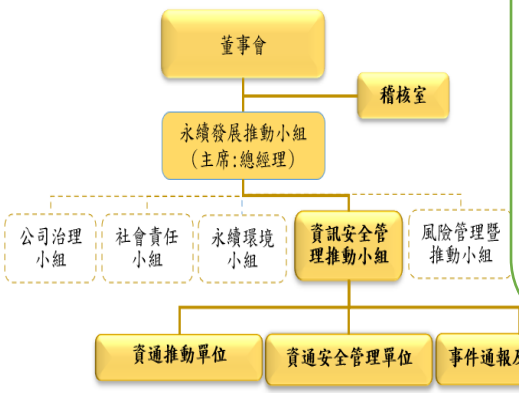
資訊安全

1 資訊安全政策及架構

有鑑於資安攻擊手法日新月異，如社交工程攻擊、APT 進階持續性滲透攻擊、DDOS 分散式阻斷服務攻擊等，為免於被惡意或意外之入侵、破壞及洩露，本公司致力於強化資訊安全管理，以確保所屬之資訊資產機密性、系統完整性及流程管理、設備及網路安全，以提供資訊業務持續運作環境，避免因資訊安全問題造成營運上不必要的損失。

為強化資訊安全管理，確保所屬之資訊資產的機密性、完整性及可用性，以提供本公司之業務持續運作環境，並符合相關法規之要求，使其免於遭受內、外部的蓄意或意外之威脅，本公司已訂定「資通安全政策」，並於永續發展推動小組下，設立「資通安全管理推動小組」，配置適當之人力、物力與財力資源，並指派適當人員擔任資安專責主管及資安專責人員，以負責推動、 協調監督及審查資通安全管理事項。資安主管已於2025年 11 月 6 日向董事會報告公司資訊安全治理與執行狀況。

資訊安全管理推動小組架構



資訊安全目標

- 確保本公司資料、系統、設備及網路之安全。
- 確保本公司資訊業務服務之持續運作。
- 確保資訊需經授權人員才可存取、使用及修改資訊，以確保其機密性、正確性與完整性。
- 確保本公司各項業務服務之執行須符合「資通安全管理法」及其他相關規定，以及相關法令規範之要求。
- 保護本公司業務及服務相關資料之安全，免於因外在威脅，或內部人員不當之管理與使用，致遭受竊取、竄改、毀損、滅失、洩漏或其他侵害等風險。
- 提升對個人資料之保護與管理能力，降低營運風險，並創造可信賴之個人資料及隱私保護環境。

2 資訊安全治理策略及防護措施

蜜望實已建立資訊安全相關管理制度，明訂相關政策、管理程序與規範，以維護公司競爭力並保障客戶權益。

資通安全管理單位每年進行資通系統盤點及資通安全風險評估，就核心業務及核心資通系統鑑別其可能遭遇之資安風險，進行風險評估，分析其喪失機密性、完整性及可用性之衝擊，並執行對應之資通安全管理面或技術面控制措施。同時，對核心資通系統定期或不定期(視需求)辦理弱點掃描、滲透測試及源碼掃描等資安檢測，並針對安全漏洞進行評估，並完成系統弱點修補。蜜望實致力於資安防護，更是參考業界做法與主管機關及專家意見，建構資安防護措施，以確保公司資安實務的有效性並降低風險。

存取控制管理

- 使用者存取管理
- 帳號密碼管理、權限控制、
- 密碼複雜度、更換週期、密碼錯誤鎖定規則、定期檢查帳應用系統存取控制號
- 網路存取控制
- 網路區隔、防火牆、網路連線控制、權限控管
- 作業系統存取控制
- 避免明碼顯示密碼、登入時間限制、登入失敗次數限制
- 應用系統存取控制
- 存取之限制、原始程式資源之存取控制
- 資料庫存取控制
- 帳號密碼管理、存取權限限制
- 遠端連線存取控制
- 核准、身分辨識、加密安全通道
- 電子郵件安全管理
- 申請、刪除、定期清查、社交工程演練
- 資通安全防護設備
- 防毒軟體、防火牆、電子郵件過濾機制、惡意程式檢測、每年資安防護控制措施與防護現況檢視

實體與環境安全

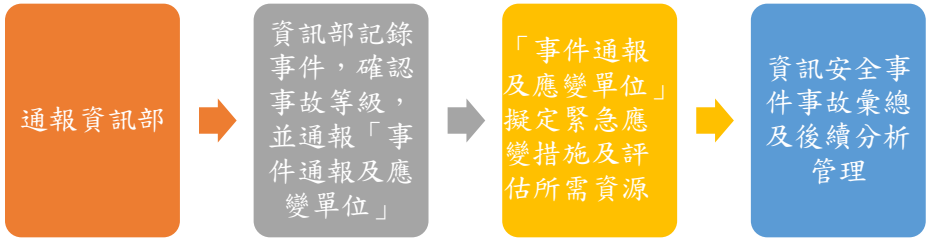
- 資訊資產管理與維護
- 採購、借出、維護、故障及汰除管理
- 資料檔案之安全控制
- 備份、回復測試、保存管理
- 資通系統之密碼管理
- 密碼管理
- 人員裝置使用管理
- 簽屬「員工資通安全管理暨裝置使用
- 規範」及「員工保密合約書」
- 重要區域安全管制
- 門禁管制、攝影監視器
- 環境支援設備管理
- 滅火器、緊急照明設備、
- 溫濕度管控機制、危險物品管制
- 電源設備管理
- 不斷電及穩壓設備、電力開關及地線接地

資料輸出入及處理

- 資料輸入控制
- 權限控管、序號控號、錯誤訊息提醒
- 資料輸出控制
- 權限控管、指定人員負責分送
- 資料輸出入錯誤控制
- 建立處理程序、錯誤更正之控制建立處理程序

3 資訊安全事件通報與處理流程

資安事件之處理效率關乎其對公司之衝擊影響程度，若重大資安事件未能及時處理將可能影響客戶交期需求，以及對蜜望實的信任。為提升資安事件處理效率，使同仁於資安事件發生時能有所依循，降低事件衝擊之潛在影響風險，蜜望實已訂有資通安全事件通報及應變程序，使同仁於資安事件發生時能有所依循，提升處理效率，並降低事件衝擊之潛在影響風險。



2025 年，蜜望實無違反法規及利害關係人之資安申訴事件，亦未發生資安事件。

4 資訊安全教育訓練

蜜望實為提升全體員工基礎資訊安全知識與緊急應變能力，規範全體員工每年皆需參與資訊安全教育訓練，全數新進人員則需依據「員工教育訓練程序」完成職前資安教育訓練，每年確保員工能了解應盡之責任與義務，以提升員工資訊安全意識。資訊部亦會不定期以郵件通知最新資安事件或訊息，以及相關注意事項，以協助同仁提升資安意識。

2025 年資安教育訓練實施狀況