資訊安全管理政策

資訊安全政策

依「公開發行公司建立內部控制度處理準則」第九條「電腦化資訊系統處理」之規定制定相關內部作業規定，以降低日新月異的資訊科技應用及環境變異所帶來未知的資安風險威脅，達方基礎資訊安全政策管控共有8項。

資訊安全說明：

1. 內外網路存取需通過防火牆 / 病毒牆 / 入侵防禦系統檢查。
2. 所有資訊設備一律安裝防毒 / 防後門軟體。
3. 每 3 個月定期更換使用者密碼，且須符合密碼複雜性原則。
4. 存取任何系統皆需申請帳號並有權限限制的開放存取，離職後帳號刪除。
5. 機密資料調閱，檔案全程加密處理。
6. 所有企業流程需經由電子簽核核准後方能生效。
7. 所有 End-point（用戶終端）資訊設備回收 Admin（管理員）權限，並安裝資產管理軟件和端點安全防護軟體。
8. 定期內外部資訊安全稽核。

資訊安全風險管理架構

本公司於 110 年第四季成立資訊安全委員會，並設立資訊安全主管，定期召開資訊安全審查會議，112 年共計召開 2 次。除資安委員外，編列負責資通安全管理之同仁，與委員會共同管控資訊安全風險並推動各項資安政策、制定及導入資安制度及資訊安全風險稽核等工作。委員會組織相關管理架構劃分如下：

(1)管理單位：資訊安全委員會設定主任委員一名，並由總經理擔任。委員若干名，主要由副總級擔任。召集人由資訊部主管擔任，主要負責資訊安全委員會組織管理、召集。下設常態編組有：

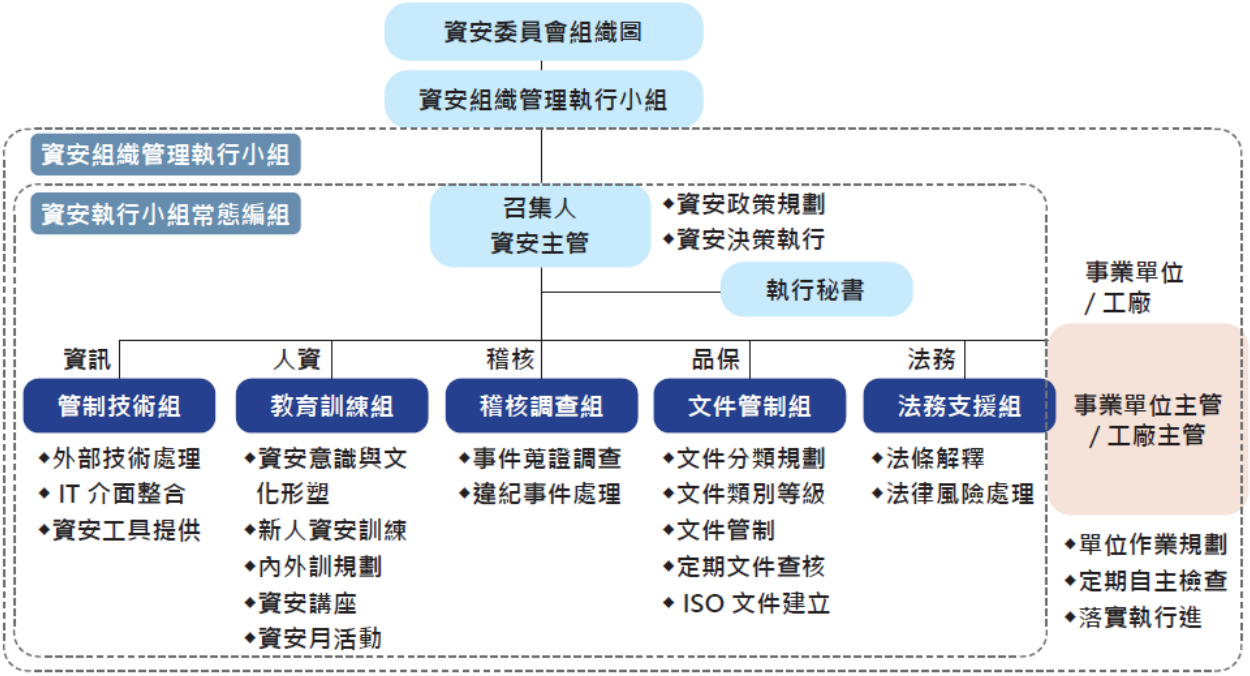
①管制技術組：由資訊部擔任，負責資訊安全技術工作、介面整合及資訊安全提供解決方案。

②教育訓練組：由人事部擔任，負責提升資訊安全風險意識、資訊安全風險訓練及講座舉行。

③稽核調查組：由稽核部擔任，負責資訊安全風險稽核，異常蒐証、調查及處理。

④文件管制組：由品質部擔任，負責包含機密文件分類、等級定義、管制及查核。

(2)其它單位：涵蓋公司所有事業單位及工廠，主要職責有與資安相關的日常作業規劃、定期進行資訊安全風險自我檢查及落實資安風險改善項目執行。



資訊安全具體管理方案及投入資通安全管理之資源

公司為強化整體資訊安全，資訊安全負責單位除每月進行資安會議，並推動相關資訊安全強化政策及投入之資源如下：

投入資源	110 年	111 年	112 年
資安專案投入金額	300 萬	1,500 萬	1,500 萬
資安專責人力配置	資安主管：1 人 專責人員：1 人	資安主管：1 人 專責人員：1 人	資安主管：1 人 專責人員：1 人

(1)重大基礎資訊安全系統建設(97 年~112 年)

- 機房環境安全

①機房自動環保氣體消防設施建置。

②機房雙迴路UPS供電系統。

③機房備援空調系統建置。

④機房全景攝像監控系統建置。

⑤機房24小時環控監控(溫度/電力/漏水/空調/門禁/消防等)和即時簡訊發報系統建置。

- 系統資訊安全

①垃圾郵件防護及郵件進出記錄備份系統建置。

②ERP歷史資料虛擬化導入，長期保存系統和資料安全。

③透過外部弱點掃描，補強系統漏洞。

④改善外部系統成為加密傳輸，降低資訊安全風險。

- 網路資訊安全

①防火牆升級功能IPS入侵偵測系統防護。

②專線線路雙備援自動切換機制系統導入。

③全公司網路導入禁止任意非法網路設備接入內網系統。

- 主機資訊安全

①虛擬化傳統架構升級為高容錯多複本超融合架構，以強化軟硬體的資訊安全高可用性。

②伺服器全面監控和即時簡訊告警系統導入。

③伺服器漏洞定期追蹤處理。

④全公司資訊設備導入端點防護禁止任意非授權軟體安裝和惡意木馬程式植入。

(2)資訊安全中長期發展規劃(110 年~113 年)

- 資訊安全制度

①導入ISO 27001資訊安全管理系統。透過ISO 27001資訊安全管理系統的定期驗證，以落實資訊安全政策、保護客戶資料及公司智慧產出、強化資訊安全事件應變能力及達成資訊安全政策衡量指標，111年10月取得ISO 27001認證，112年擴展驗證範圍至中國廠區，並於112年9月取得認證，證書效期至114年10月，未來規劃113年進行ISO 27001 2022改版。

②不定期進行社交工程演練，提升同仁資訊安全意識，112年員工社交工程信件點擊率<7.4%，符合策略目標值，並有逐年下降趨勢。

- 資訊安全預警

①導入相關資安預警設備和機制，將內部安全風險黑箱可視化。並結合外部資安情資和分析，針對外部駭客入侵行為能夠提前感知，而能先進行相關反制作業。保護企業內部資料和系統的安全。

②定期進行內外部弱點掃描，針對漏洞進行預防修補，以降低資訊全安風險曝露。

③外到內滲透測試演練，進行深入的漏洞測試與分析，找出設備及系統的潛在風險，提高安全性。

- 資訊安全防護

①導入MFA雙因子驗證，透過兩次驗證程序檢視使用者合法性，以杜絕未授權使用者獲取公司內部資訊或進行破壞活動。

②導入SIEM日誌管理，收集系統日誌集中保存，利於未來資訊安全事件追蹤、釐清及預防。

③導入PAM特權帳號管理，避免內部特權用戶濫用遭外部竊取，集中管理並定期稽核，降低入侵風險。

④導入營業祕密資料保護，避免機密資料及關鍵技術外洩，保障公司核心競爭力。

⑤導入EDR端點偵測與回應，強化關鍵主機弱點風險管控，可疑事件自動回應。

⑥導入使用者上網行為管控，透過異常行為分析，找出資安潛在風險。

- 員工資訊安全宣導及訓練

①公司內部網站不定期宣導資訊安全知識。

②不定期以E-Mail發送資訊安全公告。

③對新進同仁做資訊安全宣導。

④定期全公司資安教育訓練，每年兩次資安通識線上課程為全體員工必修課，涵蓋資安政策宣導、基礎通識、進階資安及個人資料保護，以人人資安為宗旨。

⑤資通安全人員積極參與外部研討會，安排超過80小時資安進修課程，如：CYBERSEC台灣資安大會、微軟安全性會議、數位轉型企業資訊安全研討會、TWCERT台灣資安通報年會及資安情資蒐集與分析實務，並持續計畫取得國際資安證照，如：CompTIA security+ 國際網路資安認證、

ISO 27001：2022資訊安全管理系統主導稽核員及CISM 國際資訊安全經理人等，以提升專業職能並掌握關注議題。

培訓對象	資安專責	資訊單位	全體員工
成果指標	●參與 80 小時以上的外部研討會及專業訓練課程 ●積極取得國際專業證照	全體完成 ISO 27001 體制稽核員培訓課程	●新進同仁資安宣導 ●內部網站知識宣達 ●全體資訊安全通告 ●每年兩次資通安全線上必修課程

112年資訊安全風險管理執行情形已於同年11月向董事會報告，執行情形報告內容如下：

一、管理面：

(1)每年遵循 ISO 27001-2013 資安體系之管理制度執行內稽、管審及驗證工作。

(2)111/10 總部及台南廠取得 ISO 27001-2013 ISMS(資訊安全管理系統)的認證，112/10 取得大陸 3 廠區 ISO 27001-2013 ISMS 認證。

二、技術面：

(1)111 年起總部、台南廠及大陸淮安廠執行資安監控，112 年推廣至蘇州廠及重慶廠。包括網路惡意程式檢視、使用者端電腦惡意活動檢視、伺服器端電腦惡意活動檢視等內部網路的入侵偵測資安活動監控。

(2)每月執行外部弱點掃描，每月對弱點進行改善；112/10 完成外部系統滲透測試檢測針對弱點進行改善。

(3)公司已建置防毒軟體、網路防火牆、郵件過濾規則、入侵偵測及防護等機制。

三、認知及訓練面：

(1)資安專業人員在今年完成 80 小時資安專業練課程。

(2)基礎架構及網路管理人員接受 ISO 27001 資安體系教育訓練。

(3)112/3 及 112/10 執行全體員工的資安通識教育訓練。

(4)112/6 完成全公司人員執行社交工程演練，對於上當同仁已執行調訓，強化資安意識。

四、未來計劃：

(1)遵循 ISO 27001-2022 資安體系的管理制度持續執行內稽、管審及驗證工作。

(2)每年評鑑公司各項資訊資產的風險值，針對高風險資產持續執行改善工作，降低資安風險。

(3)增加執行 Source code 資安掃描，以找出應用程式的弱點進行修補；強化資安健檢工作。