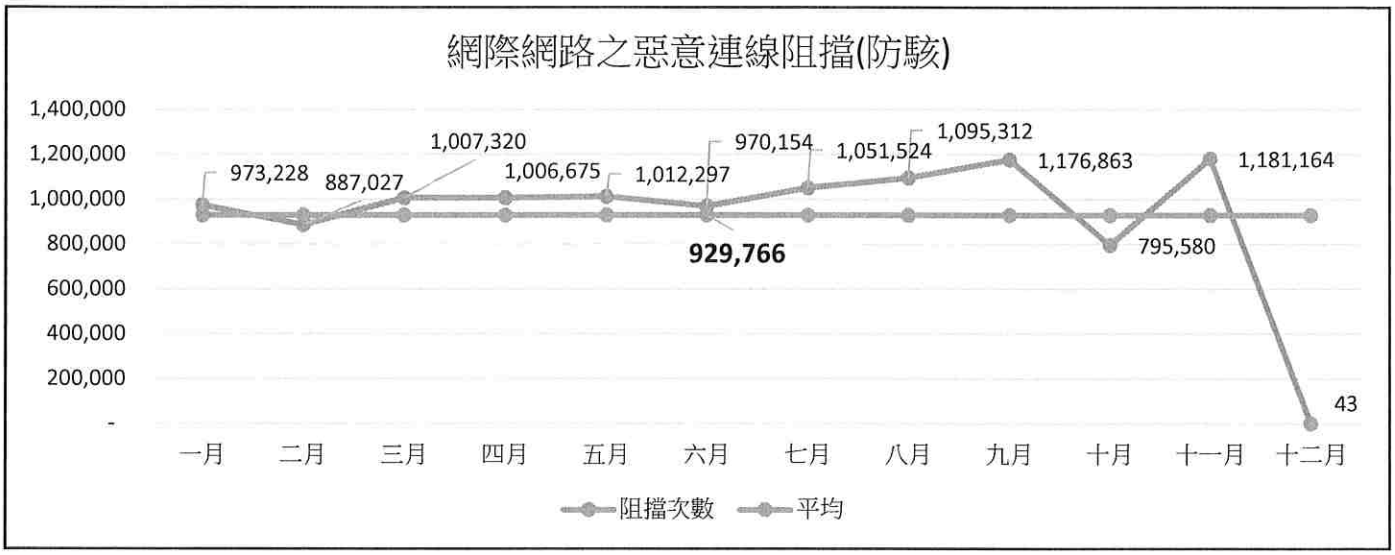
3. 脆弱分析：等級區分 3 級，最低 1 最高 3

| 平均值 - 脆弱等級 | 資產類別 | | | | |
|---|---|---|---|---|---|
| 脆弱性 | 人員 | 服務 | 資訊紀錄 | 電腦系統 | 實體設備 |
| 不清楚或不完整之開發規格。 | | | | 1 | |
| 未更新或安裝作業系統/軟體的修補程式。 | | | | 2 | |
| 未釐清委外協議的權責。 | | | 1 | | |
| 由於不當的規劃或維護而導致網路容量不夠。 | | | | | 2 |
| 交接資料不足或未建立 | 1 | | | | |
| 存取權限不對。 | | | | 1 | |
| 系統無法接收資料。 | | | | 2 | |
| 使用易燃性之材質，如紙箱或產品。 | | | | | 1 |
| 使用者認知不足。 | 3 | | 1 | 1 | 3 |
| 非單位內人員進出未有適當人員陪同。 | 1 | | | | |
| 保存不當 | | | 1 | | |
| 缺少自動滅火系統。 | | | | | 1 |
| 缺少軟體稽核。 | | | | 2 | |
| 缺少實體安控。 | 2 | | | | |
| 缺乏勞資協議。 | 1 | | | | |
| 缺乏溝通導致離職同仁可存取系統。 | | | 2 | | 2 |
| 缺乏職務代理能力 | 2 | | | | |
| 設備故障。 | | 2 | | | |
| 備份失效 | | | 1 | | |
| 備份檔案或系統無法使用。 | | | | | 2 |
| 傳輸機密資料未加適當防護。 | 1 | | | | |
| 資料分級錯誤或處理不當。 | | | 2 | | |
| 電力供應設備容量不足。 | | | | | 2 |
| 對有計畫的破壞行動缺乏懲戒處分。 | | | | | 2 |
| 維護不當。 | | 1 | | | |
| 網路連線設備故障 | | | | | 1 |
| 網路管理不足(路徑彈性)。 | | | | | 2 |
| 廠商無法及時提供設備。 | | | | | 2 |
| 變更管理流程失誤。 | | | | 2 | 1 |

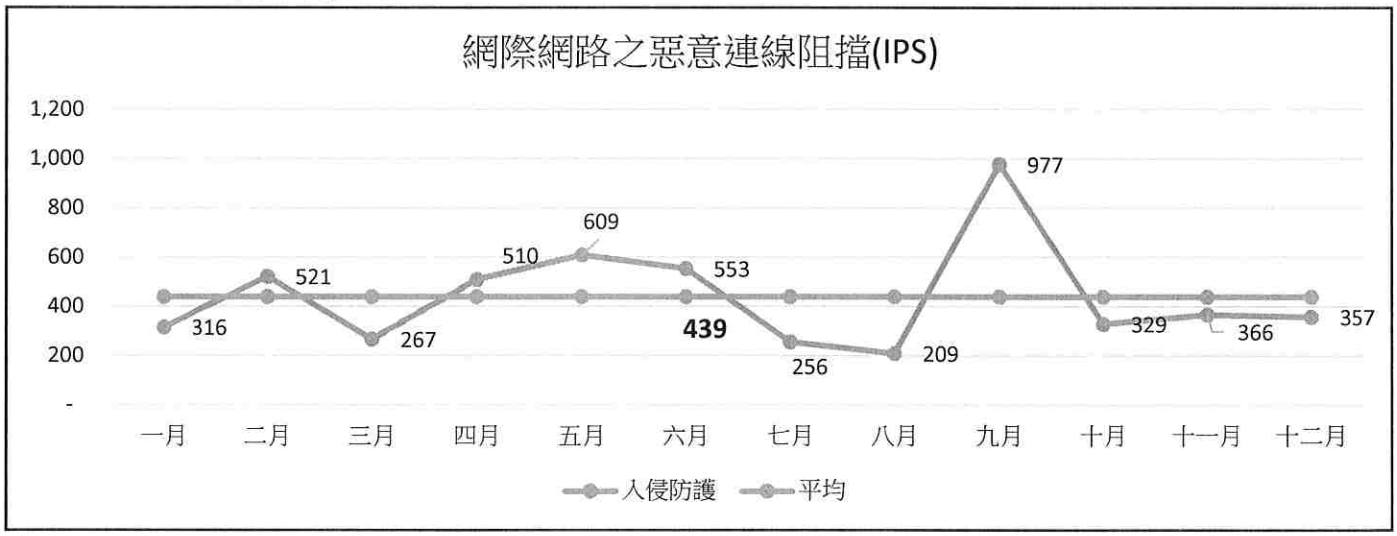
II. 資安之防禦成效

本公司導入中華電信資安艦隊之防護解決方案，以利即時防堵網路攻擊之行為，其定期產生防護報告均明確呈現已阻擋之威脅數目，將此基礎資料依風險程度予以量化，以表達對既有風險之管控成效，並做為日後改善措施之參考，請參考 6-1 防駭守門統計表、6-2 入侵防護偵測統計表。

1. 防駭守門員(因中華電信調整防護設備，故 12 月降低駭客攻擊)




2. 入侵防護偵測




3. 滲透測試

依據「上市上櫃公司資通安全管控指引」中指示，本公司每年定期辦理滲透測試，滲透方式採寄送偽造的釣魚郵件進行社交工程演練，演練期間：2023-10-23～2023-10-27、統計期間：2023-10-23～2023-10-30、演練帳號數：合計 45 帳號、測試信件 3 封，演練分析結果如下：

| 演練帳號數 | 開啟信件 | | 點閱連結 | | 開啟附件 | |
|---|---|---|---|---|---|---|
| | 帳號數 | 比率 | 帳號數 | 比率 | 帳號數 | 比率 |
| 45 | 6 | 13.3% | 0 | 0.0% | 5 | 11.1% |
| 45 | 6 | 13.3% | 0 | 0.0% | 5 | 11.1% |

針對開啟信件及附件的人員已於 2023/11/14 進行資通安全教育訓練，再次訓練同仁對不明來源的郵件，保持警覺、控制好奇心、勿任意點連結及開啟圖檔。

III. 風險等級評鑑

依 6-4 資訊風險值評估表分析出風險等級和資產類別的風險值及風險分佈，分析如下：

1. 風險等級分級：

為求風險等級之分級更為明確，特將風險區分為三個等級，說明如下表：

| 風險等級 | 風險接受 | 等級說明 |
|---|---|---|
| 高 | 不可接受 | 27 ≦ **風險值** ≦ 13 |
| 中 | 可接受 | 12 ≦ **風險值** ≦ 7 |
| 低 | 可接受 | 6 ≦ **風險值** ≦ 1 |

2. 風險分佈統計：

依 43 項資訊資產並依據資產價值及特性，用數量彙整出風險等級和資產類別的分佈

| 風險等級 | 合計 | 比率 |
|---|---|---|
| 高 | 3 | 7% |
| 中 | 18 | 42% |
| 低 | 22 | 51% |
| 總計 | 43 | 100% |

| 資產類別 | 風險等級 | | | |
|---|---|---|---|---|
| | 高 | 中 | 低 | 總計 |
| 人員 | | 3 | 2 | 5 |
| 服務 | 1 | 3 | 2 | 6 |
| 資訊紀錄 | 2 | 3 | 12 | 17 |
| 電腦系統 | | 4 | 2 | 6 |
| 實體設備 | | 5 | 4 | 9 |
| 總計 | 3 | 18 | 22 | 43 |

3. 風險值統計：

風險值計算方式為：資訊及資通系統資產價值 x 威脅等級 x 脆弱等級

| 風險等級 | 風險值 |
|---|---|
| 高 | 18 |
| 中 | 10 |
| 低 | 4 |

| 資產類別 | 風險值 | 風險等級 |
|---|---|---|
| 人員 | 8 | 中 |
| 服務 | 10 | 中 |
| 資訊紀錄 | 6 | 低 |
| 電腦系統 | 8 | 中 |
| 實體設備 | 6 | 低 |

IV. 業務衝擊分析

針對業務衝擊分析檢視各系統服務，依業務特性分析出各系統服務中斷對公司業務的影響程度，對不同影響程度採取適當的相應對策，並針對提供之系統服務，就其業務流程之重要性，依衝擊程度來訂定最大可容許中斷時間(MTPD)、系統回復時間目標(RTO)與資料回復目標點(RPO)，進行分析給予高、中、低之分級，分級為高之業務流程及即為關鍵業務流程。

| 業務流程 | 最大可容許中斷時間(MTPD) | 系統回復時間目標（RTO） | 資料回復目標點（RPO） | 重要等級 | 備註 |
|---|---|---|---|---|---|
| 網路服務 | 8HR | 4HR | NA | 中 | |
| Mail 服務 | 2日 | 8HR | 1日 | 高 | |
| ERP 系統 | 2日 | 8HR | 1日 | 高 | |
| 客訴系統 | 2日 | 12HR | 1日 | 中 | |
| 物性系統 | 2日 | 12HR | 1日 | 中 | |
| 檔案系統 | 1日 | 4HR | 1日 | 中 | |
| 考勤系統 | 2日 | 1日 | 1HR | 低 | |

衝擊等級說明：

| 分數 | 等級 | 定義 |
|---|---|---|
| 3 | 高 | 重度傷害<br>中斷公司之核心業務營運 5 個工作日以上或須投入大量的經費進行系統復原 |
| 2 | 中 | 中度傷害<br>中斷公司之核心業務營運 3 個工作日或須投入大量的人力復原 |
| 1 | 低 | 輕微傷害<br>可於 1 日內迅速修復 |

V. 風險策略

風險之應對策略分為下列四種方式：

1. Avoid.規避：迴避風險發生的可能性，以完全消除威脅。
2. Transfer.轉移：將風險由原資產轉嫁由第三方負責承擔，部分的風險仍需由己方承擔。
3. Mitigate.減輕：在執行前或執行中降低威脅發生的機率或影響，預防損失發生及降低損失的嚴重性。
4. Accept.接受：必須使用資產或無其他適合策略時，承擔不願或無法轉移的風險。

依據上述評估方法，針對資產類別進行分類，評估結果彙整如下表：

| 資產類別 | 資產價值 | 風險值 | 風險等級 | 回應策略 |
|---|---|---|---|---|
| 人員 | 2 | 8 | 中 | 轉移 |
| 服務 | 2 | 10 | 中 | 轉移+減輕 |
| 資訊紀錄 | 2 | 6 | 低 | 規避 |
| 電腦系統 | 3 | 8 | 中 | 規避 |
| 實體設備 | 2 | 6 | 低 | 規避+轉移+減輕 |

VI. 結論

從已採取的各項資安防護措施之 2022 年風險評估得知，外在的惡意連線透過防護措施均能發揮其功效，阻擋各種不當的網路連線，再加上內部控制上的各類管控，使整體風險控制在穩定的狀態；基於上述評估結果，認為本公司於 2022 年度在資訊安全維護效果、防禦措施之可靠性、資訊內部控制作業程序和方法之設計及執行係屬有效，其能確保資訊安全政策之落實。

對於未來的資通安全風險，雖評估後整體資安處在低風險的位階，但針對員工社交工程需再加強宣導及演練，但對未來更多複雜的資安威脅，本公司將秉持著高度的防禦心態積極做好防範措施。

六、附錄

6-1. 防駭守門員統計表

6-2. 入侵防護偵測統計表

6-3. 資訊資產清單

6-4. 資訊風險值評估表

核准：

審核：

製表：陳盈君

2023/12/14