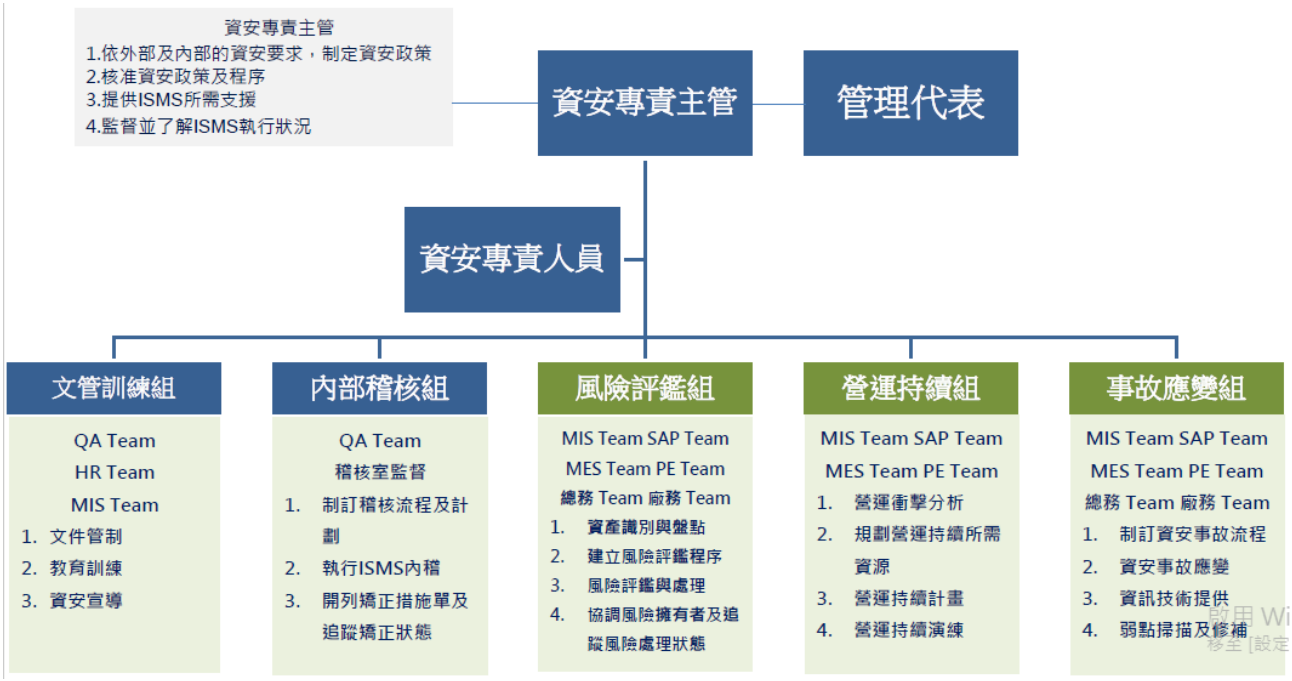
艾訊資通安全管理

目的

艾訊股份有限公司(以下簡稱本公司)為強化資通安全管理，提昇資通安全管理流程之嚴謹度與安全性，依 ISO/IEC 27001:2022 資訊安全管理條文的要求及精神，以持續改善 P.D.C.A. 循環流程管理模式，建立資訊的機密性，完整性及可用性，避免因資通安全問題造成公司及客戶營運上不必要的損失，確保企業持續營運的目的。

資通安全風險管理架構

- 本公司以資訊單位為資通安全風險管理權責單位，設置資安專責主管一名及資安專責人員一名，其它資安組織成員共計 17 名。負責訂定、規劃及執行資通安全風險管理政策，由資安專責主管核定，同時規劃及執行資通安全政策推動與落實，並定期向董事會報告公司資通安全治理概況。
- 本公司稽核室為資通安全管理之督導單位，負責督導資通安全管理執行狀況，若有查核發現缺失，即要求受查單位提出相關改善計畫與具體作為，且定期追蹤改善成效，以降低資通安全風險。
- 資安管理委員會組織架構



資訊安全政策

艾訊為工業電腦領域的領先設計者和製造商，並依據工業物聯網 (Industrial Internet of Things, IIoT) 與工業 4.0 發展趨勢，積極投入工廠自動化、智慧交通，與智慧能源等應用領域。以培植自身嵌入式電腦技術能力及推動品牌核心價值，朝向獲利較高的產業發展，提供工業電腦領域服務給全球客戶並與之建立長期互惠夥伴關係之際，願意積極深化資訊安全與機密資訊保護機制，以維護艾訊的市場競爭力及保障客戶與合作夥伴之利益，我們的資訊安全政策是：

「資安防護不中斷、風險控管要持續、企業營運有保障」

為提升產品安全品質，落實及持續更新嚴謹的資安措施並建立完善的產品安全開發管控機制，以預防及降低外部資安風險，例如：建置先進的病毒掃描工具，以防止廠區所使用之資訊系統遭受病毒感染；強化網路防火牆與網路控管以防止電腦病毒跨廠區擴散；在公司電腦上建置防毒措施及先進的惡意軟體偵測解決方案；改善資安部署時間以強化資料中心安全。瞭解產品安全政策的目標，以降低產品開發生命週期非經授權之存取、修改產品的風險或遭受網路攻擊事件，並建立與定期檢討資安績效指標；導入新技術加強資料保護；加強釣魚郵件偵測並定期執行員工警覺性測試；建立一個整合的自動化資安維運平台並強化資安事件偵測與處理自動化；持續演練資安攻擊之處理程序；委託外部專家執行資安評鑑等。每年持續進行的資安執行重點如下：

1. 網路安全控管 Network Security Management
2. 資產管理及資料安全 Asset Management and Data Security
3. 存取控制管理 Access Control Management
4. 電腦維運安全管理 Computer Operations Security Management
5. 作業安全管理 Operational Safety Management
6. 資訊系統獲取、開發及維護管理
   Information System Acquisition, Development, and Maintenance Management
7. 資安事件管理 Information Security Event Management
8. 供應商安全管理 Supplier Security Management
9. 人員資安管理與教育宣導
   Personnel Information Security Management and Education Advocacy
10. 變更與組態管理 Change and Configuration Management
11. 雲端服務安全管理 Cloud Service Security Management
12. 產品安全開發流程控管 Secure Software Development Life Cycle

具體管理方案

- 資通安全事件係指系統、服務或網路狀態經鑑別而顯示可能有違反資通安全政策或保護措施失效之狀態發生，影響資安系統機能運作，構成資通安全政策之威脅。針對風險管理，本公司掌握三個面向對應及預防資安風險事件的發生：

預防資安事件(事前)	處理資安事件(事中)	調查資安事件(事後)
• 防止入侵 • 防毒 • 防意外(備份) • 防外洩	• 防止災害擴大 • 停止損失 • 最短時間復原(還原)	• 調閱 • 查核 • 檢討 • 持續改善(P.D.C.A.) • 風險控制，防止再度發生

- 資通安全風險管理

項目	說明	容忍風險	因應對策	預計成果	容忍剩餘風險
資通安全風險	1. 駭客入侵 2. 資料外洩 3. 電腦中毒	否	1.防火牆，防毒軟體，定期更新病毒碼並進行掃毒。 2.定期 Windows Update。 3.AD 密碼定期更換。 4.M365 及 SSL VPN 使用 MFA 手機多因素驗證。 5.OpenDNS 網頁過濾。 6.使用 M365 雲端服務，即使被駭客加密亦可回溯加密前檔案。	降低發生機率及降低影響	是
資訊服務中斷風險	因人為或意外災害導致公司主機、網路或其他資訊相關設備無法使用	否	1.機房之緊急 UPS 於斷電時約可供應主機約 4 小時之電力。 2.使用 M365 雲端服務，即使伺服器設備損壞，員工仍可正常收發 EMAIL 及存取雲端檔案。 3.伺服器依備份 321 原則執行備份。 4.異地備份。 5.雲端備份。	降低發生機率及降低影響	是

- 資通安全所面臨的挑戰，如 ATP 進階持續性攻擊、DDoS 攻擊、勒索軟體、社交工程攻擊、竊取資訊等資通安全議題，本公司已採取以下策略：
  1. 提昇 IT 基礎架構

(1) 汰換伺服器主機，核心伺服器更新為 Dell VxRail 伺服器，作業系統全面升級 Windows Server 。
(2) 提昇對外網路頻寬，更新高速頻寬管理器，解決對外頻寬不足的情形。
(3) 專線升級以改善公司廠區專線品質。
(4) 建立異地備份專線及機制：將廠區資料備份至第三地。
(5) RD Lab 測試設備環境隔離。
(6) 提昇端點安全，更換防護更全面的防毒軟體，提供整合的修補程式，透過漏洞分析及修復程式列出優先順序，並提供修補，自動偵測行為入侵模式，並由防毒軟體雲端防護檢測並自動偵測多個來源的威脅。
(7) 區域網路升級 PA 及 Fortinet 內外部防火牆，無線網路升級 Cisco 方案，提昇無線存取效能及安全性。

2. 強化備份機制，重要伺服器異地備份外再備份至雲端。
3. 加強資通安全檢核機制(ISMS)。
4. 2023 年 8 月已開始導入 ISO 27001:2022 資訊安全管理系統，提昇 IT 基礎設施及各項機制，不論是伺服器升級，端點防護，網路對外頻寬，備份機制等，持續改善並提升資通安全，已於 2024 年第一季取得 ISO27001:2022 證照。

投入資通安全管理之資源

- 升級 M365 雲端協同作業並導入 ATP 進階威脅防護，提昇企業基礎架構安全性。
- 導入微軟金級資通安全 SI-自由系統，持續改善企業資通安全。
- 導入微軟 Microsoft Defender for Identity 及 Microsoft Defender for Endpoint，全面提昇 AD 帳號管理及使用者端點安全性。
- 導入 Azure 雲端備份，將重要系統本地備份後再抄寫至異地機房及雲端。
- 定期社交工程釣魚郵件演練，提昇員工資安意識。112 年進行的年度社交工程演練，點擊率為 38.86%，113 年度社交工程演練點擊率降至 18.02%，相較於 112 年點擊率大幅下降，顯見同仁資安意識提昇，每年資安教育訓練效果顯著，提昇員工資安意識確保企業持續營運。
- 定期資通安全教育訓練，落實員工資安知識。113 年資通安全教育訓練為社交工程演練，同仁只要有點選連結，就會要求上資通安全教育訓練及測驗課程，預計每年會定期執行一次。
- 導入 ISO27001:2022，並成立資安管理委員會，資安專責主管一名， 資安專責人員一名，其它資安成員 15 名，共計 17 名。
- 進行資安教育訓練，包含 CISSP 課程 40 小時，ISO27001 專業資安課程 6 堂。
- 召開資通安全會議，包含 ISO27001 資通安全討論會議 6 小時。
- 投入資安之資源：已升級及汰換外部防火牆，伺服器端內部防火牆，SIP 區域網路管理軟體，升級安全之無線網路方案。
- 加入 CERT 電腦緊急應變小組 CSIRT 電腦資安事件應變小組組織。

- 定期向董事會報告資通安全執行情形。
- 依『公開發行公司建立內部控制制度處理準則』第九條電腦化資訊系統之相關內部作業規定，以資訊單位為權責單位負責訂定資通安全政策、規劃及執行資通安全政策推動與落實，並定期向董事會報告公司資通治理概況。資通安全治理執行情形已由資安專責主管於113年10月29日向董事會報告。