資訊安全管理

昇佳電子為確保公司資訊安全管理制度之資訊安全責任，落實資訊安全政策之推行，在組織內部建立管理框架啟動與控制資訊安全的實施，建立有管理領導階層參加的管理小組，以核准資訊安全政策、分配安全責任、並協調實施全組織的安全措施。昇佳電子已於 2024 年 2 月取得 ISO/IEC 27001：2022 資訊安全管理系統認證（證書序號 10584069；有效期間 2024 年 2 月 9 日至 2027 年 2 月 8 日）。 昇佳電子 2024 年「零」重大資安事件。

目標時程

規畫方向

短期目標

- 持續進行系統日誌蒐集與分析
- 持續進行網路設備日誌蒐集與流量分析
- 持續進行端點偵測及應變措施（EDR）
- 持續進行端點設備自動化安全性漏洞更新

中期目標

建立資通安全威脅偵測與管理平台（SOC），並滿足以下目標

- 資訊安全事件高可視性
- 蒐集各系統來源數據
- 半自動化漏洞修補
- 網路終端設備管理與流量異常監控

長期目標

長期目標包括更全面的資訊安全體系建立和持續改進，以確保組織的資訊資產得到充分的保護和管理。

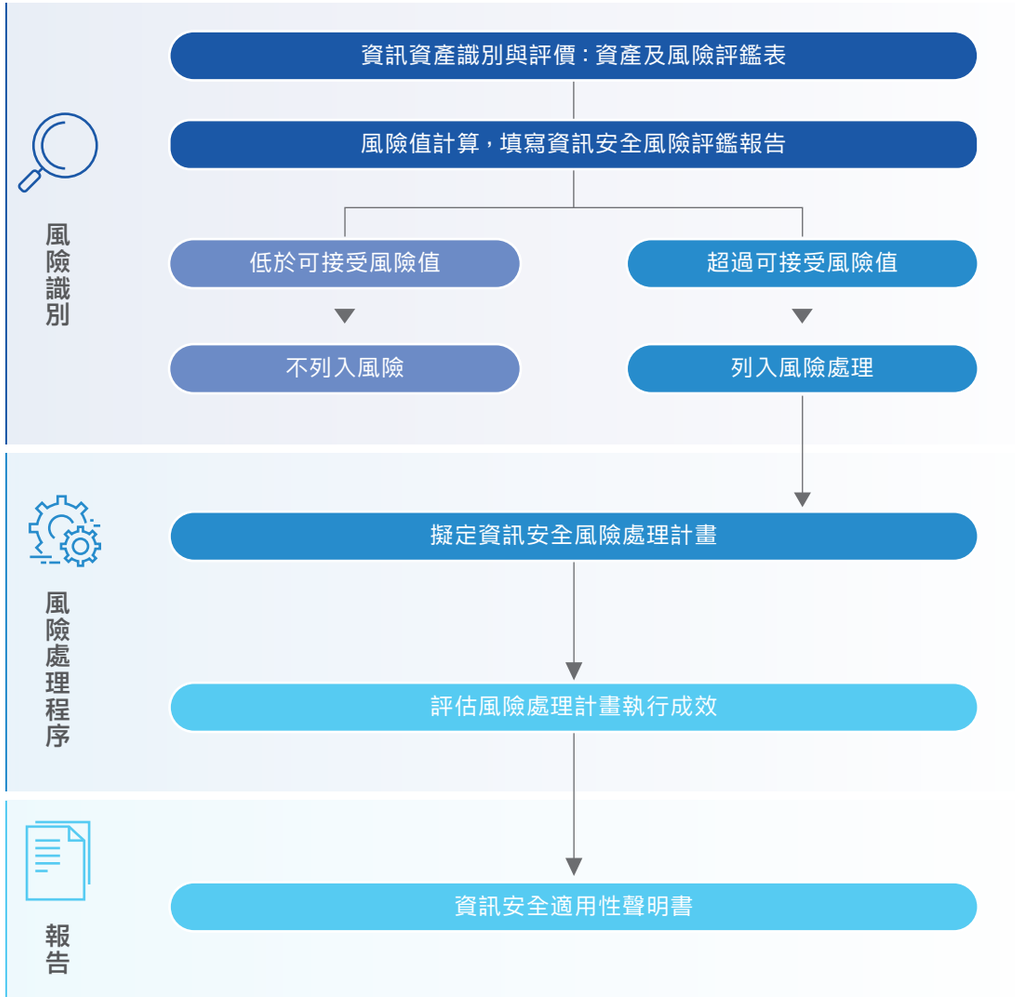
- 全面的資通安全文化建立
- 資通安全合規性與法規遵循
- 資安威脅情報分享與合作
- 資訊安全風險管理
- 持續性的資通安全教育和培訓
- IT 技術基礎設施的持續改進
- IT 災難恢復和業務持續性計劃

2024 年資安管理目標設定		執行情形
資訊安全風險管理	國際標準認證	取得 ISO 27001：2022 認證。
	資訊安全訓練	100% 新進員工均納入資安訓練對象。
	資訊安全宣導	每月發佈資安宣導，共 12 次，強化同仁資安意識。
	資安委員報告	每年召開 1 次
	個人電腦更新	每季定期更新電腦，更新率達 99%。
資訊安全稽核執行	社交工程演練	誤觸率 15% 以下，誤觸同仁參與資安意識提升講習。
	資安事件管理	無重大資安事件，持續確保資訊環境安全 。
	滲透測試	完成滲透測試演練及弱點修補。

■ 資訊安全委員會

資訊安全委員會(Information Security Committee)由總經理擔任召集人，下設「資訊安全應變中心」、「資訊安全執行小組」及「資訊安全稽核小組」。每年定期開會一次，審查公司資訊安全管理相關事宜及檢討資訊安全政策執行情形，並每年一次(2024 年 10 月 29 日)於董事會報告。

■ 資訊安全風險管理程序



■ 資訊安全事件管理程序

為確保當發生資安事件時能迅速控制事件損害情形，昇佳電子制定「資訊安全事件管理程序」，發現有可疑資訊安全事件時，應向「資訊安全執行小組」進行資訊安全事件通報。「資訊安全執行小組」應確認判定是否適切，如確定為資訊安全事故，需填寫「資訊安全事故報告單」，且近一步召集緊急處理小組進行後續處理。

01 STEP

識別與通報

發現有可疑資訊安全事件時，應向資訊安全執行小組進行資訊安全事件通報

02 STEP

評估

資訊安全執行小組應該認判定是否適切，如確定為資訊安全事故，並填寫資訊安全事故報告單

03 STEP

處理

由資訊安全執行小組召集緊急處理小組進行後續處理，若為最嚴重等級則進一步評估是否啟動營運持續計畫

04 STEP

報告與檢討

向管理層和相關利益者報告事件的詳細情況、後續行動和教訓，進行事件的詳細檢討，分析對策的有效性和改進空間

05 STEP

意識提升

定期進行資安培訓，提高員工對資安風險的認識和應對能力

■ 資訊安全管理具體方案

資安管理／控制項目	對應措施
資訊安全政策與教育訓練	● 資訊安全委員會討論後，呈報總經理核准公告資訊安全政策。 ● 透過員工教育訓練與 e-Learning、資安公告等提升同仁資安意識。
資訊分級與保護	● 依據資料安全管理規定，針對包含個人資料及客戶隱私等重要資訊進行權限控管機制建立。 ● 控管 USB 寫出／對外郵件自我稽核／檔案與目錄權限收斂等，並依據管理規定實作稽核機制。
系統與應用程式存取控制	● 雙因子認證強化存取控制。 ● 依據存取控制管理規定，簽核後開放系統權限。 ● 稽核重要資訊系統登入紀錄。
資訊紀錄的保護	● 依據資料安全管理規定，收攏與保存保護必要資訊紀錄。 ● 異地備份：針對關鍵服務，備份於台北辦公室，縮短復原時間。
網路安全管理	● 設置防火牆區隔內外網路，重點資訊區城進行連線與資料流控管，並定期檢視防火牆規則。
防範惡意碼電腦病毒防護	● 由閘口到端點建立完整的惡意碼防護機制。 ● 資安公告提升同仁資安意識。
資訊安全事故管理	● 依據資訊安全事件管理程序，建立處理程序。 ● 解析業界資訊安全事件，降低資訊安全事件發生可能性與衝擊性。
供應鏈資訊安全管理	● 依據供應商管理規範，確保供應商關係管理之安全性，並透過程序化之供應商關係管理安全控管機制，使供應商關係管理正常運作。

■ 執行成果

資訊安全報告 1 次	● 每年召開 ISO 27001 管理審查會議，其會議結果亦呈提報董事會。
資安認證 ISO 27001	● 2024 年 2 月取得 ISO/IEC 27001：2022 資訊安全管理系統認證。
教育訓練 100%	● 新進人員：100% 資安教育訓練。 ● 全體人員：針對全體員工進行 1 次資安教育訓練。
資訊安全宣導公告 12 次	● 定期資訊安全宣導公告：每月發佈資安宣導，共12次，強化同仁資安意識。
異地備份新增	● 新增異地備份位置。
災害復原演練 1 次	● 每年定期執行災害復原演練。
滲透演練 1 次	● 外部網站滲透演練：執行滲透演練，共 1 次。(滲透測試演練及弱點修補)。
社交工程演練 2 次	● 2024 年員工誤觸率 1.79%。
資訊安全稽核 2 次	● 定期資訊安全稽核內部與外部稽核。
資產及風險評鑑 1 次	● 每年定期執行資訊資產及風險評鑑。
電腦更新率達 99%	● 每季定期更新電腦。
雙因子驗證範疇擴增	● 雙因子驗證：關鍵服務增加雙因驗證。

■ 個人資料保護

昇佳電子重視合作夥伴之營業秘密，依循經濟部工業局「臺灣智慧財產管理制度(TIPS)」，將營業秘密列入公司智財管理標的，建立公司保密文件管理規範，制定文件標準與保密分級，對內針對保密文件進行資訊安全環境之建構，落實存取權限管控及擁有者之覆核機制，確保文件的存取與共享受到妥善治理與保護。昇佳電子取得 ISO 27001 國際資訊安全管理認證，於硬軟體設施、人員作業等各面向持續更新並落實嚴謹的資安措施，維護公司與各利害關係人重要資產之機密性。如發生個資外洩事件，由「資訊安全委員會」下之「資訊安全應變中心」、「資訊安全執行小組」及「資訊安全稽核小組」依據「資訊安全事件管理程序」立即啟動事件通報機制，並依照規範進行調查與處理，確保事件得到妥善處理，並在規定時間內完成報告。

昇佳電子為確保員工個人資料的隱私與安全，依據《個人資料保護法》建立「個人資料保護管理辦法」，嚴謹對待員工個資隱私安全之管理與防護措施。本辦法適用於所有公司員工，並由人力資源部門作為主要權責單位，負責相關政策的推動與執行，確保個人資料的收集、處理、使用及存儲皆符合法規要求，並落實安全保護機制。昇佳電子隱私權保護政策，請參閱**隱私權聲明**。

管理項目	內容
保密協議簽署	● 與員工簽訂聘僱契約書及個人資料使用同意書。 ● 與客戶及供應商簽訂相關業務之保密協議，避免員工、客戶或供應商等洩露營業秘密。
教育訓練	● 2024 年度針對在職員工進行「營業秘密保護基礎知識及管理制度介紹」線上訓練課程，課程總完訓人數達 199 人，課程總時數達 133 小時。
資安防護	● 釣魚郵件偵測並定期執行員工警覺性測試。 ● 演練勒索軟體攻擊。 ● 隱私與個資保護宣導。 ● 演練資訊系統災害復原計畫。