

資通安全管理

(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. 資訊安全組織架構：

公司於 111 年成立「資訊安全委員會」，負責執行資訊安全管理規劃，建置與維護資訊安全管理體系，統籌資訊安全及保護相關政策制定、執行、風險管理與遵循度查核。

資訊安全委員會由執行副總為資安長，資深處長為總召集人，各事業處指派代表，每年召開至少一次資訊安全會議，討論資訊安全政策及其他資安相關重大議題，確保資通安全管理達到機密性、完整性與可用性，並每年定期向董事會報告資訊安全執行情形一次。

2. 資訊安全政策：

- 本公司重視資訊安全，致力保護客戶隱私與機密資料，確實遵守客戶合約，保護客戶隱私與機密資料。
- 確保公司重要資產之機密性、完整性及可用性，符合相關法規與規範要求。
- 本公司通過 ISO27001 認證並遵循資訊安全管理機制，採用 PDCA 方式進行矯正預防,持續強化資安管理機制。
- 強化員工資安意識與能力，辦理全體員工資訊安全課程與資訊安全宣導。定期舉辦社交工程演練，強化員工對網路釣魚郵件的辨識能力及應變能力。



具體管理方案：

管控方案	管控成果
網路安全	<ul style="list-style-type: none"> ● 次世代防火牆:具入侵偵測及防禦機制,定期檢視防火牆政策及漏洞,即時阻擋惡意流量。 ● 網路區隔:網路分段,防止電腦病毒或惡意攻擊跨廠區擴散。 ● 資通安全威脅偵測管理機制 (SOC: Security Operation Center):彙整資安訊息,即時掌握內外資安威脅及應變處理,將損害降至最低。
裝置安全	<ul style="list-style-type: none"> ● 主動式電子郵件過濾系統。 ● 主動式個人行動裝置及可攜式媒體管控使用 ● 主動式偵測非合理申請軟體安裝 ● Dr. IP:新機台網路開通前,須完成掃毒檢測,防止病毒感染及擴散風險
資料安全與保護	<ul style="list-style-type: none"> ● USB 及列印管制:資料加密,傳輸加密,存取權限管控。 ● 文件管制程序:制定機密等級及閱讀權限,重要文件都有用加密軟體保護,防止機敏資料外洩 ● 雙因子驗證(MFA):透過兩次驗證檢視使用者合法性,以杜絕未授權使用者獲取公司內部資訊
電腦安全管理	<ul style="list-style-type: none"> ● 個人帳號密碼管理:定期強制變更密碼,且符合密碼複雜度規則。 ● 防毒軟體:及時更新病毒碼,自動派送更新到使用者電腦,每週定時全機掃描。
外部威脅偵測與防護	<ul style="list-style-type: none"> ● 滲透測試和弱點掃描:定期委外第三方資安廠商進行,並加以補強與修護,以降低資安風險 ● 第三方風險評估系統:監控及分析資安風險和漏洞
供應商管理	<ul style="list-style-type: none"> ● 簽署保密合約:確保使用本公司的資訊資產,以防止遭未經授權存取,擅改、破壞。 ● 供應商教育訓練:定期舉辦供應商之資訊安全教育訓練
提升資安防禦能力	<ul style="list-style-type: none"> ● 新進員工資安教育訓練及簽署保密協議書 ● 全體員工:每年定期進行全體員工資安意識教育訓練且完訓率為 100% ● 社交工程釣魚郵件演練:每年定期執行,提升員工資安意識

	<ul style="list-style-type: none"> ● 資安意識宣導: 不定期透過電腦開機畫面及海報進行宣導
營運持續及資安事件管理	<ul style="list-style-type: none"> ● 執行災難復原演練: 每年針對重要系統執行演練 ● 建立資安事件通報及處理程序: 判定事件影響及損害評估, 內外部通報流程

4. 投入資通安全管理資源：

單位：新台幣

投入資源	2022	2023	2024
資安專案投入金額	500 萬	700 萬	1,000 萬
資安專案人力配置	資安主管：1 人 專責人員：2 人	資安長：1 人 資安主管：1 人 專責人員：2 人	資安長：1 人 資安主管：1 人 專責人員：2 人 兼職人員：2 人
訂定資通安全政策及目標	√	√	√
定期召開資安委員會	√	√	√
取得 ISO27001 認證	√	√	√
弱點掃描、滲透測試、社交工程演練	√	√	√
資安教育訓練與宣導	√	√	√
加入資安聯防	√	√	√
定期向董事會報告	X	X	√
資安事件	X	X	X

- 專責人員：設有兩位專職之資安人員和兩位非專職之資安人員，負責公司資安政策規劃與推行，資訊系統安全管理及資安技術導入，以維護及持續強化資通安全管理。
- 認證：通過 ISO27001 資訊安全驗證(目前證書之有效期為 111 年 10 月 13 日至 114 年 10 月 31 日)，相關資安稽核無重大缺失。
- 資安委員會：每年召開至少 1 次資通安全委員會檢視資安政策推動成效。
- 資安教育訓練：新進同仁皆須完成新人資安教育訓練；所有員工每年必須完成 1 次線上教育訓練並通過測驗，完訓率 100%；資訊單位每年至少 3 小時資安教育訓練；資安專責人員每年參與 40 小時以上外部研討會及專業訓練課程；每年執行 1 次社釣魚郵件測試。

- 資安宣導：每年至少 5 次不定期透過開機畫面或海報宣導資安規則和注意事項。
- 本公司已加入台灣電腦網路危機處理暨協調中心(TWCERT/CC)，台灣資安通報年會集資安情資蒐集與分析實務，CYBERSEC 台灣資安大會,定期收集外部威脅情資，並依據情資內容進行風險評估，藉由強化外部資安威脅防護。
- 資訊安全執行情形每年向董事會報告一次，最近一次報告日期為 113 年 11 月 8 日。

(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：最近年度及截至年報刊印日止，本公司並未發現任何對公司營運有重大影響的網路攻擊事件。