資訊安全管理制度

資訊安全是本公司長期以來重視、關注的重要工作之一，為了確保各項資訊安全管理作業之有效落實，並及早發現不正當之行為以及安全漏洞或威脅，早期識別可幫助阻止不法行為並盡可能減少潛在的風險。

本公司為提升資訊安全管理已成立「E 化作業委員會」，定期於每季度針對資安進行宣導及資安改進措施報告，並定期對全體員工就資安議題及釣魚信件等資安案例說明，亦不定時以 email 通知全體員工有關防禦惡意郵件通知。

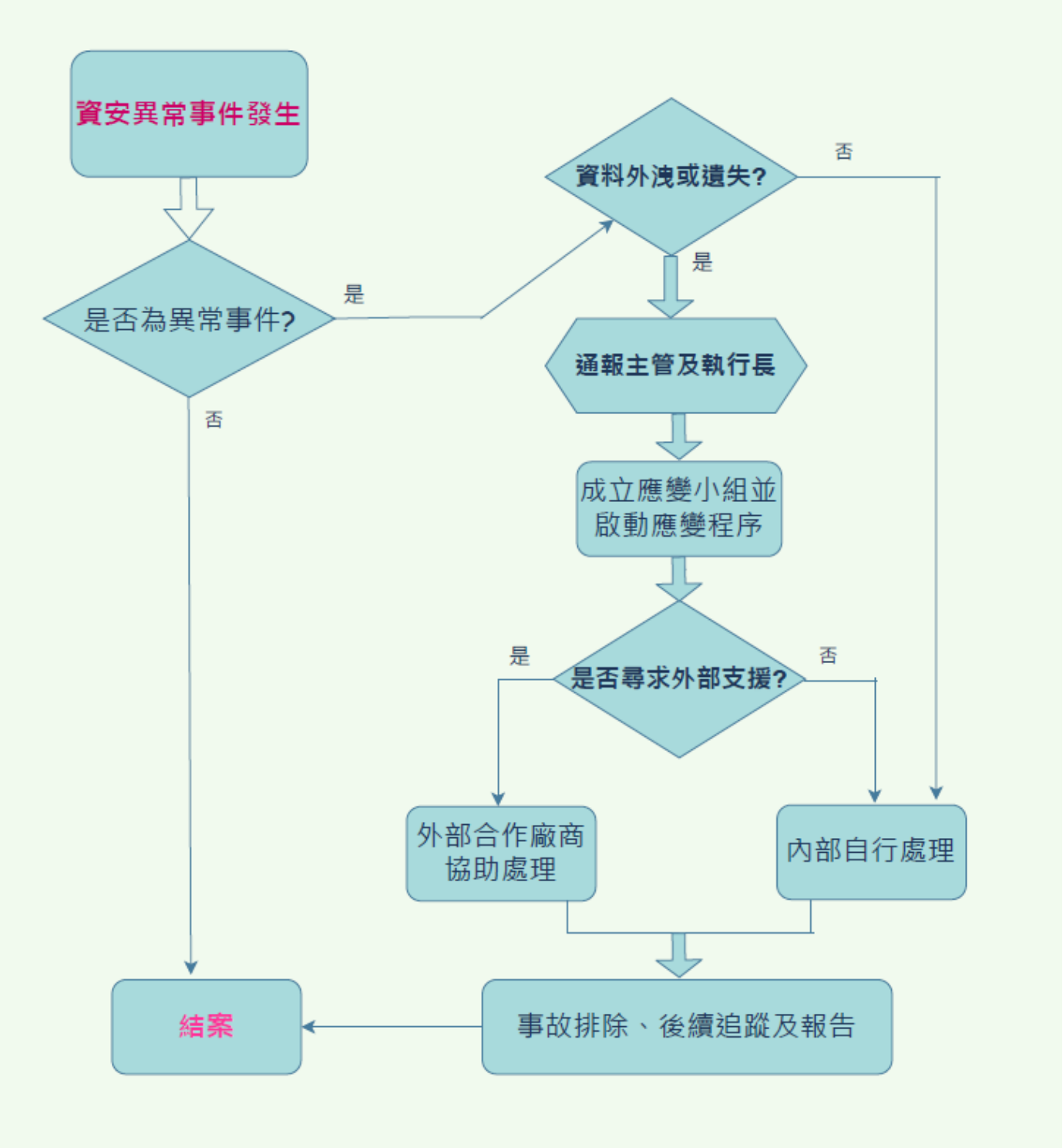
資訊安全管理措施

1. 明訂資訊安全政策：已於資訊系統管理程序中訂有資訊安全規範，明訂員工各項資訊安全的必要執行原則及措施：。

類型	項目	防範目的	相關作業說明
員工管理	•資訊安全推行及宣導	•預防降低中毒機率	隨時掌握政府及業界最新資安與預警訊息，定期對於員工進行國內外重大資安異常事件案例分享。
裝置控管	•防毒軟體 •非信任裝置阻檔	•預防中毒	•系統判定符合規範之電腦才給與網路連接權限。 •非經公司許可之電腦設備嚴禁接入公司網路，如有未經許可之設備接入系統將自動進行網路封鎖。
權限管理	•雙因素身分驗證 •專案權限控管	•避免帳號冒用	•同仁登入個人電腦需通過雙因素身分驗證，以避免帳號被竊取冒用的情況發生。 •各研發專案皆有嚴格權限控管，專案成員需提出表單申請，經主管同意後由資訊管理人員設定存取權限，並定期進行一次存取權限覆核，以確保權限管理之正確性。
資料管理	•專業型儲存設備 •本地備援架構 •異地資料備份	•避免資料遺失	•專業型儲存設備具有高可用性的備援能力，專案研發資料皆有權限控管，僅允許授權成員進行存取。 •公司研發資料有完整的定期備份機制。 •採取異地存放，以確保災難發生時的復原能力。

2. 制訂資訊系統緊急應變辦法，為使資訊作業在發生天災或人為破壞後，能依序採取緊急應變措施，儘速回復各項電腦作業，以維持公司業務之運作。並規定倘若發生資安事件，應立即成立緊急狀況重大危安事故應變小組，由執行長及各部門主管依職權編組，負責資訊安全事件緊急應變處理，並由資訊部門負責執行資訊安全預防、危機通報及緊急應變處理等相關措施。

   資訊安全處理程序：



實際與預計投入資通安全管理之資源

✧ 已投入之資通安全管理資源

1. 資安會議：每半年召開 TQM E 化委員會會議。
2. 防毒防護：防火牆、自動更新病毒碼等，確保最佳防護機制。
3. 備援機制建置：建構備份管理機制與系統，確保資料之安全與可用。
4. 資安案例分享與強化資安意識：不定時，隨時接獲可疑案件即進行分析與宣導。
5. 投入人力如：每日各系統狀態檢查、每週定期備份及備份媒體異地存放之執行、不定期資安宣導、每年系統災難復原模擬演練、每年對資訊循環之內部稽核、會計師稽核等。

✧ 預計投入之資通安全管理資源

1. 資安專職人員：負責資安架構設計、資安維運與監控、資安事件回應與調查、資安政策檢討與修訂。

本公司資訊部門執行作業依規定程序均能落實執行，風險評估結果尚屬良好， 近來資安攻擊事件頻傳，本公司積極加強資訊安全維護措施，建立員工資安 觀念，降低公司營運風險。最近年度並無因重大資通安全事件之情形。