中釉資通安全政策

為確保公司資訊財產保有機密性、完整性、可用性之資訊安全要求，資訊室制定中釉資通安全政策，由總經理核定頒布後供全體員工遵守依循，其目標為確保公司資訊環境運作正常、公司各項業務持續營運。

主要管理策略為適時宣導資訊安全相關訊息並提升公司所有電腦用戶資安意識，提升中釉資訊安全控管技術與能量、降低危害因素與風險，透過內部及外部稽核制度檢視資訊安全狀況並評估公司資訊作業內部控制之有效性。

為落實資安管理，資訊室訂有資通安全管理辦法，期望全體同仁共同努力達成下列目標

- 確保公司資訊環境安全。
- 確保使用人員權責清楚劃分。
- 確保資訊系統正常運作。
- 確保資訊安全落實執行。

中釉資通安全管理方案

- **人員管理**

  新進員工確實填寫帳號及權限申請單。

  離職員工確實通報資訊室停用其相關資訊帳號。

- **系統管理**

  各單位依據相關需求申請適當系統使用權限，並經由主管簽核後交由資訊室處理。

- **機房管理**

  人員進出機房須確實登記並定期檢視維持資訊設備正常運作。

- **備份還原管理**

  落實系統及資料備份作業以確保資料之完整性及可用性，定期實施還原演練。

- **資料管理**

  資料存取依照使用者權責權限申請經相關主管簽核後由資訊室設定規範。

- **網路管理**

  落實用戶端上網管控並建立網路防火牆與相關網路防護安全機制杜絕網路危害。

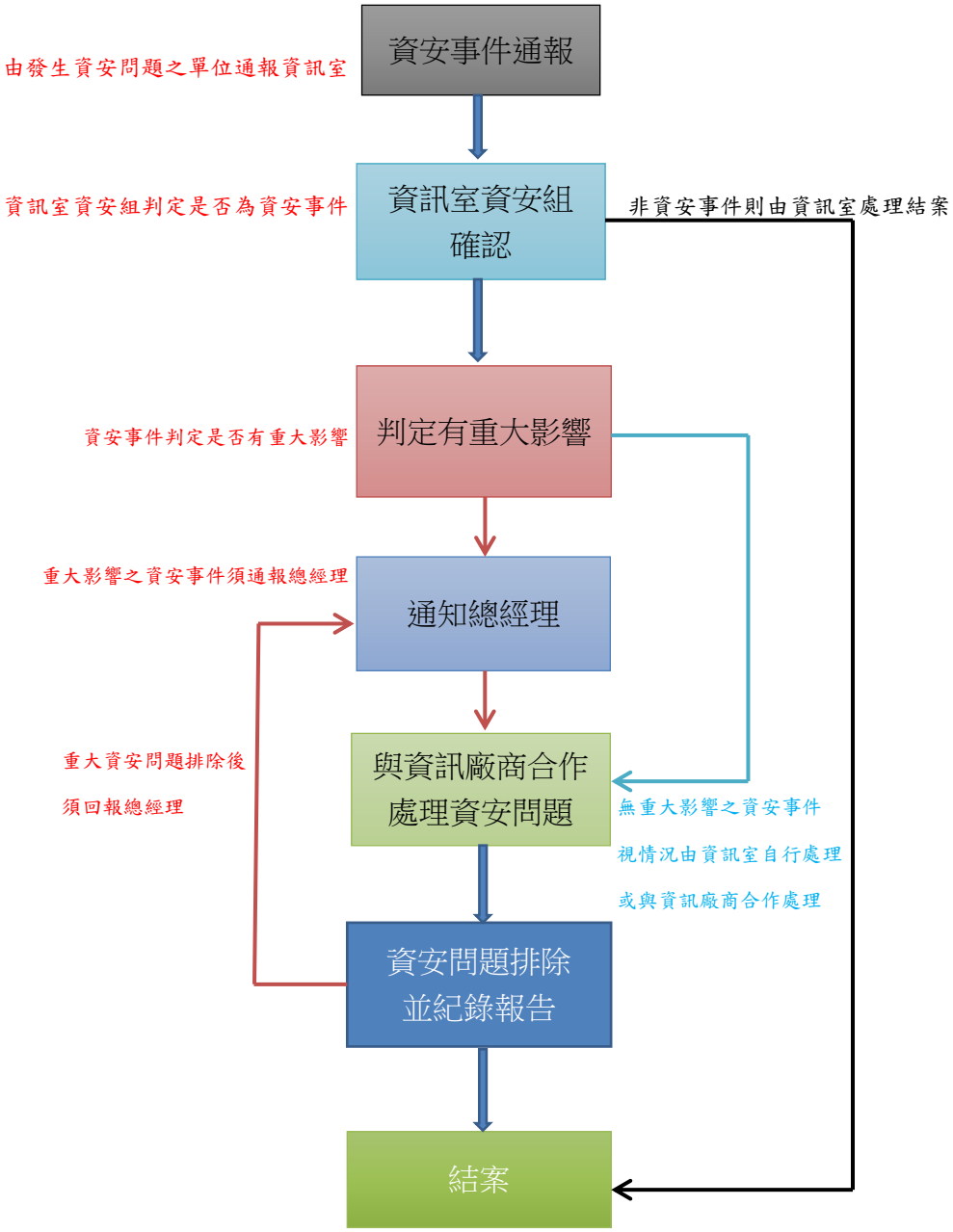
- **用戶電腦管理**

  防毒及端點防護系統確實安裝並執行、USB 及相關移動儲存裝置列入控管。

- **資訊系統維運服務廠商管理**

  確保廠商執行作業時符合資安管理規範。

中釉資安事件通報處理流程



流程說明：

資安處理流程 → **非資安事件** → **一般資安事件** → **重大資安事件** →

備註 ： 重大資安事件係指造成公司營運受到影響以致營運發生無法正常作業。

資通安全具體防護與因應措施

- 網路安全
  對外網路與中華電信簽訂企業網路防禦系統服務及企業資安服務。
  更新網路頻寬管理及防火牆設備。

- 系統安全
  確實執行每日系統及資料備份，系統主機全面建置 Kaspersky Hybrid Cloud Security 伺服器防毒系統。

- 郵件安全
  導入 SPAM 郵件進階防護方案，加強防護釣魚郵件、病毒郵件、勒索郵件、惡意郵件等危害郵件攻擊。

- 用戶端安全
  全面更新用戶端防毒軟體並導入 EDR 端點防護，全面控管用戶端 USB
  及移動儲存設備之使用。

- 資安聯防
  加入台灣電腦網路危機處理及協調中心及資安聯誼會，隨時掌握最新資安威脅，
  並採取適當應對方案

重大資通安全事件

- 111 年度截至目前為止，本公司無重大資安事件發生。