聚賢研發股份有限公司

資訊安全管理

在當今數位化時代，資訊安全已成為企業營運中不可或缺的一環，為保障資訊完整性並防範潛在風險，本公司建構一套全面的資訊安全管理系統，涵蓋數據加密、存取控制、監控系統、災難恢復計劃等多個層面，確保資訊在儲存與傳輸過程中均受到妥善保護。此外，聚賢持續透過內部教育訓練與政策更新，強化全體員工對資訊安全的理解與遵循，不僅保障客戶資訊安全，更有效降低人為疏失風險。

重大主題	**資訊安全**
重大主題意義	戰爭與全球不穩定因素加劇了駭客攻擊風險，對企業的經濟、環境與人群均可能造成深遠影響。在此情況下，強化資訊安全防護已成為企業不可忽視的任務，不僅可防止財務損失與營運中斷，更應納入環境保護與人權責任等永續發展考量。資訊安全的成熟度不僅關乎企業競爭力與穩定性，更在保護環境、保障隱私與促進社會責任方面扮演關鍵角色，已成為現代企業邁向永續發展的重要基石。
政策／承諾	聚賢雖尚未成立跨部門資訊安全委員會，目前由營運管理部兼任資訊安全相關事務，並於 2024 年 3 月 29 日經董事會決議通過設置資訊安全主管。工作範圍涵蓋電腦資訊、實體環境、產品資安以及法規遵循等多方面的議題。公司已採取多項資安管理措施，如建置資料保護機制、定期更新防毒軟體、進行風險評估，以及落實施行個人資料保護及資訊安全教育訓練等，並於每年度檢視設備狀況，適時汰換老舊設備，以預防潛在風險並維持資訊系統效能與穩定性。
目標	**短期：** • 每年至少一次落實公司內部同仁對於資訊安全的認知 **中長期：** • 每年持續宣導，確保同仁具有資訊安全意識 • 加強公司資訊安全管理並符合合作夥伴間的資訊安全協定，其中包含資安政策，資安設備
行動辦法	每年度公司會舉辦大型活動進行資訊安全宣導，並於每年 7 月和 12 月進行釣魚信件演練，確保同仁具備防範意識。在年度資訊安全稽核中，會檢視員工的權限是否符合當前職務需求，並遵循最小權限原則，同時檢查是否有員工瀏覽不良網站或下載含有威脅的檔案，以確保公司資料不會外洩。

2024 年實際績效	• 持續進行資訊安全人員培訓 • 設置「電腦化資訊系統作業辦法」與「個人資料保護作業辦法」，規範員工個人與客戶隱私之資訊安全 • 定期維護防火牆與備份裝置 • 全面評估資安風險定期辦理系統弱點掃描、網站安全檢測、滲透測試、防火牆規則檢視等作業 • 提升人員資安意識持續為同仁辦理資安宣導課程及社交工程演練，提升同仁資安意識，並控管業務單位的電腦對於 USB 及藍芽之使用，以降低人為之資安風險 • 新增 L2 與 L3 交換器，並對防火牆設備進行全面更新 • 強化資料備份，並對於重要資料庫欄位採加密處理 • 導入 Active Directory 網域服務，確保所有電腦設備皆納入控管範圍，加強結構化資料存取控制
申訴機制/溝通管道	• 員工意見回饋平台 • 於本公司網站設置聯絡信箱，提供利害關係人溝通。請至聚賢官網：https://www.geniideas.com.tw/about?siteRevision=488

資訊安全管理政策

聚賢秉持誠信原則，致力於嚴格保護客戶隱私，制定「內部重大資訊保密作業程序」與「個人資料保護作業辦法」，並要求員工於入職時簽署保密協議，以及進行資訊安全宣導，強調不得隨意洩露個人或客戶隱私資訊，落實資訊安全責任。

為建構全面性的資訊安全防護機制，公司從制度面、技術面與管理面同步推動相關政策與措施，並依據實際營運需求與風險評估結果，強化各項安全控管措施，確保資訊安全管理貫徹至各項營運場域與日常工作中。因應科技廠區相關規範，所有具備拍照、錄影、錄音等功能之電子設備禁止攜入廠區。為確保作業聯繫不中斷，公司統一配發無拍攝功能之簡易型手機予現場同仁使用，以兼顧資訊安全與溝通效率；以及公司為強化網域防護及資訊安全管理，公司不開放員工於非公司設備（如個人電腦）連線至內部網路。各廠區均設有辦公室空間供工務及行政人員處理庶務作業，確保作業資料安全並維持工作效能。

2024 年度，聚賢未發生任何違反相關規範之事件，亦無資安威脅與系統弱點通報紀錄，顯示聚賢在客戶隱私及資訊安全管理上的高度重視與嚴謹執行。

- **資訊安全管理政策**

策略	目的	因應方式
資安管控	強化設備維運與資訊資產安全	定期檢測弱點、限縮連線來源 門禁管制、環境監測、定時巡檢 資訊資產盤點、異動變更管理
網路及資安管理	提升網路使用安全並防範外部威脅	密碼強度要求 網段區塊隔離、網路流量監測管控 防火牆更新、入侵防禦偵測、惡意郵件攔阻
資訊存取控制	確保資訊存取權限分工與控管落實	權限分級與分工管理 員工異動即時調整權限 委外廠商簽署保密協議與資訊使用規範
資料備份與復原	確保資訊可用性與災後復原能力	建置資料備份計畫與監控機制 定期備份與還原演練
資安宣導與稽核	提升資安意識與制度有效落實	定期辦理資安講習與宣導活動 新進人員簽署保密協定 實施內部資安稽核作業

更多資訊安全管理政策內容可參考公司 113 年股東會年報

- **資訊安全管理規範**

管理機制	目的	方法
網路威脅控管	主動防禦，即時封鎖網路異常行為	設置適當防火牆防範惡意網路攻擊，並定期測試
本地備份與異地備份	預防重要資訊因外部天災 或人禍而遭遺失或破壞	重要資訊系統或設備已建置適當的備份或監控機制並定期演練，以維持其可用性
網路弱點評估	針對上網行為管控及威脅 偵測，以防止威脅入侵	個人電腦均已安裝防毒軟體且定期確認病毒碼之更新，並禁止使用未經授權的軟體
		持續評估內外部威脅可能造成之資通安全風險，透過系統弱點掃描、網站安全檢測、滲透測試、防火牆規則檢視等作業。並定期評估網路基礎架構環境，持續修補內部系統潛在弱點，及導入資訊安全設備及資安技術應用，強化資安基礎防禦力
資安意識	增強資訊安全意識，減少資安風險	不定期辦理資訊安全及個人資料保護之宣導作業
權限管理	防範員工任意移動或存取 機密資訊	依據文件與職權設定存取權限、保管、加密、解密流程之管理措施
商業機密安全	防範員工使用可移動儲存 裝置洩漏機敏資訊	針對本公司以外之機構或人員因參與本公司併購、重要備忘錄、策略聯盟、其他業務合作計畫或重要契約之簽訂，應簽署保密協定，並不得洩露所知悉之本公司內部重大資訊予他人
郵件安全	防範員工遭受釣魚信件等 社交工程作業威脅	為提升郵件安全與資安意識，故不定期向員工宣導定期更改郵箱密碼（符合複雜密碼規則）與不隨意點擊信件內之連結的重要性
網路存取控管	增強資訊安全意識，強化網路憑證	要求同仁帳號、密碼與權限應有保管與使用之責任，並定期更換密碼

- **資訊安全教育訓練**

聚賢於每年度 1 月與 7 月期間，借助公司大型活動的機會定期為全公司同仁進行資訊安全教育訓練。本年度訓練主要聚焦於社交網路工程，跟同仁宣導最新的詐騙手法，提供公司對於社交網路工程犯罪的認知。2024 年度，聚賢實施兩次釣魚信件演練及一次資訊安全宣導活動，整體社交演練違規率為 0.7%，對於演練中違規之 10 名同仁，公司安排資安意識宣導講座，共計 20 小時，加強其資訊安全防護觀念，持續強化全體員工的資安意識與應對能力

- **資訊安全處理流程**

本公司稽核單位每年度至少會進行一次資訊安全及個資保護控制作業之稽核作業，同時依據內部控制制度自行檢查作業，總結內部控制實施成效並提報董事會覆核確認。若發生重大資訊洩漏情事，則應依循資訊事件通報程序，儘速向管理部門報告，並擬定處理對策，必要時應邀集內部稽核等部門商討處理對策，並於結案後將結果做成紀錄，以供內部稽核進行查核。

