資通訊安全管理

（一）敘明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等。

1.資訊安全目的：

面對商業競爭與全球化的挑戰，資訊安全與營運資料保護已是企業永續發展與維持核心競爭力的重要基石；為確保資訊系統之穩定性、安全性及可用性，公司致力於強化資訊安全管理機制與防禦能力，建立安全及可信賴之電腦化作業環境，確保系統、資料、設備及網路安全，以保護公司重要資訊資產及資訊系統作業正常運作。

為落實永續發展，保障公司機密資料，本公司成立「資訊安全管理小組」，執行資安政策佈達與建立溝通機制，有效防止資訊遭竊取、竄改、滅失或遺漏，除了保障資訊的機密性(Confidentiality)、完整性(Integrity)及可用性(Availability)之外，更要求能符合相關資訊安全標準或法規。

2.資訊安全適用範圍與對象：

適用於公司及其他具有實質控制能力之集團關係企業，範圍包含各營運據點同仁及接觸集團內部資訊之委外廠商。

3.資訊安全風險架構：

(1)公司成立跨部門之「資訊安全管理小組」，建立與實施資訊安全管理制度，每年固定召開會議，負責審議資訊安全規劃與執行之有效性及資訊安全重大決議事項，並協調分配資訊安全所需資源。

(2)資訊安全管理小組主要負責資訊系統之資訊安全管理制度規劃、建立、實施、維護、審查與持續改善，並將資訊安全相關議題於資訊安全管理委員會提報。

(3)資訊安全管理小組定期召開會議檢討執行情形，並每年定期向董事會報告執行情形與檢討(於 114 年 11 月 13 日向董事會作報告)。

(4)本公司依上市上櫃資通安全指引於 112 年 3 月 20 日決議並公告設立資安專責單位，資安專責單位包含一位資安專責主管及一位資安專責成員，主要負責公司企業整體資安架構設計、資安維運與監控、內外部資安事件回應與調查，並定期向「資訊安全管理小組」匯報工作進度，並每年定期於董事會呈報年度資安辦理情形。

4.資訊安全目標和政策與相關方案：

(1)資訊安全目標：

①維持公司企業營運業務的穩定性和持續性，避免系統中斷或其他資安事件造成營運損失。

②對公司企業之營業秘密等機敏資料採取適當保護措施，以降低發生毀損、竊取、洩漏、竄改、濫用以及侵權等資安事件之衝擊與風險。

③持續提升公司企業各資訊資產之機密性、完整性與可用性。

(2)資訊安全政策：

①確保公司資訊的機密性(Confidentiality)、完整性(Integrity)及可用性(Availability)，管理制度與流程的合規性(Regulation Compliance)。

②從組織、人員、流程、技術四大面向強化縱深防護能力，強固核心資通系統之韌性，確保持續營運。

③定期因應內外在資通安全情勢變化，檢討風險管理措施及資安事件應變處理作業程序之有效性。

④落實機敏資料保護及資料備份/還原作業，避免因人為疏失、或蓄意作為、或自然災害，資訊資產遭致不當使用、竄改、毀損等，影響業務運作，造成公司權益及競爭力之損害。

⑤辦理教育訓練，同仁應確實參與訓練，以提高同仁之資訊安全意識及個人資安防護能力。

(3)資訊安全之範圍：

①人員管理及資訊安全教育訓練。

②電腦系統安全管理。

③網路安全管理。

④系統存取管制。

⑤系統發展及維護安全管理。

⑥資訊資產安全管理。

⑦實體及環境安全管理。

⑧資訊系統永續運作計畫管理。

⑨資訊安全稽核。

(4)資訊安全的原則及標準：

①定期辦理資訊安全教育訓練及宣導，包括資訊安全政策、資訊安全法令規定、 資訊安全作業程序、以及如何正確使用資訊科技設施等，促使員工瞭解資訊安全的重要性，各種可能的安全風險，以提高員工資訊安全意識，並遵守資訊安全規定。

②為預防資訊系統及檔案受電腦病毒感染，對於電腦病毒應採取偵測及

防範措施， 對入侵及惡意攻擊應建立主動式入侵偵測系統，以確保電腦資料安全之要求。

③為預防本公司遭遇天災或人為之重大事件，將造成重要資訊資產及關鍵性業務或通訊系統等中斷，應建立資訊系統永續運作規劃之政策。

(5)員工應遵守之相關規定：

①資訊單位接收帳號申請單後，建立「使用者帳號」。

②電腦資料及設備，不得任意破壞、攜出、外借、不正當修改，以維護資料完整性。

③禁止使用無版權軟體。

④進入主機後，若作業結束或長時間不使用機器時，應退出機器，以免資料機密外洩，為別人所破壞或造成當機之困擾。

⑤離職或新舊職務交接時，由資訊單位衡量資料相關性作適當處置。

⑥電腦設備無法正常作業時，使用者應立即通知資訊單位，以便檢查或維修。

5.資訊安全控制措施：

(1)主機系統安全：

①為確保主機作業平台及資料庫之安全，使操作程序標準化，應不定期檢查主機狀況及委外定期保養，且重要主機需有備援或備份機制。

②時常檢查電腦是否有不明程式啟動執行，不要開啟無法確定及不必要的服務，如.zip，.exe，.scr，.vbs...等，避免遭受植入木馬程式。

③定期檢視更新系統安全修補、防毒軟體及防毒碼，保持更新至最新狀態，勿自行關閉系統自動更新程式，以維持系統正常運作。

④個人電腦不使用時，需採用密碼保護、鎖定或登出離線等安全措施。

⑤禁止使用點對點互連(P2P)、tunnel 相關工具或任何有危害單位網路、設備及造成網路壅塞佔用頻寬等軟體及架站軟體(FTP)作私人用途。

(2)網路安全與電腦病毒防範：

①為確保網路服務及使用之安全，對新進人員進行教育訓練且不定期發佈相關網路安全宣導。

②所有電腦皆需安裝公司所購買正式版權的防毒軟體，進行電腦的防制及定期偵測，防止電腦病毒等惡意軟體的侵入。

(3)日常作業之安全管理：

①資料備份：

A.定期對重要資料進行備份作業，以防發生意外或儲存媒體失效。

B.備份資料除存放在主作業區之外亦需有異地的備援機制存在，以防

主要作業場所發生意外。

C.每年進行備份資料的還原回復作業，以確保備份資料的可用性。

②密碼設定原則：

A.電腦設備應設定帳號密碼並定期檢查，密碼建議每3個月更新一次。

B.核心系統設定原則密碼建議長度至少8個字元，且包含文數字特殊符號等。

③環境安全管理控管：

為確保相關設施之安全，非單位指定之人員不得擅自進入機房或使用相關資訊設備。

(4)網路安全規劃與管理：

①網路安全規劃：

A.應建立電腦網路系統的安全控管機制，以確保網路傳輸資料的安全，保護網路連線作業，且防止未經授權的系統存取。

B.對於跨組織、地區之電腦網路系統，應特別加強網路安全管理。

②防火牆安全管理：

A.與外界網路連結的接口應加裝防火牆，以控管資料傳輸與資源存取。

B.防火牆應由網路管理員管理且禁止由遠端登入，以避免登入時資料遭竊取。

③伺服器資訊安全管理：

A.設定防火牆以控管外界與單位內網路間之資料傳輸與資源存取，並關閉不使用的通訊埠，以避免病毒感染及駭客攻擊。

B.開放外界連線作業之伺服器主機，應避免外界直接進入資訊系統或資料庫存取資料。

C.伺服器主機管理之安全性，應視需要之使用情況，加密通道（VPN）等各種安全控管技術。

D.各單位開發之系統及網站(含委外開發)等運作中系統及網站亦會定期進行必要的系統及網站弱點掃瞄。

E.重要系統設定檔、網頁資料、伺服器檔案、資料庫及機敏性檔案資料均應訂定備份週期，並依據週期執行系統排程或手動備份。

(5)資訊系統安全管理

①公司主機伺服器、統一安裝防毒軟體，並自動更新病毒碼，並定期檢視更新狀況。及時派送系統安全性漏洞的修補程式，確保安全性修補作業完善。

②個人電腦及筆記型電腦統一安裝防毒軟體，並自動更新病毒碼，並定期檢視更新狀況。及時派送系統安全性漏洞的修補程式，確保安全性修補作業完善。

③郵件系統建置垃圾郵件過濾功能、惡意郵件偵測功能、提升整體郵件

資訊安全。

④應用系統及資料庫，每日進行資料備份，符合 3/2/1 資料備份原則，3 份備份、2 種媒體儲存、1 份異地存放，每年定期實施系統資料還原演練作業，並監控每日備份結果，以確保資料儲存安全性。

⑤各部門移除管理者權限，使用公司授權之合法軟體，並遵守相關法令規定，非經合法授權及與業務無關之軟體，無法安裝使用，以確保公司軟體授權合規性，並降低使用非法軟體感染病毒、後門程式之風險。

⑥資訊系統業務委外時，於事前審慎評估可能潛在安全風險，並與廠商簽訂適當的資訊安全保密協議。

(6)網路安全管理

①公司對外服務應用系統以防火牆與外部網際網路隔離，並限制存取端口阻斷惡意連線，並定期檢視異常連線報告。

②公司對外網路佈署七層式防火牆，過濾所有進出封包流量，針對違反網路安全之流量進行阻絕，並定期檢視異常報告進行分析處理。

③管控員工私人電腦設備，針對非公司合法電腦裝置進行偵測及阻絕，以避免私人設備接入公司網路竊取公司機密資料。

④建置內部防火牆，達成防禦縱深目標，保護公司各部門重要資訊，避免遭受外部駭客惡意攻擊，並進行應用程式存取控管。

⑤管理公司筆記型電腦進行對外資料分享的行為，以避免員工攜出筆記型電腦，洩漏公司重要機密資訊。

(7)系統存取控制

①員工新進、調整職務及離職時，需上系統提出申請，通知資訊中心執行使用者之新增、調整或刪除其使用權限，確保系統存取安全。

②公司對外網路佈署七層式防火牆，過濾所有進出封包流量，針對違反資訊系統必需設定帳號密碼，使用者通行密碼應符合安全原則，密碼需符合長度及複雜度之原則，並要求使用者定期更改系統密碼。

③內部相關應用系統依照人員工作需求，由使用者登入系統提出資訊系統帳號申請單，再經由相關主管進行審核，最後由資訊中心進行系統權限設定。

④針對廠商系統建置及維護作業，限制其可接觸之系統權限範圍，並嚴禁核發長期性之系統帳號、密碼。基於實際作業需要核發短期或臨時性之系統帳號、密碼供廠商使用，需事先申請並於使用完畢後，立即取消其使用權限。

⑤在公司外部欲存取公司內部資料時，導入雙因子認證機制，確保連線的安全性。

(8)人員使用安全教育與訓練：

①針對新進員工需進行資訊安全教育訓練，使新進員工瞭解資訊安全的重要性及各種可能的安全風險，並遵守公司相關資訊安全規定。

②定期對員工進行資訊安全教育宣導及 eLearning 教學，以提高人員對資訊安全之認知的重要性，與防範各種可能會發生的資訊安全意外。

6.114 年度執行情形：

(1)於 114 年 6 月及 11 月排定兩次委外執行弱點掃描作業，針對檢測結果中的高風險項目進行改善，透過強化措施持續提升資安防護品質。

(2)在 114 年上下半年各進行一次的社交工程演練，模擬駭客的釣魚郵件，檢測員工資安風險意識，輔以資安宣導及教育訓練，來提升同仁對於資安的意識及警覺性。避免受到社交工程之危害以致資訊安全事件發生。

(3)公司員工教育訓練中加入資訊安全課程項目，且建立 e-Learning 學習課程，另不定期的資訊安全教育宣導，以加強員工資訊安全認知及尊重智慧財產權概念，保護個人及公司資訊。

(4) 114 年資安主管及資安人員皆有外派參加資訊安全教育訓練。

(5)加入資安聯盟及臺灣電腦網路危機處理暨協調中心(TWCERT/CC)，達成資安聯防作業。

(6)不定期發佈有關病毒及駭客相關郵件訊息，提升同仁對於資安的意識及警覺性。

(7)公司於 113 年導入新的備份管理系統後，依 3-2-1 備份原則，為企業進行資訊系統的全面性保護。

(8)公司已於 2024 年 6 月導入端點防護 XVR 系統，監控內網 Core Switch、DMZ Switch 的網路活動。且透過部屬 Agent、Sensor 監控內網，以了解內網的網路活動狀態，便以查找有無異常連線、惡意行為的軌跡，可讓相關人員及早檢查及發現。

(9)公司於 2025 下半年更換新的 VPN(虛擬私人網路) 雙因子認證機制，進一步提升資安的保護。

（二）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。

本公司 114 年度及截止年報刊印日止，並無遭受重大資通安全事件，且未有相關之損失及影響。