資通安全風險管理

1.資通安全風險管理架構：

本公司組織結構設有資訊部，經 112 年 11 月 09 日董事會通過由財務長兼任資安長，另配置資訊專責人員一人，負責公司電腦網路及應用系統開發與維護，電腦硬體、周邊設備及資訊檔案維護與管理，以及資訊系統安全之規劃與執行。

本公司稽核室為資訊安全監理之查核單位，若查核發現缺失，旋即要求受查單位提出相關改善計畫並呈報董事會，且定期追蹤改善成效，以降低內部資安風險。

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」，由資訊部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。

簡述如下:

(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。定期進行電子郵件社交工程演練測試及以電子郵件公告的方式，提高全體員工之資訊安全意識，以防止個資外洩發生。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，達成資通安全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。

(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。

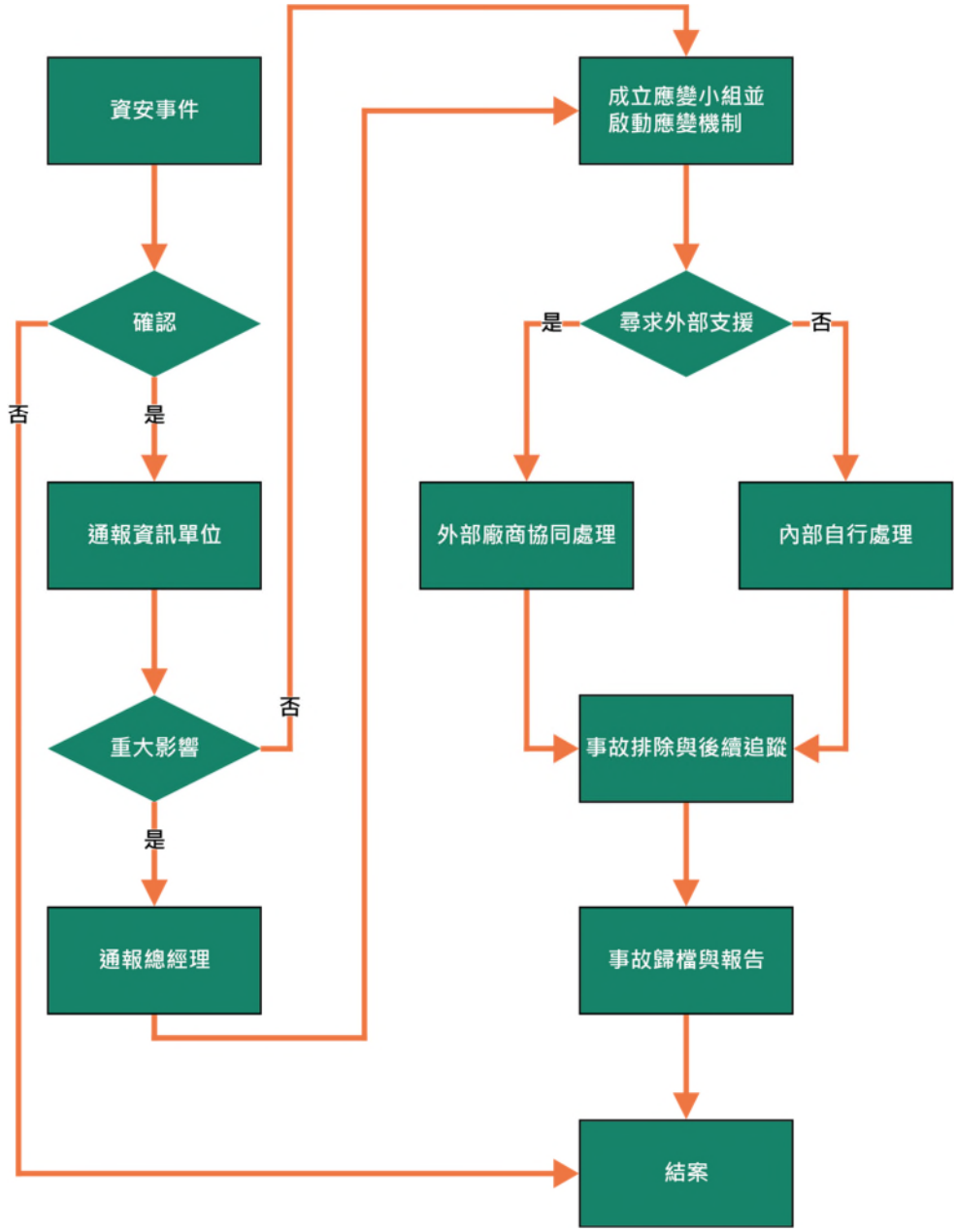
(5) 資通系統或資通服務委外辦理

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依內部重大資訊處理作業程序辦理。

以下為通報流程圖：



3.具體管理方案：

本公司具體管理方案如下：

類別	採行措施/作法	
網路安全	網路資源管理	✓關閉網路設備不使用的服務與功能，以降低風險。 ✓建立網路監控系統，及時瞭解網路運作情況，及早發現網路失效的情形或潛在風險。
	網路安全管理	✓設置防火牆(Firewall)於公司的內部網路與外部網路接界處，防止外部未經授權進入公司內部網路，並且定期檢視防火牆規則，以確認防火牆規則已適當設定。 ✓不定期委由外界專家或自行評估網路系統安全並進行安全修補，提高安全防禦能力。 ✓針對開發外界連線資訊系統，依照資料及系統的重要性，採取資訊加密、身分辨別、電子簽章等不同安全等級的技術或措施，降低資訊及系統受到入侵、破壞、篡改、刪除及未經授權存取的安全風險。 ✓自動過濾使用者上網可能連結到有木馬病毒、勒索病毒或惡意程式的網站。 ✓如有特殊連線需求需額外申請開放。
	無線網路安全	✓無線網路架設與使用須經過審慎的安全評估。 ✓無線網路卡與無線基地台間使用加密通訊協定。
電腦安全	電腦系統與實體設備保護	✓各式電腦的系統應及時進行安全修補。 ✓各式電腦軟體及版權，集中由資訊單位管理。 ✓任何電腦均應設定螢幕保護裝置程式並設定密碼保護，防止他人未經授權使用電腦。 ✓注意使用任何電腦設備時，其電源使用不可超過電源負載量。 ✓廠商維護電腦主機設備時應有公司資訊單位人員陪同。
	防毒軟體	✓公司所有電腦系統均安裝防毒軟體，實施並自動更新病毒庫，並定期執行病毒掃描。
	存取安全	✓每位電腦系統使用者，應賦予獨立的通行帳號，且帳號應依業務需求賦予最低能滿足作業的許可權。 ✓職員離職或職位調動時，需立即取消或調整其帳號許可權。 ✓定期審查帳號及使用權限情況，確保符合現狀。
	密碼安全管理	✓所有通行帳號的登錄應設立獨立密碼，密碼設定需達一定強度設定原則。 ✓輸入密碼時，電腦螢幕不得明白顯示所輸入之密碼。 ✓保存密碼的檔案應予以加密。

應用系統管理	電子郵件使用安全	✓明確規定員工禁止利用公司電子郵件從事工作業務以外的活動，並且宣導員工不開啟來路不明的電子郵件。 ✓開啟郵件過濾及防毒機制，以過濾垃圾及可能含有病毒的郵件。 ✓個人電腦接收郵件後，防毒軟體也會掃描是否包含不安全的附件檔案。
	資料安全與備份	✓機房採門禁管制，限定僅特定人員才可進入，資料庫每日備份，並建立異地備援機制。 ✓公司內各部門重要檔案存放於伺服器，由資訊部統一備份保存。 ✓任何資料存儲媒體進行報廢時，須徹底將其內資料銷毀，直至無法解讀。 ✓實體的機密資料，如紙張檔、重要合約等，宜妥善存放與保管。
	異常事件處理常式及災害複原計劃	✓針對常見資安事件與異常情況，擬定異常事件處理常式，以增加處理時效，並降低異常事件發生的傷害。 ✓按企業持續經營的原則，評估並理清重大業務衝擊威脅事件，據以制定災害復原計劃。
人員安全	人員安全管理	✓對公司資訊單位人員的職責進行明確定義。 ✓負責資訊安全相關工作或處理機密資訊的人員，需簽署保密協定 。 ✓各種資訊安全工作各種資訊安全工作，需有 2 人(或以上)瞭解，以應付緊急情況的需要。
	安全認知訓練	✓資訊安全事件應立即公告公司員工。 ✓不定期提供員工適當的資通安全認知或教育訓練。
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。