資訊安全

本公司為維護競爭優勢與寶貴的智慧財產，成立「資訊安全委員會」，並訂定資訊安全管理政策，以強化本公司資訊安全管理，確保資料、系統、設備及網路安全，保障公司與全體員工之權益。透過各類資訊安全活動，以有效保護公司智慧財產，強化資安意識。為確保相關資訊系統的運作風險得以有效控制，資訊安全委員會每年至少召開一次管理審查會議。

董事會每季聽取經營團隊的營運報告(包含 ESG、資訊安全等)，並經常檢視策略的進展，需要時提供必要指導。

▼資訊安全管理組織

本公司設立「資訊安全委員會」及「資訊安全執行小組」以維護並加強本公司之資訊安全。由「資訊安全委員會」核定「資訊安全執行小組」所擬訂之資訊安全政策，並定期召開管理審查會議，或於組織有重大變更時（如組織調整、業務重大異動等）重新評估本政策之適用性。

•資訊安全委員會：

由本公司總經理擔任主任委員，資訊部最高主管擔任召集人，各單位一級主管及部級主管擔任委員，如因職務調動應即刻指派遞補人員並辦理交接。

•資訊安全執行小組：

由召集人指派資訊安全專責主管一名與資訊安全專責人員一名，負責規劃及執行各項資訊安全作業，包含資訊安全預防及事件處理。

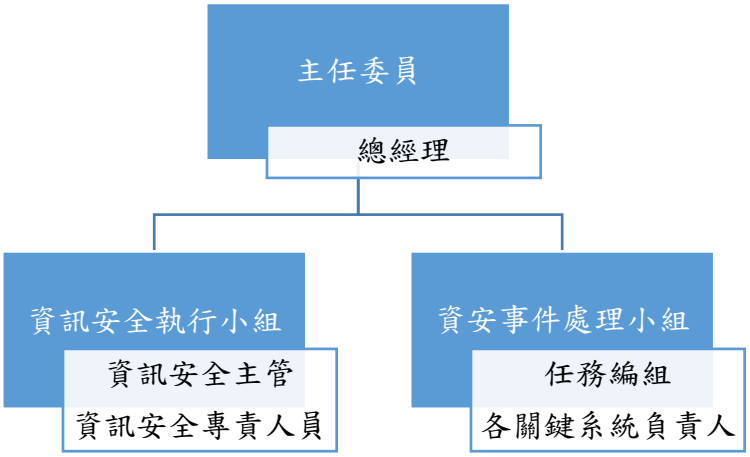
•資安事件處理小組：

資安事件處理小組為任務編組，當發生重大資安事件時，由資訊安全主管召集指派各關鍵資訊系統負責人員組成。

•稽核室:

本公司稽核室為內部資安監督查核單位，若查核發現缺失，立即要求相關單位提出改善計畫並追蹤改善成效，並定期對董事會進行稽核報告。

▼資訊安全委員會架構



▼資訊安全管理政策

1. 改善公司內部各項資訊安全管理機制，資訊化作業得以持續不間斷運作，維持內部制度管理之有效性，提升資訊服務品質。
2. 確保處理與利用之所有資訊的機密性、完整性與正確性。
3. 進行資安事件應變演練及透過各類資訊安全教育訓練課程的宣導，提升同仁資訊安全意識。

▼資訊安全管理具體方案

本公司目前的管理方式已能有效防護資訊安全，相關具體執行措施如下：

項目	具體管理方案
防火牆防護	防火牆設定連線規則，預設關閉所有電腦對外連線。 如有特殊連線需求需經資訊部主管核准才能開放。
使用者上網控管機制	使用自動網站防護系統控管使用者上網行為。 自動過濾使用者上網可能連結到有木馬病毒、勒索病毒或惡意程式的網站。 未經核准禁止使用即時通訊軟體、網路硬碟、檔案傳輸等網路服務。
防毒軟體	使用多種防毒軟體，分散新病毒中毒機會。
USB 磁碟存取管制	使用者電腦預設禁止使用 USB 裝置，因公務需求需使用 USB 裝置，需經部門主管核准後始得使用，資訊部做事後稽核。
作業系統更新	有自動更新系統統一控管，自動派送更新與安裝到公司電腦。 資訊部監控因故未更新者，由資訊部協助更新。 機台設備附屬電腦由設備部工程師負責更新。
郵件安全管控	有自動郵件掃描威脅防護，在使用者接收郵件之前，事先防範不安全的附件檔案、釣魚郵件、垃圾郵件，及擴大防止惡意連結的保護範圍。 個人電腦接收郵件後，防毒軟體也會掃描是否包含不安全的附件檔案。
使用者郵件收發管控	可統計使用者外部郵件收發件數與明細，監控異常收發狀況，避免機密資料外洩。
網站防護機制	網站有防火牆裝置阻擋外部網路攻擊。
高可用性機制	各項重要資訊系統，皆有建立高可用性機制。可在系統故障時於最短時間內恢復系統運作。
資料備份機制	重要資訊系統資料庫皆設定每日完整備份。
資訊系統備份機制	資訊系統程式每日完整備份一次。
異地存放	伺服器與各項資訊系統備份檔，分開存放於不同廠的資訊機房。
重要檔案上傳伺服器	公司內各部門重要檔案上傳伺服器存放，由資訊部統一備份保存。
資訊機房檢查紀錄表	檢查紀錄表紀錄機房溫溼度、資料備份、異地備份移送等紀錄。
資安意識培養	不定期進行資安宣導教育訓練。 不定期資安新聞分享。 每年進行一次社交工程演練。

▼投入資通安全管理之資源

本公司截至 2023 年 12 月底，投入資通安全管理之費用為 NT 8,236 仟元。執行內容包含:資訊安全架構檢視及改善;網路設備、伺服器及終端機等設備檢測;網路活動檢視;網站安全檢測;資安防護檢測…等)

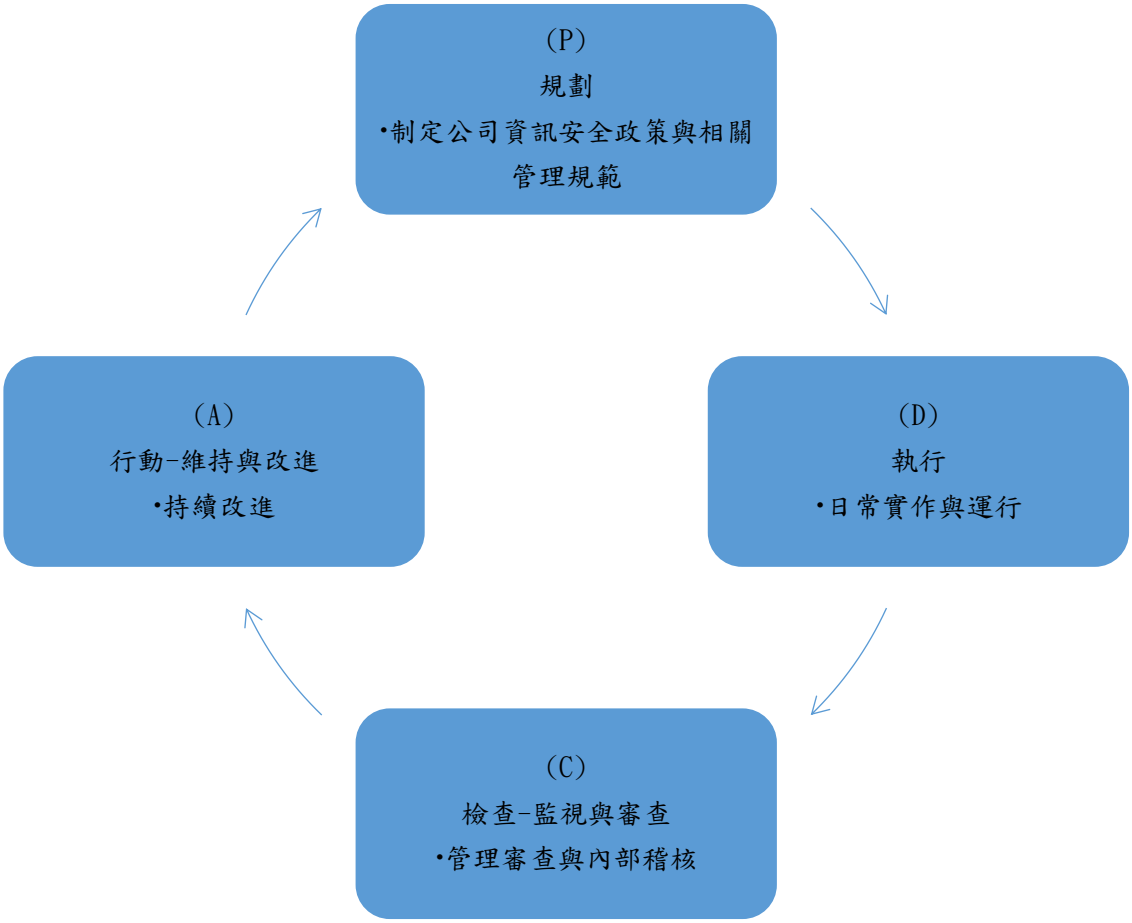
本公司也持續提升員工資安素養，除不定期發送資安宣導與對員工進行資訊安全教育及訓練，促使員工瞭解資訊安全的重要性，並促其遵守資訊安全規定。
截至 2023 年 9 月底資安外部訓練時數共計 16 小時；2023 年 2 月舉辦「資訊安全宣導-釣魚詐騙郵件」內部教育訓練，共 810 人次，訓練時數為 810 小時。

社交工程演練計畫：
本公司於 2023 下半年度針對 568 位同仁的 E-Mail Address 舉行社交工程演練，有點擊釣魚網站連結&輸入資料同仁，將會持續安排進行線上資安意識教育訓練課程。

▼資通安全風險與因應措施

1. 資訊安全持續精進及管理機制

本公司資安管理組織組織運作模式-採 PDCA 循環式管理，確保可靠度目標之達成且持續改善。透過定期辦理內部資安稽核，並就發現事項擬定改善措施，且定期追蹤改善情形。



2.科技改變(包括資通安全風險)及產業變化對公司財務業務之影響及因應措施:

本公司已建立全面的網路與電腦相關資安防護措施，每年皆投入固定支出於網路安全、裝置安全、應用程式安全與資料安全保護技術強化。

除持續檢視和評估資訊安全規章及程序，並針對核心業務及核心資通系統鑑別其可能遭遇之資安風險，執行多項對應之資通安全管理面或技術面控制措施，(詳參: 資通安全具體管理方案及投入資通安全管理之資源)，確保資通安全運作之適切性及有效性。

於執行公司所制定的所有資安政策與程序，均能落實執行並與時俱進，在確保公司資訊與資產之機密性、完整性與持續可行性，風險評估之結果為良好，故近年本公司並無因資安事件而造成公司不利之影響與相關之營運風險。

▼重大資通安全事件

因資訊安全管理的落實,近年我們並未發生重大資安事件,亦無因資安遭受相關主管機關裁罰。此外，本公司利用個人資料皆限於特定目的範圍內。近年亦無接獲主管機管投訴之案件；亦無侵犯供應商、客戶或相關利害關係人之隱私或遺失供應商、客戶或相關利害關係人資料的投訴。

▼客戶隱私權與資安防護

本公司深知隱私的重要性，並致力於確保尊重和保護客戶的隱私和機密。

針對資訊安全，本公司則訂有「公司機密資料、資訊管理辦法」等資安管理相關規範，針對機密文件的保護以權限限制，確實保障人員資料隱私與客戶權益，降低公司資訊不當外洩之風險。

本公司訂有「道德行為準則」，從業人員皆與公司簽訂「勞動契約保密約款」，員工就職務上所知悉之事項或機密資訊，應謹慎管理，避免員工個人行為因素外洩機密。