本公司於 2019 年成立資安小組，由管理部副總經理擔任召集人，定期評估資訊安全風險並向董事長報告，本公司資訊安全評估重點如下：

一、 資訊架構檢視

二、 網路活動檢視

三、 網路設備、伺服器及終端機等設備檢測

四、 網站安全檢測

五、 安全設定檢視

六、 防毒及備份作業。

各項主要評估項目與具體管理方案分述如下：

一、 資訊架構檢視：

檢視對於持續營運所採取相關措施之妥適性檢視相關措施之架構與維運機制是否存在單點失效之風險，並尋求外部專業廠商，針對對資訊及資安架構進行風險分析，並提出安全評估之結果與建議。

二、 網路活動檢視：

檢視設備之存取紀錄及帳號權限檢視網路設備、資安設備及伺服器之存取紀錄、帳號權限之授予與監控機制是否符合內控作業規範；以最小權限原則清查該等設備之帳號權限及存取紀錄，識別異常紀錄與確認警示機制。

三、 網路設備、伺服器及終端機等設備檢測：

定期或適時辦理網路設備、伺服器及終端機的弱點掃描，並針對所發現之弱點進行改善、修補作業。評估弱點掃描作業之範圍、作業模式及弱點改善計畫與修補情形，針對掃描結果提出評估建議，重點在於找出架構中可能存在的弱點與漏洞，予以改善及修補，降低整體之資安風險。

四、 網站安全檢測：

針對網站進行安全檢測，儘早發現網站暴露於外之弱點，並進行修復。

五、 安全設定檢視：

檢視伺服器(如：網域服務 Active Directory)有關「密碼設定原則」與「帳號鎖定原則」之設定，透過工具分析及人工作業，檢視相關網域安全性原則設定是否符合內控規範。

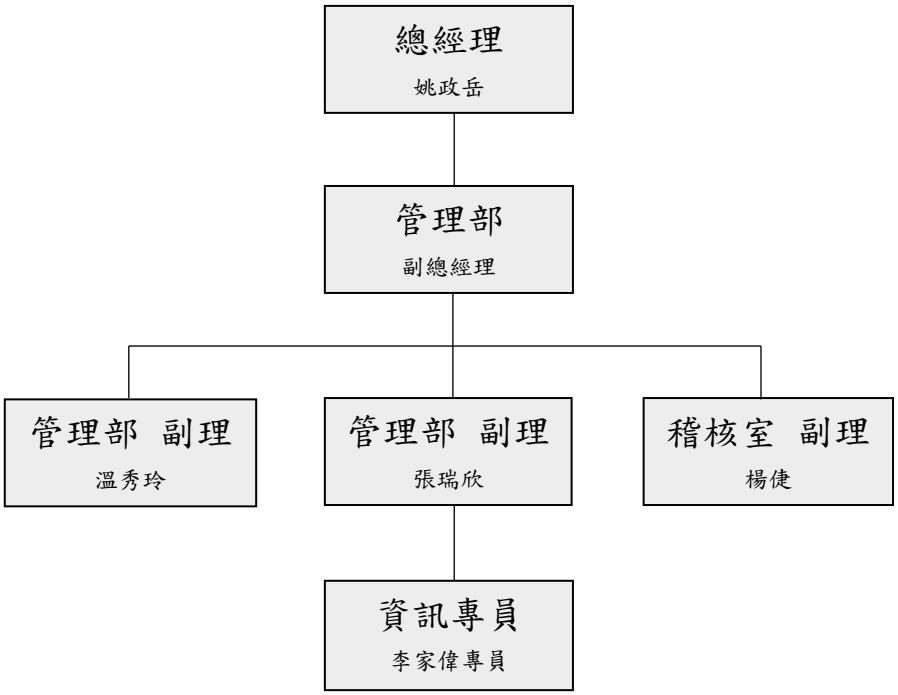
六、 防毒及備份作業：

讓同仁瞭解使用電子郵件之風險，提高同仁防範釣魚郵件等攻擊所造成之風險，並強化異地備份作業，進而達到保護資料及重要營運資訊與服務之目的。

亞昕國際開發股份有限公司

資訊安全組織及架構

設立目標:為確保公司內部資通安全管理事項之推動，以強化公司資安治理能力。



亞昕國際開發股份有限公司

資通安全管理之資源量化數據

項目	2022 年
資通安全相關人力投入	2 人
資通安全相關軟硬體採購	$935,000
資通安全相關會議	4 次
資通安全相關教育訓練	132 hr