2024 年資通安全管理

1. 資通安全風險管理架構

本公司組織結構設有「資訊安全委員會」，經 2023 年 12 月 23 日董事會通過由資訊部門經理曹建華擔任資訊安全主管及一名資訊安全人員，負責推動、協調監督及審查資通安全管理及執行等事項。每年至少一次向董事會報告投入資通安全管理之資源及運作情形。2024 年度向董事會報告日期為 2024 年 12 月 13 日。

2. 資通安全政策：

為確保公司網路和資訊使用環境安全及穩定，本公司依主管機關發佈之「上市上櫃公司資安管控指引」經 2023 年 12 月 23 日董事會通過訂定本公司「資通安全風險管理作業程序」，並由資訊安全主管負責推行及落實本規定之資通安全作業，其內容包括核心業務及其重要性、資通系 統盤點及風險評估、資通系統發展及維護安全、資通安全防護及控制措施、資通系統或資通 服務委外辦理之管理措施、資通安全事件通報應變及情資評估因應、資通安全之持續精進及績效管理機制等。

(1) 核心業務及其重要性

權限申請表單經直屬單位主管依業務需求審查其使用權限之適當性，並由系統管理者設定程序化控制措施，以確保維持資訊安全的必要等級以符合法律、法規、契約及營運要求。加強資安宣導，督導全體同仁落實資通安全管理，持續進行適當的資通安全教育訓練，降低資通安全風險，達成資通安管理法及個人資料保護法等相關法令要求事項。資訊系統定期執行備份並估算回存所需時間，以供緊急應變計畫參考。

(2) 資通系統盤點及風險評估每年最少一次盤點資通系統，並建立核心系統資訊資產清冊，以鑑別其資訊資產價值； 每年最少一次資訊資產衝擊影響評估，藉以客觀的評估各資產的風險，了解未來可能遭 受之危害，以達先期改善之效。

(3) 資通系統發展及維護安全 應將資安要求納入資通系統開發及維護需求規格，包含機敏資料存取控制、用戶登入身 分驗證及用戶輸入輸出之檢查過濾等。另定期執行資通系統安全性要求測試，包含機敏 資料存取控制、用戶登入身分驗證及用戶輸入輸出之檢查過濾測試等妥善儲存及管理資 通系統開發及維護相關文件。

(4) 資通安全防護及控制措施 本公司應依網路服務需要區隔獨立的邏輯網域，並將開發、測試及正式作業環境區隔，且針對不同作業環境建立適當之資安防護控制措施。

(5) 資通系統或資通服務委外辦理 委外的管理需充分注意並儘量降低因委外所造成的資安問題發生的機會，資訊委外（如 電腦設備維護、系統開發等）應與委外廠商簽訂契約，並將保密條款納入其中。

(6) 資通安全事件通報應變及情資評估因應公司應確實遵循主管機關對資訊系統、資訊安全等相關法令規定，避免在資料處理上發生違法情形。各部門發生資安事件時，應第一時間通報資訊專責人員，並遵循資訊專責 人員指示之應變處置，後續由資訊部及各業務主管聯合判定事件影響及進行損害評估，內部通報由

資訊專責人員執行、外部主管機關之通報由財務部及業務部依相關業務通知 外部受影響機關。
(7) 資通安全之持續精進及績效管理機制 本公司由資訊部每年至少一次向董事會報告資通安全執行情形，確保運作之適切性及有效性。資訊專責人員不定期檢核內部及委外廠商之資安情形，並針對發現事項擬訂改善 措施，且追蹤改善情形。

3. 具體管理方案：

類別	採行措施/作法	
電腦安全及應用系統安全	電腦實體設備保護	· 本公司各應用伺服器等設備均設置於專用機房，機房之門禁須採用感應刷卡進出，且保留進出記錄存查。 · 機房內部備有獨立空調，維持電腦設備於適當的溫度環境下運轉；並放置藥劑式滅火器，可適用於一般或電器所引起的火災。 · 機房主機配置不斷電與穩壓設備，避免主機意外瞬間斷電造成系統當機，或確保臨時停電時不會中斷電腦應用系統的運作。
	防毒軟體	· 伺服器與員工終端電腦設備內均安裝有端點防護軟體，病毒特徵采自動更新方式，確保能阻擋最新型的病毒，同時可偵測、防止具有潛在威脅性的系統執行檔之安裝行為。 · 電子郵件伺服器配置有郵件防毒、與垃圾郵件過濾機制，防堵病毒或垃圾郵件進入用戶端的資訊設備。
	系統訪問控制	· 員工對各應用系統的使用，透過公司內部規定的系統許可權申請或軟體需求（許可權）申請程式，經權責主管核准後，由電腦資訊部建立系統帳號，並經各系統管理員依所申請的功能許可權做授權方得存取。 · 員工離(休)職時，工程師根據人事離職資訊進行各系統帳號的停用刪除等作業。
	系統備份	· 業務數據必須完整、真實、準確地轉儲到離線的介質或備份伺服器上，並要求集中和異地保存，依照業務數據的性能設置備份數據保留年限
	災害復原演練	· 核心系統資料庫復原時間目標（RTO）為 24 小時，資料庫資料復原時間點目標（RPO）為 8 小時，每年實施一次對關鍵數據進行災難恢復演習，確保數據可以在規定時間內完整得到恢復。
人員安全	資安宣導與教育訓練	· 所有新進有帳號的員工，每季皆須完成員工資訊安全意識教育訓練課程和考核。 · 宣導妥善管理個人電腦密碼，並已在系統中設置在每個週期提前要求用戶修改密碼，以維持帳號安全。 · 定期通過電子郵件、培訓等方式對內部員工實施資訊安全相關的教育訓練宣導。
委外	委外管理	· 資訊委外時，應與委外廠商簽訂契約，並將保密條款納入其中。 · 電腦系統資訊委外業務完成後，應要求委外廠商提供詳細的系統檔及手冊。 · 委外廠商人員如有派駐公司情況，派駐的委外人員電腦系統使用 權限應予以適當控管。

(二)　投入資通安全管理之資源及運作情形：

本公司新購入電腦安裝即時防毒軟體，並啟動自動與定期更新病毒碼功能，為確保各項資訊系統能持續提供穩定的服務，定期執行弱點掃描作業，找出潛在風險，進行弱點補強作業，採用 NGFW 防火墻和上網行為管理器，針對網路異常流量、入侵攻擊、惡意連線等，建立 24 小時即時防護，定期寄送防護報表，即時掌握防護效益；集團內持續由資訊部發布資訊安全意識文章，加強員工資訊安全知識，期能持續保持無資訊安全事故發生情形。為持續保持本公司無資訊安全事故導致系統資料遺失發生情形，針對機房設置溫度控制 設備及消防設備，機房採門禁管制，限制特定人員進入，ERP 和每日備份，建置異地備援機制，備份資料保留 30 天。 本公司一向重視集團資訊安全相關作業，以維護公司資訊之機密性、完整性、可用性與適 法性為目標，並致力於避免發生人為疏失、蓄意破壞與自然災害時，遭致資訊與資產遭致 不當使用、洩漏、竄改、毀損、消失等情形；本公司資訊系統硬體基礎設施及各項防護設 施由集團專業資訊團隊統一管理，集團專業資訊團隊所設計目前尚未導入 ISO 27001 資訊管理系統，未來視整體情況評估。

資訊安全委員會每年均定期執行各項資訊安全相關之檢測及評估作業，2024 年度各項資安檢測評估作業頻率及執行結果如下

項 目	作業頻率	2024 年度作業期間	結果
ERP 系統災難復原測試	每年 2 次	2024 年 4 月、2024 年 10 月	無應列重大風險情形
電腦合法性軟體檢查	每年 1 次	2024 年 12 月	無應列重大風險情形
ERP 系統權限設定檢查	每年 1 次	2024 年 10 月	無應列重大風險情形
ERP 系統個人密碼定期通知	每 90 天 1 次	2024 年 1 月-12 月	無應列重大風險情形
資訊安全宣導	每年 3 次	2024 年 4 月、2024 年 8 月 5 日、8 月 14 日	無應列重大風險情形
機房巡檢	每个工作日	2024 年 1 月-12 月	無應列重大風險情形
資料庫備份作業	每天	2024 年 1 月-12 月	無應列重大風險情形
持續發布資訊安全意識文章	每月	2024 年 1 月-12 月	無應列重大風險情形
人員進修	每年 1 次	2024 年 12 月	無應列重大風險

			情形
持續保持無資訊安全事故發生(資訊 安全)	每个工作日	2024 年 1 月-12 月	無應列重大風險情形
持續保持無資訊安全事故導致系統資 料遺失發生	每个工作日	2024 年 1 月-12 月	無應列重大風險情形

2024 年度目標規劃	項目	控管方法及執行情形
持續保持無資訊安全事故發生(資訊 安全)	人員帳號與許可權授權管理	· 人員帳號許可權管理與審核 · 人員帳號許可權定期復核 · 人員密碼定期更換
	人員存取內/外部資源、及資料傳輸控制	· 內/外部網路連線與存取管控機制 · 電腦軟體安裝和文件存儲修改許可權管制
	病毒入侵防護	· 定期掃描/病毒庫及時更新 · 防火牆入侵偵測/病毒/惡意程式防護
	郵件防護	· 郵件帳號和容量管控 · 郵件病毒防護及惡意程式偵測 · 郵件惡意連結保護，避免網路釣魚防垃圾郵件過濾
持續保持無資訊安全事故導致系統資料遺失發生	系統可用狀態與服務中斷預防	· 系統/網路可用狀態監控及通報機制 · 服務中斷之應變措施 · 本地/異地資料備份措施和機房備援 · 每年定期災害復原演練

2024 年度本公司無因重大資通安全事件遭受損失或嚴重影響營運運作的情形。