114 年資訊安全管理執行情形報告

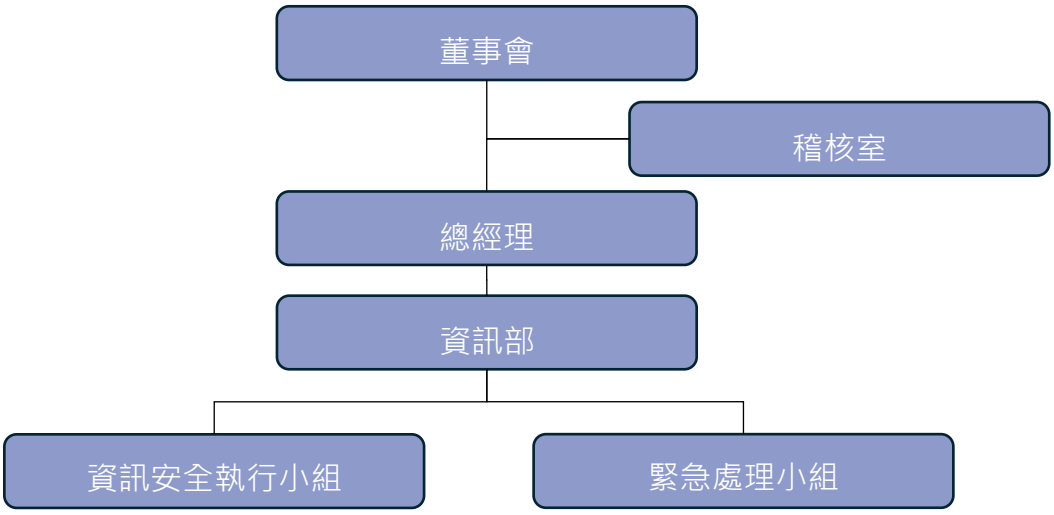
一、資訊安全管理架構

(一) 資安組織架構

本公司設置資訊安全執行小組，隸屬於資訊部，為資訊安全專責管理單位，定期每年至少一次向董事會報告資訊安全管理執行情形。

最近一次向董事會報告日期為 114 年 12 月 16 日。

本公司依規定設置一名資訊安全專責主管及一名資訊安全專責人員，其作業為統籌資訊安全及保護相關政策制定，並不定期與相關單位主管人員召開會議討論推動機制及工作重點。



(二) 資通安全管理與持續改善架構

為有效落實資安管理，以下管理為資安持續改善架構。

1. 規劃：制定資安政策及相關規範。
2. 執行：推動資安防護措施及資安教育宣導。
3. 檢查：持續監控資訊及執行資訊安全查核。
4. 改善：改善及檢討資訊安全相關問題。
5. 追蹤：追蹤資訊安全違規狀況及相關改善情形。

二、資訊安全管理架構

為強化資訊安全，確保所屬之資訊資產的機密性、完整性、可用性與個人資料之要求，以提供本公司之資訊業務持續運作之資訊環境，並符合相關法令、法規之要求，使其免於遭受內、外部蓄意或意外之威脅，本公司制定管理辦法「CX-155 資訊安全政策」、「CX-156 資訊安全管理內部控制制度」及「CX-157 資通安全事件通報與應變機制相關程序」，提供公司全體同仁共同遵循。

三、資訊安全管理方案

為增進本公司資訊安全及穩定之運作，提供可信賴之資訊服務，確保資訊系統之機密性、完整性及可用性，提升用戶端資訊意識，實行各項管理作業：

管理事項	作業說明
資訊資產之安全管理	● 資訊設備資產每年定期盤點。 ● 重要資產定期更新維護、保固作業。 ● 重要系統及資料推行本地備份、異地備份及異地備援機制。
實體及環境安全管理	● 機房資訊相關設備，應適當地進行安全保護、監控，以降低環境因素所造成的損害，例如機電設備、空調、保全、監視系統及消防設備。 ● 確保只有經過授權人員才可進入，需有門禁控制。外部人員因業務需要進入機房作業時，應由機房管理人員陪同。
電腦系統及網路安全管理	● 具備防火牆防護。 ● 具備防毒軟體防護。 ● 具備垃圾電子郵件過濾機制。 ● 外部及個人設備與網路設備未經授權不得私自連接公司網路。 ● 於公司外部需使用安全連線及多因子驗證才能存取公司內部限定之服務。 ● 重要資料採用加密並保護機制。 ● 系統每日產生的日誌應予以留存。 ● 作業系統需定期更新。 ● 定期辦理弱點掃描。
系統存取控制安全	● 每年定期進行權限檢核作業。 ● 系統權限依管理職權需求調整。 ● 停用久未使用之帳號。 ● 使用者需定期更改密碼。
資料備份機制	● 重要資訊系統皆需定期備份，並保留 14 天以上。 ● 具有異地備份功能。 ● 具有 3 份以上的備份資料組。
系統發展、開發及維護之安全管理	● 自行開發及委外之系統應納入資訊安全需求分析考量；系統之維護、更新、上線執行及故障排除應遵循相關作業程序，以確保系統之穩定性。
應變持續運作	● 每年依公司營運持續計畫進行因應演練及災難復原演練測試，並依計畫進行系統災難復原演練，確保資訊系統之可用性。 ● 定出目標回復時間(RTO)及資料回復點目標(RPO)。
人員管理及教育訓練	● 持續進行、宣導及推廣員工資訊安全認知，以提升資訊安全。

管理事項	作業說明
	● 新進同仁資訊安全宣導訓練。 ● 不定期各類資訊安全宣導。 ● 資安人員每年需接受資訊全安相關教育訓練。 ● 定期辦理電子郵件社交工程演練，並對誤開啟信件或連結之人員進行教育訓練。
資訊安全事件管理程序	● 依資安事件等級通報及應變，請參照資訊安全事件管理程序書。 ● 加入台灣 CERT/CSIRT 聯盟，掌握最新情資，實踐電腦網路安全防護與危機處理之相關作為。 ● 3 級事件以上需通報至總經理。 ● 4 級事件以上除需通報至總經理，也需通報至董事會。 ● 3,4 級事件還另需通報至國家資通安全通報應變網站。

四、投入資通安全管理資源及執行情形

為增進本公司資訊安全及穩定之運作，提供可信賴之資訊服務，確保資訊系統之機密性、完整性及可用性，提升用戶端資訊意識，實行各項管理作業：

項目	114 年執行情形	
	說明	金額
資安作業	WMS/MES 主機 Dell R760 一台 , 5 年保固	680,000
	身份認證系統一套 IDExpert , 40 使用者+MOTP 行動動態密碼系統 3 個	358,000
	垃圾郵件伺服器(Spam) , 防毒引擎模組	352,800
	電子簽核系統(BPM)維護合約 1 年	313,000
	虛擬平台(VMWare)軟體授權訂閱 3 年	1,860,000
	主機防毒軟體 , 20 套	60,900
	伺服器日誌主機(NReporter)維護合約 3 年	237,000
	備份伺服器(Veeam)維護合約 3 年	198,000
	網路備源線路昇級 , 台灣固網	10,800/月
	東莞鼎立 , 上海鼎特適 , 防火牆維護合約 1 年	31,680
	防毒軟體 Kaspersky , 230 使用者 1 年	404,800
	R740 主機 3 台, SC3020 存儲設備 1 台, 維護合約 3 年	489,600
	弱點掃描+社交工程演練	67,00
	高雄防火牆 Token 5 個授權	27,00
	SAP B1 越南維護合約 1 年 , 顧問合約半年	90,851
	TWCERT SSL 憑証 5 年	94,286

查核作業	日期	說明
	114/01/03	內部稽核
	114/01/15	資誠資訊稽核
	114/07/31	明基供應商資訊安全稽核
資安演練	日期	說明
	114/10/02	災難復原驗証
資安會議	日期	說明
	114/01/15	資產異動_主機報廢
	114/02/03	視訊會議軟體昇級
	114/02/03	資訊訊管理辦法 ， 修改討論
	114/02/03	資通安全管理年報
	114/02/20	資訊盤點, 資訊資產風險評鑑清冊
	114/03/14	SAP HANA 網路建置會議
	114/03/24	Apple 全景多因子認証導入
	114/06/11	鼎基網站建置需求
	114/08/22	虛擬主機 ESXi , vCenter 弱點修正
	114/09/19	日誌伺服器昇級
	114/09/25	備份軟體 Veeam 最佳實踐
	114/10/15	SAP HANA Client Copy
資安宣導	日期	方式/主題
	114/02/06	駭客偽冒財政部發動社交工程郵件攻擊
	114/0220	2024 年資安風險調查結果出爐
	114/07/31	中華電信已完成商業及政府機關網站憑證換發
	114/08/04	AI 相助駭客 1 小時就能突破資安防線 Chatgpt 執行長示警
	114/07/21	公務網路電話遭盜用詐騙
	114/08/06	趨勢科技證實 Apex One 重大漏洞遭攻擊利用
	114/08/11	Salesforce 相關事件最新受害品牌
	114/08/11	公開網域控制器變成 DDoS 殭屍網路
	114/08/11	WinRAR 零時差漏洞遭
	114/11/07	普發現金即將上路，財政部揭露有人架設冒牌網站企圖行騙
	114/11/21	社交攻擊教育宣導

	日期	課程名稱/證書	時數/人數
教育訓練	114/02/18	113 年上市(櫃)公司資安人員資通安全影音課程	6 小時/1 人
	114/08/06	資安宣導課程	1 小時/13 人
	114/10/27	資通系統防護基準實務課程	12 小時/1 人

五、115 年預備推動計劃

推動項目	說明
SAP R3 更新改版 評估 目前版本只支援到 2027 年。 財政部電子發票系統強迫 2025 年底前改版	導入期 12+1 個月 第 1 年顧問導入及 SAP 授權費用約 4500 萬 第 2 年後，每年 1100 萬 SAP 授權費用
導入中華電信 4G 行裝置企業內網	用於 SAP 倉庫人員行動裝置上
子公司建立 VPN(虛擬網路)	可讓子公司連線至總公司，存取總部之服務
電話交換機 AVAYA 主機評估	現有電話交換機 AVAYA，於明年保固到期，屆時會評估後續電話交換機的使用狀況
防毒軟體 Kaspersky 評估	防毒軟體 Kaspersky 已列入美國實體清單，將討論是否更換防毒軟體。
討論未來系統更新(Patch Management)如何管理	現有的系統更新機制整合在 Kaspersky，如要更換 Kaspersky 需評估未來如何系統更新
討論未來行動裝置如何管理(Mobile Device Management)	現有的行動裝置管理機制整合在 Kaspersky，如要更換 Kaspersky 需評估未來行動裝置如何管理
討論未來資訊資產如何管理(Asset Management)	現有的資訊資產管理機制整合在 Kaspersky，如要更換 Kaspersky 需評估未來資訊資產如何管理
SAP B1 落地化	SAP B1 為現有美國、越南子公司，未來將會使用 SAP HANA 系統，現有的 SAP B1 將不再使用，但需要留下來備查，將系統移回總部之機房自行維護。

六、資安事件

資安指標	資安客訴事件	外部破壞、竊取資料或病毒威脅事件	資訊系統異常或設備異常影響營運事件	其他重大事件
114 年事件統計(件) (統計期間至報告日)	0 件	0 件	0 件	0 件