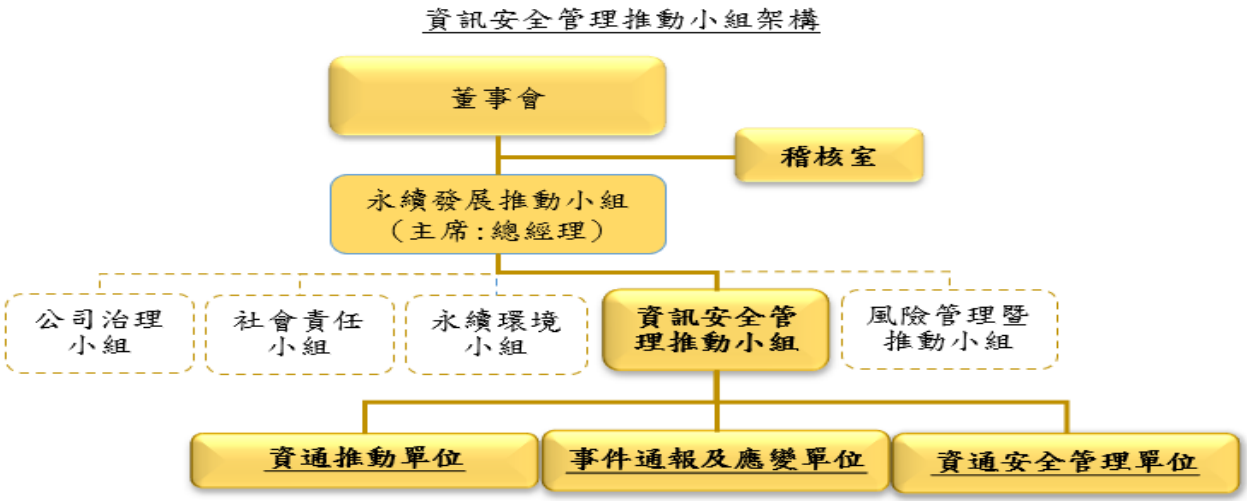
蜜望實企業股份有限公司
資訊安全管理

資訊安全風險管理架構

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。



資訊安全政策

一、目的：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。

二、目標：本公司為有效運用資源，配合資訊安全工作之推行，對於資訊資產其重要性予以不同優先等級之保護，以達到最大資訊安全效果。本公司資訊安全政策旨在確保公司營運順暢、資訊資料完整、企業機密安全，以保障公司本身之信譽。目標如下：

(一)建立安全及可信賴之資訊化作業環境，確保本公司資料、系統、設備及網路之安全，以保障本公司業務永續運作。

(二)建立本公司核心業務持續運作計畫，以確保本公司資訊業務服務之持續運作。

(三)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。

(四)保護本公司業務服務之安全，確保資訊需經授權人員才可存取及使用資訊，以確保其機密性。

(五)保護本公司業務服務之安全，避免未經授權的修改，以確保其正確性與完整性。

(六)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。

(七)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。

蜜望實企業股份有限公司
資訊安全管理

資訊安全具體管理方案

一、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。

二、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。

三、資通安全防護

本公司為防範各種外部資安威脅，建置多項資安防護系統，以提昇整體資訊環境之安全性。

項目	具體管理方式
存取控制	使用者存取控制 建立使用者通行碼管理之作業規定，以管理使用權限，如：密碼長度、密碼複雜度、強制定期更新密碼、登入失敗鎖定機制。 定期審查使用者帳號及權限，停用久未使用之帳號。 網路存取控制 區隔內部網路及聯外方式，設置對外之網路防火牆，以防止駭客非法入侵。 建置訪客使用之無線*網路*名稱(SSID)及無線密碼，限制*使用*者存取無線網路的權限。 對於開放提供外部客戶或廠商存取之服務，必須限制使用者之網路功能以確保網路安全。 作業系統存取控制 避免明碼顯示密碼。 設定系統登入之不活動時間限制，如果超出時間限制，啟動螢幕保護程式或系統將自動中斷登入。 限制登入失敗次數及超過次數暫時鎖定帳號時間。 應用系統存取控制 應用系統資訊之使用，僅限業務相關之授權使用者，並加強權限控管措施。 應用程式原始碼，應集中存放控管。應用程式之異動需經適當控管。 資料庫存取控制 資料庫預設帳號應變更密碼，或是關閉使用。 資料庫之存取權限，應經適當程序之授與及移除，且須使用獨立之帳號及密碼登入。 遠端連線存取控制 控管遠距工作，遠端連線必須經過加密之安全通道，例如：SSL-VPN，以維護網路及資料安全。 員工或廠商由遠端登入公司內部網路系統，應取得權責單位主管之核可，且均留有使用紀錄可稽查。 電子郵件安全管理 電子郵件伺服器應設置防毒及垃圾郵件過濾防堵系統，並適時進行軟硬體之必要更新。 定期進行電子郵件帳號清查。 定期舉辦電子郵件社交工程演練，並檢討執行情形。 資通安全防護設備 建置防火牆、電子郵件過濾機制或其他入侵偵測設備等防止外部網路入侵對策，並定期更新。 與網路相聯之資通系統，應隨時更新，並安裝防毒軟體，定期執行惡意程式檢測。

蜜望實企業股份有限公司
資訊安全管理

項目	具體管理方式
	每年檢視資安防護控制措施與防護現況。
實體與環境安全	備份 系統、資料庫及各類檔案定期定期備份，並做成紀錄。 備份檔案應保留一份以上之備份資料，並應分別放置不同處所。 資訊設備維護 指定專人負責機房內各項機器保養及維護，並適當紀錄，必要時應與設備供應商簽訂維護合約，以保障各項硬體設備之正常運作。 資訊設備汰除時，由資訊單位執行儲存媒體資料清除或銷毀作業。 人員裝置使用管理 員工簽屬「員工資通安全管理暨裝置使用規範」及「員工保密合約書」，使員工了解相關使用規範及保密之義務。 環境與區域設備安全控制 重要區域門禁管制，重要之進出入口應建置可攝影監視器進行進出軌跡記錄。 電腦主機、各應用伺服器等設備均設置於專用機房，機房門禁採用感應刷卡進出，全天候錄影監控，且保留進出紀錄存查。 機房內外或其他重要區域應設置滅火器及緊急照明設備。 機房應建置溫濕度管控機制（如空調設施），維持電腦設備於適當的溫度環境下運轉。 電源設備管理 配置不斷電與穩壓設備，避免台電意外瞬間斷電造成核心資通系統與重要設備應當機，或中斷運作。
資料輸出入處理	透過權限控管、序號控號及錯誤訊息提醒進行資料輸出入控制。 建立資料錯誤更正處理程序，以利管理。
永續運作	為確保本公司業務持續運作，應建立重要系統之業務持續運作計畫並落實定期進行演練。 租用電信公司兩條數據線路，透過頻寬管理設備，兩線路並聯互為備援使用，確保網路通訊不中斷。 指定專業人員負責處理有關資訊系統安全預防及危機處理相關事宜，以防範電腦網路犯罪，維護資訊系統安全。

四、訂定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。發生符合「財團法人中華民國證券櫃檯買賣中心對有價證券上櫃公司重大訊息之查證暨公開處理程序」規範之重大資安事件，應依據「內部重大資訊處理暨防範內線交易管理作業程序」規定辦理。

五、訂定資訊作業委外安全管理程序，包含委外選商、資通安全責任、保密、監督管理（如：對供應商與合作夥伴進行稽核）及委外關係終止之相關規定，確保委外廠商執行委外作業時，具備完善之資通安全管理措施。

六、人員安全與訓練

(一)資安專責主管及資安專責人員每年應參加資通安全相關之教育訓練。

(二)為提升全體員工基礎資訊安全知識與緊急應變能力，新進人員則需完成職前資安教育訓練，而全體員工每年皆需接受資訊安全宣導課程，以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。

(三)資訊部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。

(四)對於在電子郵件社交工程演練中誤開啟信件或連結之人員進行教育訓練，並留存相關紀錄。

七、定期向董事會報告資通安全執行情形，確保運作之適切性及有效性。

投入資通安全管理之資源

為實踐資通安全政策，投入之資源如下：

一、網路硬體設備如防火牆、郵件防毒、垃圾郵件過濾、上網行為分析、網管型集線路等。

二、軟體系統如端點防護系統、備份管理軟體、VPN認證及加密軟體等。

三、電信服務如多重線路、入侵防護服務等。

四、投入人力如: 每日各系統狀態檢查、每日定期備份及備份媒體異地存放之執行、每年至少一次資安宣導教育課程、每年系統災害復原執行驗練、不定期通過電子郵件向整個公司發送網絡安全信息等。

五、資安人力：於112年3月10日第11屆第18次董事會通過任命資訊部門主管劉芳利協理為資安主管，轄下有專業資訊人員2名，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。資安主管已獲得國際電子商務顧問局（EC-Council）CEH Master、ECSA v4、LPT、CHFI v8、CTIA認證。專業資訊人員皆取得NSE 4網路安全專家認證。

六、為提高員工資訊安全意識，於113年8月20日至8月26日共7天，進行社交工程演練，本次社交工程演練結果皆有達到20%以下的標準。

七、本公司於113年9月10日及12日舉辦資訊安全教育訓練課程，受訓人數81人。

八、資安專責主管及資安專責人員113年度參加資訊安全培訓課程共計111.5小時。

九、加入「臺灣電腦網路危機處理暨協調中心」(TWCERT/CC)及台灣資安主管聯盟等資安情資分享組織，取得資安預警情資、資安威脅與弱點資訊。

十、資安主管已於113年11月7日向董事會報告公司資訊安全治理與執行狀況。

本公司資訊部門執行作業時，依公司規定程序均能落實執行，確保資料完整及安全。113 年度，資訊安全並無重大不利影響且無重大營運風險。