1.資通安全風險管理架構

(1)本公司資訊安全之權責單位為資訊中心，負責規劃、執行及推動資訊安全事項。

(2)本公司稽核單位，負責資訊安全查核工作，若查核發現缺失，則要求受查單位提出相關改善計畫並呈報董事會，且定期追蹤改善成效，以降低資安風險。

組織運作模式採 PDCA（Plan-Do-Check-Act）循環式管理，確保目標之達成及持續改善。

2.資通安全政策

本公司於資通安全管制程序規範資通安全政策，包含網路資源、硬體資源、軟體版權及資料安全，主要目的為

(1)維持資訊相關系統持續運作

(2)防止內部人為非法使用軟體及資訊

(3)防止外部駭客，病毒入侵損壞設備，竊取資料造成營運中斷

(4)保護敏感機密資料，防止資料外洩

3.具體管理方案

(1)網路資源安全管理

帳號/密碼管理：

帳號管理：當有帳號需求或異動，應填寫申請單申請。

密碼管理：密碼設定需依照資訊單位公告密碼最小長度及複雜度規則進行設定並於每季強制變更密碼。

帳號清查：資訊單位每年第一季執行超過一年未登入之閒置帳號清查作業，並記錄帳號清查結果。

Internet 及電子郵件使用守則：

訂定規範使用守則，如違反使用守則，資訊人員對使用者開立單據，由該單位提出改善措施。

防毒系統安全管理：

為有效防止病毒入侵，強化資訊安全，並監控公司全區個人電腦狀況，由資訊單位依防毒系統規劃標準建制本公司之防毒系統，設定防毒自動防護機制，由病毒監控中心統一更新病毒碼並設定排程掃描全機。

網路流量監控管理：

為掌握公司網路使用狀況，資訊單位依網路流量統計系統進行日常監控。

個人電腦使用權限：

A.考量資訊安全，一般單機電腦於購入後，資訊單位即會將使用者網域及使用權限設定為公司網域及一般使用者權限。

B.公司給予個人使用之電腦，除公事外禁止其他用途之使用。

防火牆管理:

A.為阻隔來自網際網路未知入侵及攻擊，確保公司內部資料安全及完整性，資訊單位依公司資安政策建置防火牆控管網際網路連線。

B.資訊單位每半年進行規則清查作業，如有作業異常，則確認該規則之適用性後進行改善，經確認改善完成後，記錄結果。

(2)硬體資源安全管理

本公司之硬體資源購入後，由需求單位管理，若購置之硬體資源為主要設備時，則由資訊單位進行管理及登錄。

主要設備需安裝於 UPS(不斷電)電力系統裝置上，安裝時須注意電源負載及平衡。

(3)版權軟體資源安全控制

版權軟體請購與管理：

A.基本配置軟體：由資訊單位於每年評估需求提出建議並編列預算，購入後進行保管及登錄。

B.非基本配置軟體：由需求單位依需求進行請購，購入後進行保管及登錄。

C.軟體應置於適當的儲存地點，並由專人妥善保管。

軟體安裝管理：

A.基本配置軟體，於新機購入時由資訊單位依單機整體效能考量，選定適當的版權軟體版本後安裝。

B.非基本配置軟體之安裝新增或異動，應填寫申請單，由資訊單位安裝。

C.資訊單位應隨時稽核軟體的安裝與使用情形，如有異常，則通知責任單位進行改善。

(4)資訊安全教育訓練

資訊單位於新進人員教育訓練時，說明資訊資源之適當使用方式，並讓使用者明瞭資訊安全的威脅與顧慮。

除新進人員教育訓練外，資訊單位應將資訊安全相關資料置放於企業入口網站，讓使用者可隨時取得。

(5)資料安全控制

電子檔案資料存放

A.公司使用之相關文件，統一規定放置於檔案伺服器中存取。各單位如須建立伺服器資料夾權限時，應提出申請，由資訊單位進行設定。

B.資訊單位每月稽核伺服器資料夾權限管理情形，記錄清查結果。

伺服器資料備份

A.公司儲存之系統及檔案資料需進行備份，並留存每日之異動紀錄，需要時可進行調閱某時間點歷史資料。

B.備份之媒體及主機應有密碼保護。

C.備份資料應置於適當的儲存地點，並由專人妥善保管。非經同意，不得借出備份資料。

D.備份資料應有原地備份及異地備份二種以上之備份保存方式。

E.備份資料的保存期限最少一年。

可攜式儲存裝置之控管

考量資訊安全，依單位屬性應停用外接儲存裝置之功能。

(6)委外資訊安全

資訊單位於委外合約中，應明訂該供應商需對資料處理及過程保密，嚴禁外洩，並於合約中擬定相關條款或罰責。

供應商於作業進行前需經資訊單位同意，或由資訊單位人員陪同進行。

(7)機房安全管制

機房應設置門禁，監視，消防，溫溼度管理等相關配置。

機房門禁由資訊單位負責管制，人員進出須經資訊單位同意後始得進出機房作業，並登錄記錄。

維護廠商進出機房作業須由權責單位陪同，並限制於該次作業範圍內行動且不得操作無關之設備。

機房內除軟硬體設備及相關文件資料外，非作業所需物品禁止攜入機房。

資訊單位應不定期巡視機房，對於易燃物之存放及未經核准之電器擺設、飲食或吸菸行為加以制止。

(8)資安事件通報與復原

通報：

資安事件發生後，資訊單位應判斷災害種類後，立即通報資訊單位最高主管。若無法即時修復，資訊單位主管應立即呈報總經理及執行長，並通告同仁影響範圍及可能修復的時間。

緊急應變：

A.就資通安全危害事件之徵兆，查明事件原因、判定可能影響範圍、評估可能損失、判斷是否需要支援申請等作業進行處置；並保留被入侵或破壞等證據。

B.透過系統弱點資料庫、上網、技術支援單位等方式，獲得解決方案。

復原：

A.檢測硬體設備是否可正常運作，如果硬體設備毀損不堪使用，可暫以備援之設備替代並聯繫廠商進行維修。

B.檢測資安風險是否影響正常運作，待排除資安風險後執行系統修復或環境重建等作業。

C.運作正常後，即進行資料回復、資料重置。

檢討/演練：

A.當災害解除恢復後，資訊單位應將事件發生原因、災害應變、復原過

程及檢討改善方案記錄。

B.資訊單位需針對主要設備依災害復原程序進行實機演練。資安事件演練每年實施一次，以確認此系統之有效性，演練過程需留存演練紀錄。

4.投入資通安全管理之資源

本公司持續投入資源於資通安全管理，投入事項包含完善治理面及技術面之安全基礎架構、強化資安防禦設備、與教育訓練等。資訊系統定時執行安全性更新、加強員工資安觀念，利用會議、企業內部網站向同仁宣導提高資安意識，如有可疑之資料及電子郵件勿開啟，避免遭到駭客攻擊，適時更新資安防護設備，使防護效果最佳化。

2024 年度資訊安全執行實績

資訊安全教育訓練 655 人次

資安演練*2 次

弱點掃描*1 次

安訊安全評估*3 場

於第九屆第二十一次(民國 113 年 11 月 13 日)董事會進行資通安全風險管理報告