資訊安全政策及管理方案

資訊安全管理目的

確保本公司資訊安全，維護公司資訊之機密性、完整性及可用性，以符合公司客戶、廠商及公司投資人期待，規劃資訊安全風險管理架構進行流程循環管理，並訂定資訊安全政策，資訊人員應依照資訊安全措施事項執行相對應控制項目。

資訊安全風險管理架構

1. 本公司資訊安全之權責單位為資訊部，該部設置資訊主管一名與專業資訊人員數名，負責訂定內部資訊安全政策、規劃暨執行資訊安全作業與資訊安全政策推動與落實。
2. 本公司資訊部門直接對總經理匯報內部資訊安全執行狀況，若有發現缺失，即提出相關改善計畫與具體作為，且定期持續追蹤改善成效，以降低內部資訊安全風險。
3. 本公司資訊部採用循環流程管理模式，確保可靠度目標之達成且持續改善。
4. 資訊安全風險管理循環流程各相關單位，需配合執行需求召開會議，檢討流程執行成效，稽核室應協助督導執行單位積極配合，確保資訊安全管理工作確實執行。
5. 資訊部定期於年度資訊績效評估，就執行資訊安全政策過程中發現需改善之項目，出具報告向稽核室說明修正並達成共識，得修正之。

資訊安全政策

本公司資訊安全政策，包含以下四個面向：

1. 規範辦法：訂定公司資訊安全管理辦法，規範人員作業行為。
2. 硬體建置：建置完善資訊安全設備，落實資訊安全管理。
3. 人員教育：定期及遇有重大資訊安全事件進行知會，以提昇全體同仁資訊安全意識。
4. 政策檢討：推動資訊安全持續改善，確保企業永續經營。

資訊安全管理措施

本公司定期審視內部資訊安全規範，根據資產價值、弱點、威脅與影響性，分析內部風險水平，並以此風險評估結果制定安全措施強化項目，精進且提升整體資訊安全環境，以確保本公司持續營運能力。

1. 本公司資訊風險管理程序如下：

未發生前：定期自主盤點檢驗，從流程與技術多方面著手，主動預防資訊安全事故

a) 防入侵：主動防禦來自內外網攻擊，侵入資訊系統造成破壞。
b) 防外洩：主動防範公司機敏資訊及營業秘密遭外流外洩，影響公司永續營運。
c) 防意外：主動預防環境內因素（故障/跳電 / 病毒 / 設備遺失）造成的生產損失。

事件發生時：損害控制緊急應變

a) 完善機制：建立有效的災害應變機制，迅速將損害控制。
b) 落實演練：運用演練經驗，在最短時間內恢復正常，維持企業體持續營運。

發生以後：追查並列入預防

a) 避免問題發生：調閱系統紀錄追蹤問題原因，擬定對策成新預防措施。
b) 查核方法再強化：引入外部顧問/弱點檢測團隊，定期查核盲點提高內控機制可靠性。

2. 具體管理措施如下表：

管理項目	說明	具體作法
權限管理作業	帳號、系統權限管理措施	●帳號的申請、異動、刪除管理。 ●權限的分級控管、盤點與查核。 ●不同職務別的網路存取控制。
資料管理作業	人員存取系統及資料之管理與控制措施	●資料及系統之存取權限控管。 ●存取使用軌跡之紀錄。 ●文件加密系統的佈署。
外部威脅管理	檢視所有可入侵的管道，進行封阻及建置相關預防措施	●建置次世代防火牆設備與主動式端點可疑的滲透攻擊偵測系統，防堵入侵攻擊於機房主機與使用者端，有效阻絕目前各式各樣的網路攻，強化駭客入侵預防。 ●垃圾郵件篩選及隔離機制，以防止收到夾帶病毒之電子郵件。 ●伺服器與使用者電腦皆安裝防毒軟體，定期掃毒，防範病毒攻擊。 ●伺服器、使用者電腦定期漏洞更新。
系統穩定管理	建立相關預防措施，減少因系統中斷所造成的損失	●系統/網路可用狀態監控及通報機制。 ●系統中斷之應變措施。 ●資料備份與還原管理措施。 ●系統災難復原管理措施。

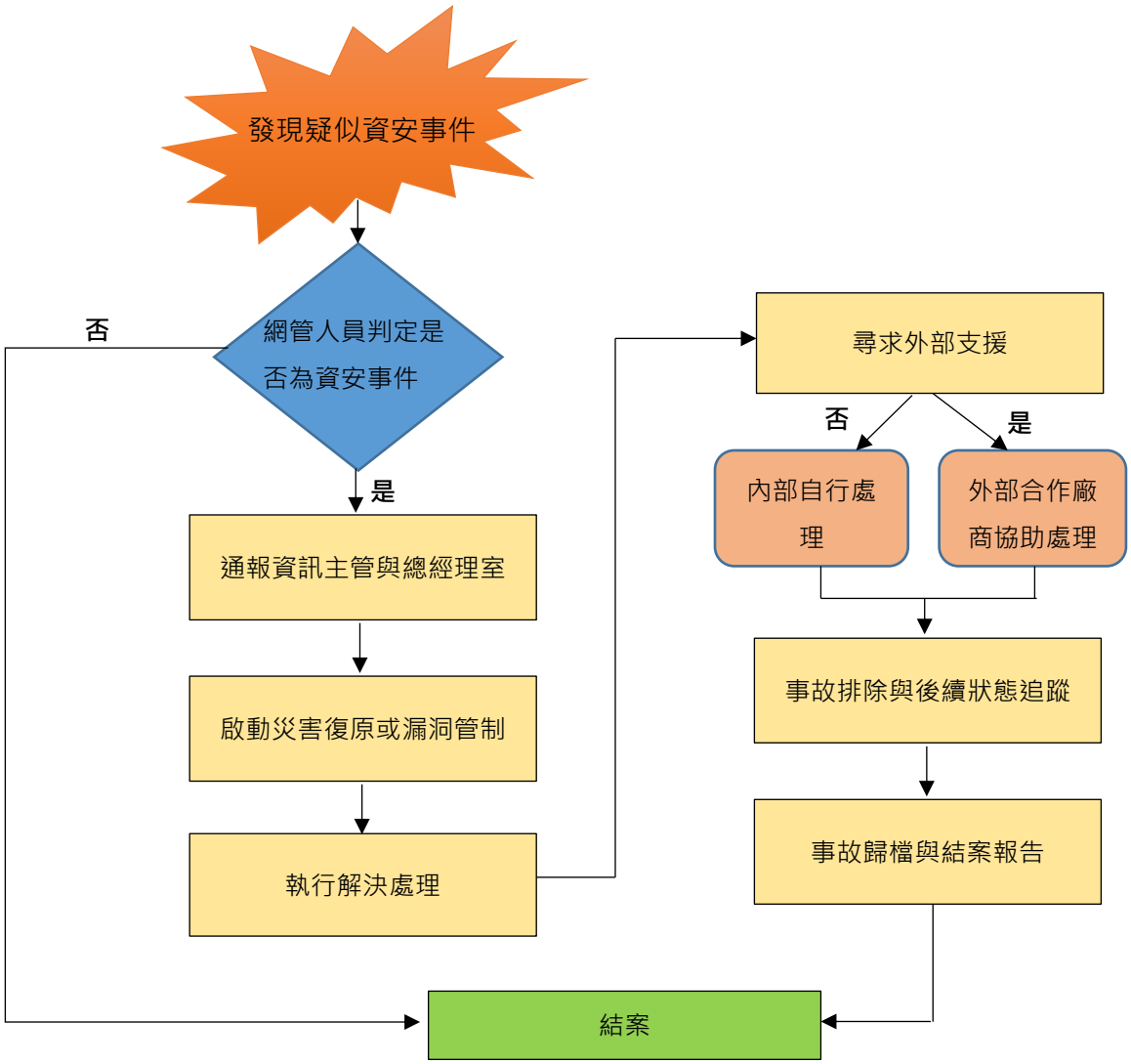
3. 定期執行弱點與漏洞辨識掃描、異常行為檢測

健診類別	健診項目	定義
營運韌性檢視	網路架構檢視	檢視網路架構與資安設備配置是否合宜，包含網域伺服器等相關主機
	防火牆規則檢視	檢視防火牆規則與存取控管設計是否妥善
	目錄伺服器檢視	檢視目錄伺服器群組原則安全性，可依「政府組態基準」為標準判定
異常行為偵測	使用者端電腦惡意活動檢視	單次惡意程式檢測，確認使用者電腦是否存在惡意程式活動
	伺服器主機惡意活動檢視	單次惡意程式檢測，確認伺服器是否存在惡意程式活動
弱點與漏洞辨識	伺服器弱點掃描(含複測)	使用工具/軟體辨識伺服器中存在那些可被攻擊/威脅的弱點
	滲透測試	針對特定主機進行灰箱滲透測試，驗證弱點可利用性

113 年資訊安全執行情形

- 一年四次社交演練測試，並對不合格人員進行資安意識強化訓練考試，加強員工對於資訊安全防範的警覺性與意識。
- 113 年進行兩次資安教育訓練，公布考試不合格人員會並加強宣導。
- 執行資安弱點掃描與滲透測試，檢視內部資訊安全漏洞並即時漏洞修補。
- 各廠防火牆 SOC 即時監看告警服務，強化資訊安全即時防禦功能。
- SOC+SIEM 關聯分析服務，提供全時段資安防護監控告警。
- 強化內部網站安全性(SSL 憑證)，提高系統資料傳輸安全性。
- 系統雲端異地備援導入，強化備份資料災害復原可用性。
- 授權軟體管控軟件，嚴格禁止綠色軟件、非授權軟件使用。
- 通過 ISO 27001(證書有效日期 2024/2/22~2027/2/21)資訊安全管理制度複查。

資訊安全事件通報程序


發現疑似資安事件
網管人員判定是否為資安事件
否
是
通報資訊主管與總經理室
啟動災害復原或漏洞管制
執行解決處理
尋求外部支援
否
是
內部自行處理
外部合作廠商協助處理
事故排除與後續狀態追蹤
事故歸檔與結案報告
結案