✧ 資通安全風險管理架構

為確保資訊資產的安全性，提高資安層級以強化公司之資訊安全管理、系統及網路安全，由本部總經理室所轄之資訊室，包含資安長與資安人員各一名，負責制定及規劃公司資訊安全政策與執行辦法，藉由政策執行和法規遵循查核，持續檢討資安風險控管機制之有效性。

本公司已於114年導入 ISO 27001 資通管理系統，並定期取得 ISO27001 認證，目前證書之有效期為 114 年 1 月 12 日至 117 年 1 月 12 日。透過 ISO27001 資通安全管理系統之導入，強化資通安全事件之應變處理能力，保護公司與客戶之資產安全。

✧ 資通安全政策

為確保公司所管理資訊資產之機密性、完整性、可用性、適法性，特訂定本政策作為資訊安全管理系統之目標，以加強資安管理之運轉機制，確保本公司資訊處理之正確性，作業人員所使用之電腦軟體、硬體、周邊及網路系統之可靠性，並確保上述資源免受干擾、破壞、入侵之行為或企圖。

1. 資訊安全目標
   - 1.1 確保本公司所保管資訊資產之機密性、完整性與可用性，防止非法使用公司資料。
   - 1.2 確保本公司所提供資訊服務之完整性與可用性，提供全公司員工便利和穩定的資訊服務。
   - 1.3 確保本公司所提供軟硬體資源之可用性，合法及正確地使用。
   - 1.4 每年於「管理審查會議」中檢討本公司資訊安全目標的設定、實施及修正之方式是否合宜。

2 資訊安全責任與要求
   - 2.1 確實遵守「個人資料保護法」、「著作權法」、「電子簽章法」等資訊安全相關法令。
   - 2.2 本公司從業人員與契約委外廠商皆須依照本政策要求，以維護資訊安全，任何蓄意違反資訊安全的行為將受到相關規範或法律責任。
   - 2.3 應使用具合法版權並經公司同意使用之軟體，嚴禁下載來路不明之軟體。
   - 2.4 本公司從業人員有責任通報及處理資訊安全事件和任何已鑑別出的資訊安全弱點。
   - 2.5 進行資訊處理時，若含有個人資料，應依據「個人資料保護法」及相關規定審慎處理，不得私自蒐集或洩漏業務資訊，非公務用途嚴禁調閱使用。
   - 2.6 依角色及職能為基礎，針對不同層級人員，資訊安全教育訓練及宣導，瞭解資訊安全的重要性及各種可能的安全風險，以提高資訊安全意識

並熟悉工作中之資訊安全職責，促其遵守資訊安全規定。

2.7 對於資訊安全事件須有完整的通報及應變措施，以確保資訊系統及重要業務的持續運作。

2.8 委外廠商應遵循本政策以及相關程序之規定，不得未經授權使用或濫用本公司之各類資訊資產，如有業務需求，應簽署資訊安全保密切結書。

2.9 每年至少召開一次管理審查會議，審核資訊安全業務執行狀況、建立管理指標量測方式與評估管理指標量測結果。

2.10 應建立資訊資產風險評鑑機制，每年至少進行一次風險評鑑，並由資訊安全小組召集人決定可接受風險值。

2.11 每年應至少進行一次業務持續演練及資安事故通報程序演練。

3 資訊安全政策之審查與宣導

3.1 本政策每年應至少評估檢討一次，以反映本公司資訊安全需求、法令法規、外在網路環境變化及資訊安全技術等最新發展現況，以確保本公司營運持續及提供適當服務的能力。

3.2 本政策如遇重大改變時應立即審查，以確保其適當性與有效性。必要時應告知相關部門及委外廠商，以利共同遵守。。

3.3 資通安全政策應每年透過教育訓練、內部會議、張貼公告等方式，向本公司內從業人員及委外廠商進行宣導。

✧ 具體管理方案

項目	具體管理措施
機房環境與監控	資訊機房設置錄影監視系統，防止未經授權者進出，並設有環境控制系統，定時檢視以確保維運持續與安全
防火牆架設	架設防火牆並依網路服務需求區隔獨立網域，保護網路和系統免受外部威脅和未經授權的訪問，有效遏制非法入侵 防火牆規則每年檢視一次，是否有未經授權之異動，針對防火牆設定異動或特殊連線需求需另提出申請
防毒軟體	使用防毒軟體進行病毒碼更新與病毒掃瞄，以保護資料安全，自動過濾可能連結到有木馬病毒、勒索病毒或惡意程式的網站
入侵偵測	入侵防護系統(IPS)協助即時辨識惡意流量，並主動封鎖此類流量進入公司網路以防止潛在攻擊
電子郵件安全管控	電子郵件過濾機制執行自動掃描，防範不安全的附件檔案、釣魚郵件等，即時啟動防護，降低電子郵件夾帶惡意程式或病毒的風險
資料備份機制	重要資訊系統之資料庫設定每日備份，並留有紀錄備查 程式原始碼、執行檔與組態檔或設定檔執行備份，並做版本控

	制
業務持續運作	保護重要業務於遇到重大意外或造成資訊系統運作中止的突發狀況時，以期將傷害降低至可承受範圍，除了完善異地備援機制，每年亦定期執行業務持續運作演練，確認計畫之可用性
資安宣導及檢測	新進人員須接受資訊安全教育宣導課程 每年兩次資安教育訓練並完成相關測驗來確保教育訓練的有效性 每年不定期社交工程演練，藉此提高資通安全智能及緊急應變能力，降低資通安全風險 負責資訊安全之主管及人員，每年接受資安專業課程訓練

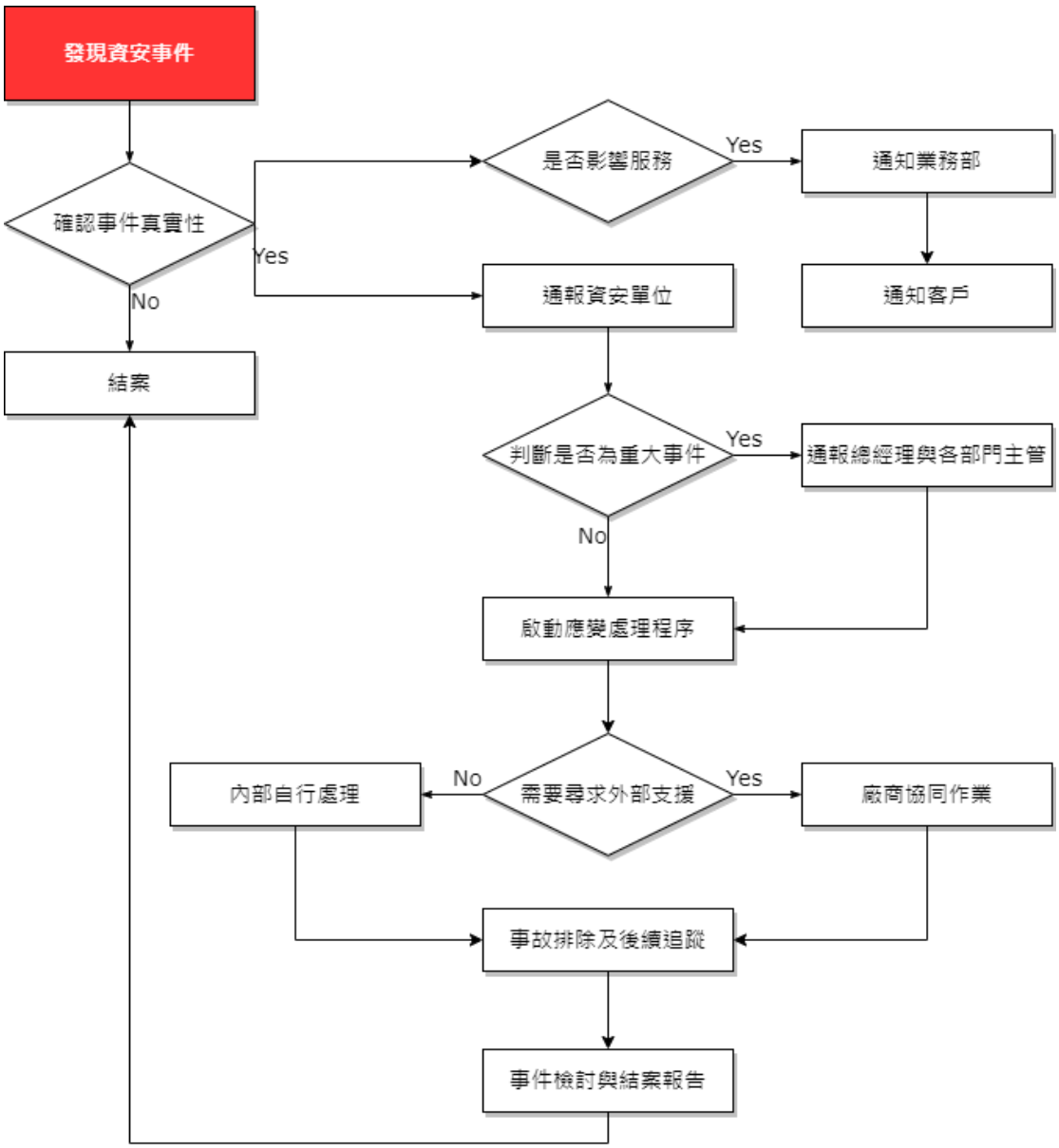
✧ 投入資通安全管理之資源

每年研議資安預算以投入資安技術設備和軟體，並定期進行資安培訓，提升員工的安全意識與應對能力。此外年度風險評鑑和內、外稽核等工作，確保資通安全管理的持續改善和有效運作。

1. 人力資源
   - 專責資安管理人數：資安長與資安人員各一名
   - 每年全體員工接受資安培訓的總時數：4 小時
2. 財務資源
   - 113 年投入資通安全的總預算金額包含新建 IDC(是方機房)、資安設備與資安維護等花費：逾 55,000,000 元
3. 技術資源
   - 資安防禦系統數量(防火牆、IPS 等)：21
   - 系統和安全軟體的升級次數與頻率：2-4 次
   - 新增是方機房，共三個 IDC 使 AA 備援機制更加完善
   - 導入 ISO/IEC 27001:2022 資訊安全管理系統
4. 時間資源
   - 每年投入年度風險評估與管審會議時間：8 小時
   - 每年業務持續運作計劃與演練時間：8 小時
5. 資安教育培訓
   - 員工參加資安培訓的比例：100%
   - 每年資安教育訓練次數：2 次，另安排新進人員資安宣導課程 1 次

✧ 緊急通報程序

（見下頁）


發現資安事件
確認事件真實性
No
結案
Yes
是否影響服務
Yes
通知業務部
通知客戶
通報資安單位
判斷是否為重大事件
Yes
通報總經理與各部門主管
No
啟動應變處理程序
需要尋求外部支援
No
內部自行處理
Yes
廠商協同作業
事故排除及後續追蹤
事件檢討與結案報告