資訊安全管理

為確保落實資訊安全管理制度與資訊安全政策之推行，昇佳電子依據「資訊安全管理程序」管理，且透過系統性的管理框架，啟動與控制資訊安全的實施，且每年定期執行資安緊急應變之災難復原演練計畫 1 次，以確保資安有效性。

2021 年 11 月成立資訊安全委員會（Information Security Committee），由總經理擔任召集人，下設「資訊安全應變中心」與「資訊安全執行小組」，負責資訊安全管理、規畫、督導及推動執行，每年定期開會一次，審查資訊安全管理相關事宜及檢討資訊安全政策執行情形，且每年向董事會報告一次。此外，昇佳電子自 2022 年加入台灣電腦網路危機處理暨協調中心（Taiwan Computer Emergency Response Team / Coordination Center，TWCERT / CC），掌握可能之資安事件或漏洞，及早預防、改善與管理。

2023 年導入 ISO 27001，已於 2024 年第一季取得第三方驗證，以強化與制定資訊安全事件之管理程序。2023 年昇佳電子無發生重大資安事件。

2023 年資安管理目標設定		執行情形
資訊安全風險管理	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	發佈 5 次資安宣導，強化同仁資安意識。
	資安委員報告	每年召開 1 次，ISO 27001 之導入新增 16 條資訊安全政策。
資訊安全稽核執行	社交工程演練	全體員工，26.67% 同仁參與資安意識提升講習。
	資安事件處理	無資安事件，持續稽核，確保環境安全。
	弱點掃描	外部執行弱點掃描，減少 46% 資訊安全修補。

目標時程	短期目標	中期目標	長期目標
規畫方向	• 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。	• 建立資通安全威脅偵測與管理平台（SOC），並滿足以下目標 1. 高可視性 2. 蒐集各系統來源數據 3. 半自動化漏洞修補 4. 網路終端設備管理與流量異常監控	• 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。 1. 全面的資通安全文化建立 2. 資通安全合規性與法規遵循 3. 資安威脅情報分享與合作 4. 資訊安全風險管理 5. 持續性的資通安全教育和培訓 6. IT 技術基礎設施的持續改進 7. IT 災難恢復和業務持續性計劃

資訊安全委員會

組織架構與職掌

制定公司資訊安全政策，負責資訊安全管理制度相關事項之決議執行。

資訊安全委員會

負責評估資訊安全管理制度之執行情形。

資訊安全稽核小組

資訊安全應變中心

針對非預期資訊安全事件，建立相對應的解決辦法，蒐集軌跡與事件鑑定，「風險改善計畫」彙整與控管，持續追蹤至改善完成。

資訊安全執行小組

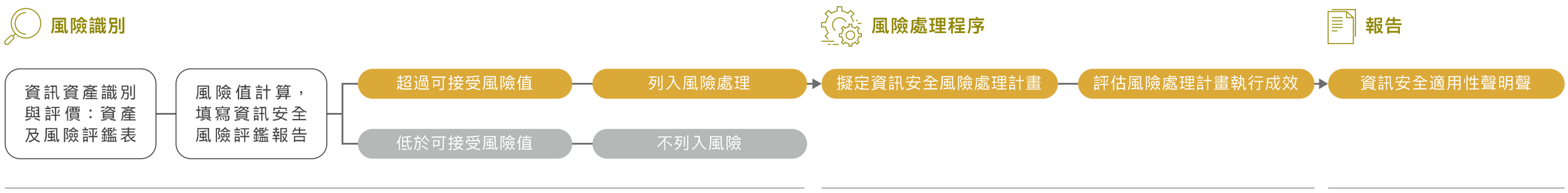
負責規畫及執行各項資訊安全作業，提供資訊安全宣導、外部協力廠商資安稽核事宜。

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，並填寫「資訊安全事故報告單」，由「資訊安全執行小組」召集緊急處理小組進行後續處理。

01	**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	**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	**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	**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	**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

資訊安全風險管理程序



資訊安全管理具體方案

資安管理／控制項	風險說明	對應措施	預期效益
資訊安全政策與教育訓練	資訊安全政策是否由管理階層制定、核准、公佈並傳達給所有員工，並以確保其持續的適用性與有效性。	• 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。	資安政策的有效性，使同仁提升資安意識。
資訊分級與保護	資訊應依未經授權的揭露或法律要求、價值、重要性與敏感度加以分級，並應依照分類，實作保護程序。	• 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。	確保包含個人資料及客戶隱私等機密資訊的合理保護措施。
系統與應用程式存取控制	根據存取控制政策，限制資訊與應用系統功能之存取，並由安全登入程序控制系統與應用程式的存取。	• 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。	依據授權原則與核准程序，避免不當存取。
資訊紀錄的保護	紀錄應依據法令、法規、契約及營運要求，加以保護，以免於遺失、毀損、偽造、未授權存取。	• 依據資料安全管理規定，收攏與保存保護必要資訊紀錄。	確保紀錄的證據能力，符合法規需求。

資安管理／控制項	風險說明	對應措施	預期效益
網路安全管理	網路是否適切地加以管理與控制，以保護系統與應用程式的資訊。	• 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。	避免不當存取與資料洩漏。
防範惡意碼電腦病毒防護	是否建立防範惡意碼偵測、預防及復原控制措施，並結合適切的使用者認知。	• 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	強化網路存取與資訊服務安全。
資訊安全事故管理	是否建立管理責任與程序對應，以確保對資訊安全事故做出回應。並藉由分析資訊安全事件降低發生可能性與衝擊性。	• 依據資訊安全事件管理程序，建立處理程序。 • 並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。	強化資安事件處理程序，降低發生可能性與對於營運的衝擊。
供應鏈資訊安全管理	是否建立供應鏈資訊安全管理做法，提升整體產業鏈資訊安全。	• 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。	強化資安事件處理程序，降低來自供應鏈資安事件對於營運的衝擊。

資訊安全教育訓練

- **新進人員資安教育訓練：**

  2023 年新進人員 100% 資安教育訓練。

- **全體人員資安教育訓練：**

  2023 年針對全體員工進行 1 次資安教育訓練。

- **定期資訊安全宣導公告：**

  2023 年宣導內容如電子郵件社交攻擊等 5 次。

- **進行社交工程演練，強化同仁資安意識：**

  1. 2023 年進行 2 次社交工程演練，員工誤觸率 26.67%（2022 年 37%），原訂誤觸率目標設定為 20%，未達目標主因為員工資安意識薄弱，需強化宣導機制，規劃資安宣導最少每季一次。
  2. 課後問卷：平均分數 99 分。