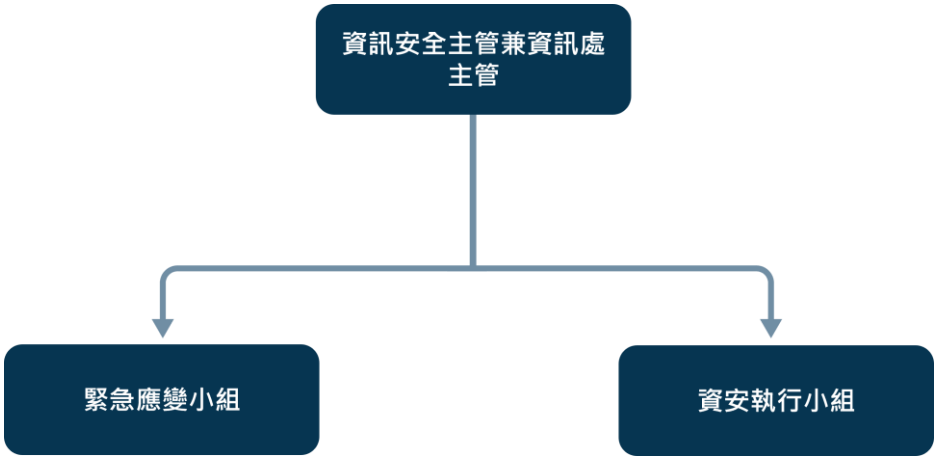
資訊安全管理

一、 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處，設置資訊主管一名與專業資訊人員四名，負責訂定企業內部資訊安全政策、規劃暨執行資訊安全作業及推動與落實資安政策，並定期公佈公司資安治理概況。

   以下為本公司資安小組組織架構：



2. 本公司稽核處為資訊安全內控之督導單位，該處負責督導內部資安執行狀況，若有查核發現缺失，即要求受查單位提出相關改善計畫與具體作為，且定期追蹤改善成效，以降低內部資安風險。
3. 組織運作模式採用 PDCA（Plan-Do-Check-Act）循環式管理，確保可靠度目標達成且持續改善，流程如下圖所示：

二、 資訊安全政策及具體管理方案

1. 目的：

(1) 為維護企業整體資訊安全、強化各項資訊資產之安全管理，確保其機密性、可用性、完整性，以維持公司正常營運需要。

(2) 為確保公司主機、網路相關設備與通訊安全，並能降低因人為疏失、蓄意與天然災害導致之資訊資產的遭竊、誤操作、洩漏、遭竄改、中止服務或是破壞等風險，建立資訊安全管理規範。

2. 原則：

(1) 資訊安全是全體從業人員責任。

(2) 資訊安全管理系統必須符合公司業務需求。

(3) 資訊安全管理須符合相關法令、公司規範與契約要求。

（4）資訊資產應訂定分類分級程序，依安全等級標示分級管理。

（5）從業人員若違反本安全政策或相關法令以致危害公司資訊安全，資訊部門應即報准停止其使用，並依情節輕重送公司相關單位處置。

3. 管理措施：

本公司除建置安全的資訊環境外並逐年投入預算期能改善弱點以提升作業效能，相關管理方案如下

（1） 網路安全

a. 建置防火牆以阻斷外部網路攻擊
b. 建置 Client 端防護，防止電腦病毒與駭客入侵
c. 電子郵件的鏡像、防毒與落實 DMARC、SPF 機制，以防止垃圾郵件與惡意程式攻擊

（2） 資料安全

a. 每日與固定排程將重要系統資料與資料庫做備份與落實異地備援機制並定期做還原測試
b. 重要的系統虛擬化並每日排程備份與異地備援建立
c. 每年度作災難復原演練

（3） 教育訓練與宣導

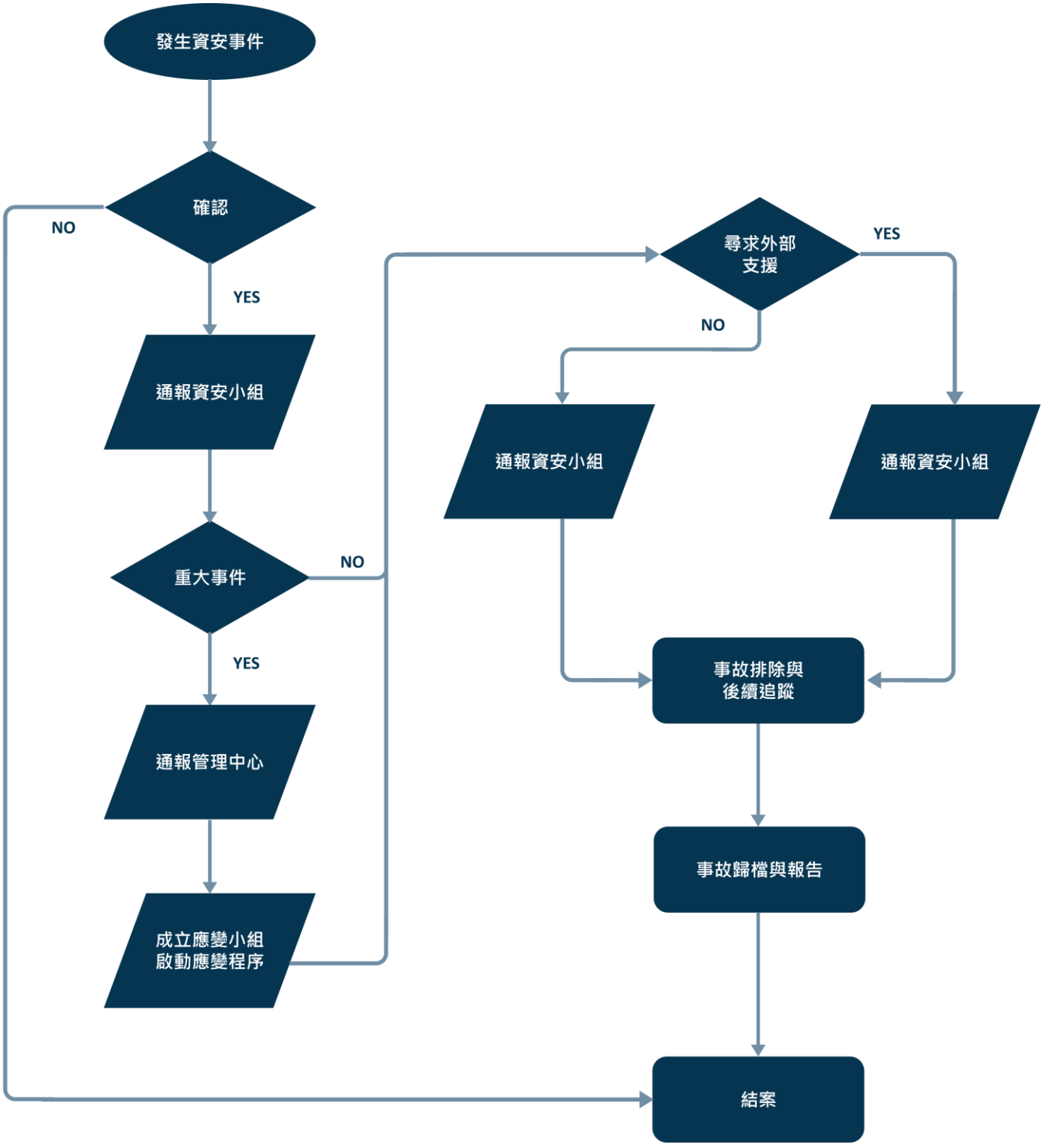
a. 定期公告資安事件與提醒
b. 日常加強從業人員對郵件社交工程之警覺性
c. 訓練時數如下：

年度	教育訓練參與人數	訓練時數
114	531 人	531 小時
113	385 人	385 小時
112	329 人	329 小時

（4） 從業人員資安

a. 簽訂從業人員安全保密切結書
b. 提供從業人員在職期間之教育訓練，以確保資訊相關資產與作業時的安全與正確

4. 本公司資訊安全通報與事故處理流程程序如下圖：



三、投入資訊安全管理之資源

1. 外部連線存取

   為避免外點人員因使用 VPN 服務而造成帳號密碼外洩，導致駭客入侵的威脅，在人員的識別及認證部份，啟用多因素認證因子機制來強化，提高連線存取安全性。

2. 系統規範（密碼強度）

   調整密碼長度應至少 8 碼以上，並且混合大小寫英文字母、數字，以降低密碼洩漏風險。

3. 資安人員與素養

   本公司之資安小組，設置資訊安全主管一名（由資訊處主管兼任）與資安人員兩名（由資訊處成員兼任）。

   (1) 資安小組成員參與不定期的資安講座，與線上訓練課程，讓資安人員可以掌握最新的資安訊息，以提高風險意識，每一年訓練時數至少為 12 小時。

   (2) 資安小組每年針對公司資安政策會議討論兩次。

4. 基礎建設

   防毒軟體更新與核心防火牆更換、ERP 系統虛擬化與更換虛擬化主機。

5. 人員資安意識

   (1) 每個月於 EIP 內分享一篇資安相關議題與建議處置措施。

   (2) 每個月教育訓練中做資安宣導。

   (3) 除資安宣導外，針對內容同時施作測驗以確認理解程度。