第一章 總則

第一條　為強化資通安全防護與管理機制，並符合「公開發行公司建立內部控制制度處理準則」相關控制作業第九條，使用電腦化資訊系統處理者相關控制作業，及參照「上市上櫃公司資通安全管控指引」，特訂定本管理辦法。

第二條　名詞定義:

一、 資通系統：指用以蒐集、控制、傳輸、儲存、流通、刪除資訊或對資訊為其他處理、使用或分享之系統。

二、 資通服務：指與資訊之蒐集、控制、傳輸、儲存、流通、刪除、其他處理、使用或分享相關之服務。

三、 核心業務：公司維持營運與發展必要之業務。

四、 核心資通系統：支持核心業務持續運作必要之資通系統。

五、 機密性資料：依公司業務考量，評估需保密或具敏感性之重要資料，如涉及營業秘密資料或個人資料等。

第二章 資通安全政策推動組織

第三條　公司在MIS資訊部門外另成立資訊安全室（以下稱資安室），隸屬行政處暨財務總處，配置資安主管1名及資安人員1名，以負責推動、協調監督及審查資通安全管理事項。資通系統經資安室審查後發現之弱點由MIS資訊部門進行強化改善。

第四條　資通安全政策及目標由總經理核定，並定期檢視政策及目標且有效傳達員工其重要性。

第五條　訂定資通安全作業程序，包含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。

第六條　公司員工每年至少接受1次資安教育課程，全體員工參加，由資安室主辦。另負責資訊安全之主管及人員，每年至少安排1次資訊安全專業認證訓練課程。

第三章 核心業務及其重要性

第七條　各部門主管應鑑別所承辦業務是否符合機密性質，如部門主管無法鑑別應由資安主管鑑定之。資安主管應每年一次檢視公司之核心業務及應受保護之機密性資料。

第八條　員工應遵守部門作業程序之規範、資通安全宣導之要求。公司與同仁均應遵循個人資料保護法之規範。

第九條　年度結束後於次年1月3日之前，資安主管應鑑別可能造成營運中斷事件之發生機率及影響程度，並訂定預期性改善計畫並出具報告。另為有效控制資訊業務在中斷後能盡速回復，制定「復原時間目標（RTO）」為**4**小時、「資料復原時間點目標（RPO）」為**24**小時。備份機制上，公司ERP系統資料庫每日備份一次、檔案伺服器（NAS）資料每日備份一次。上述資料備份後採異地保存，另地存放。備援機制上，為避免NAS硬碟損毀而無法復原，公司常備備援硬碟**2**顆以利損毀時替換。

第十條　為確保業務持續運作，每年檢視備援設備妥善狀態，並進行備分還原演練，檢視與演練結果應作成報告以利精進改善。

第四章 資通系統盤點及風險評估

第十一條　每年定期盤點資通系統，並建立核心系統資訊資產清冊，以鑑別其資訊資產價值。

第十二條　每年進行機櫃及伺服器檢查性安全，評估並有無外力侵入或破壞之可能性。

第五章 資通系統發展及維護安全

第十三條　資通軟硬體設備採購依公司採購辦法辦理，程序為:需求簽核，經核決權人核准之後招商、估價及報價。資通系統開發及維護之需求規格需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。

第十四條　每年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。

第十五條　妥善儲存管理資通系統開發商及維護合約相關文件，包含規格書、

開發供應商之保密承諾、程式專利權歸屬等。

第十六條　對核心資通系統辦理下列資安檢測作業，並完成系統弱點修補。

一、 定期辦理弱點掃描。

二、 定期辦理滲透測試。

三、 系統上線前執行源碼掃描安全檢測。

第六章 資通安全防護及控制措施

第十七條　依網路服務需要區隔獨立的邏輯網域（如：DMZ、內部或外部網路等），並將伺服器與作業區域之網段予以區隔。

第十八條　具備下列資安防護控制措施：

一、 防毒軟體。

二、 網路防火牆。

三、 如有郵件伺服器者，具備電子郵件過濾機制。

四、 入侵偵測及防禦機制。

五、 如有對外服務之核心資通系統者，具備應用程式防火牆。六、進階持續性威脅攻擊防禦措施。

七、 資通安全威脅偵測管理機制（SOC）。

第十九條　針對機敏性資料之處理及儲存建立適當之防護措施，如：實體隔 離、專用電腦作業環境、存取權限、資料加密、傳輸加密、資料遮蔽、人員管理及處理規範等。

第二十條　員工到職、在職及離職管理程序依據公司人事規章辦理，全體員工應簽署保密協議。

第二十一條　建立使用者通行碼管理之作業規定，如：預設密碼、密碼長度、密碼複雜度、密碼歷程記錄、密碼最短及最長之效期限制、登入失敗鎖定機制。

第二十二條　每年審查特權帳號、使用者帳號及權限；停用1年未使用之帳號予以刪除。

第二十三條　檔案伺服器中對於身分驗證失敗、存取資源失敗等行為自動建立日誌以利追蹤查閱。

第二十四條　電腦機櫃周邊配置空調或除濕設備、滅火器，並安裝攝影機以監控機櫃之安全性。提供機櫃開啟登記簿供開啟機櫃之人員

（含外包廠商）登記。機櫃平日應上鎖，鑰匙由管理員及資訊部門主管各持1把。

第二十五條　留意臺灣電腦網路危機處理暨協調中心的安全漏洞通告，即時修補高風險漏洞。定期評估設備、系統元件、資料庫系統及軟體之安全性漏洞修補狀況。

第二十六條　資通設備汰除程序上由資訊部門以破壞性之方式銷毀，並會同資安室確定機密性資料已刪除後方可進行後續報廢流程。

第二十七條　電腦裝置使用管理規範；不得安裝無版權、盜版或未經許可之軟體。電子信箱僅供收發與業務有關郵件、個人可攜式媒體不得連接至公司電腦設備。

第二十八條　每年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，並留存相關紀錄。

第七章 資通系統或資通服務委外辦理之管理措施

第二十九條　於資訊軟體作業委外安全管理上，公司在選商時需確認廠商具有ISO 27001認證、或是能提供原始碼掃描報告以證明其具備較佳之資安管理資格。

第三十條　對委外廠商之資通安全責任及保密規定作為上，須於採購文件或合約中載明服務協議、資安要求及對委外廠商資安稽核權。

第三十一條　合約應訂明委外關係終止或解除時，廠商應返還、移交、刪除或銷毀履行契約持有之資料。

第八章 資通安全事件通報應變及情資評估因應

第三十二條　資安事件發生應立即依據「（ 附圖 ）資安事件應變及通報作業流程圖」通報並辦理。

第三十三條　本公司已加入臺灣電腦網路危機處理暨協調中心(TWCERT/CC)資安情資分享組織。資安室須每日至該組織網站取得即時資安預警情資與威脅資訊，如有影響公司資安者須立即告知資訊部門強化或修正。另如發現任何資安疑慮應立即回報至該組織。

第三十四條　發生符合「臺灣證券交易所股份有限公司對有價證券上市公司重大訊息之查證暨公開處理程序」規範之重大資安事件，應依規定申報及公告。

第九章 資通安全之持續精進及績效管理機制

第三十五條　資通安全推行於年度結束次年1月底，向管理階層報告資通安全執行情形，確保運作適切性及有效性。

第三十六條　定期辦理內部及委外廠商之資安稽核，並就發現事項擬訂改善措施，且定期追蹤改善情形。

第十章 附則

第三十七條　本辦法經董事會通過後實施，修訂時亦同。

本辦法制訂於民國113年6月20日。

(附圖)資安事件應變及通報作業流程圖