6.3 資料安全與隱私保護

本公司為強化資通安全防護及管理機制，並符合「公開發行公司建立內部控制制度處理準則」，於2022年董事會通過新增訂《資通安全管控辦法》，並成立資通安全推動組織以強化資安之風險控管，負責推動、協調監督及審查資通安全管理事項，並由資安主管每年定期向董事會進行業務報告。年度資通安全政策及目標，由提報總經理以上主管核定，並定期檢視政策及目標且有效傳達員工其重要性。

本公司已自組資訊團隊，陸續延攬相關專業人才加入團隊，2022年度除完成SAP主機演練及下表資安防駭管理措施外，在資源投入方面， IT人力配置至少有5人以上，投入數千萬元以上金額在ERP軟硬體設備升級，並委託符合ISO 27001：資訊安全管理系統的專業廠商負責公司資訊系統之規畫、推行、維護、管理及支援作業等。在教育訓練方面，IT資安小組依據年度防駭計劃方案，首次外聘國內具備豐富資安服務經驗公司的專業講師來向藥華醫藥進行2場「社交工程資訊安全教育訓練」，出席人數185人，出席率71.71%。加強宣導員工的資訊安全意識並落實於日常營運當中，透過員工反饋，以確保本公司資訊安全管理認定之責任。

資料安全

- 增訂《資通安全管控辦法》，並成立資通安全推動組織
- 2024 年導入 ISO 27001：資訊安全管理系統

隱私保護

- 嚴格遵循如歐盟一般資料保護規範（GDPR）
- 對於病患與員工隱私及個資安全，本公司恪遵相關政策與法律規範以確保其權益

185人次

成立資安推動小組進行
2場社交工程教育訓練

資訊安全行動計畫

本公司資訊團隊及硬體設備已逐步建置完善，未來將持續落實《資通安全管控辦法》之規範，確保資安運作之適切性及有效性，定期追蹤改善，建立PDCA的良性循環。

另預計於2024年導入ISO 27001：資訊安全管理系統，建立有效的資訊安全管理機制提升全員的資訊安全意識。

藥華醫藥資安防駭措施

- ✓ 重要核心資訊系統備份強化
- ✓ 資訊安全政策草擬（符合櫃買資安管控指引）
- ✓ 資訊安全健檢規劃與執行（年度執行）
- ✓ 員工社交工程訓練規劃與執行（年度執行）
- ✓ 資訊系統與網路弱點掃描 (於公司內部年度執行)
- ✓ 資訊系統與網路滲透測試（從公司外部年度執行）
- ✓ 檔案加密系統規劃與實施
- ✓ Data loss prevention(DLP) 終端設備資安防護
- ✓ O365 多因子認證 (MFA) 資訊安全強化

落實保護個人隱私

藥華醫藥的隱私政策主要是保護個資隱私及蒐集和進一步處理病患、醫療保健專業人員、公司之間有業務往來之其他個人的隱私資訊的規範。隱私保護主要分為人體臨床試驗階段和藥品上市階段，無論委外研究機構對於受試者資或臨床試驗醫院端相關的全員都必須嚴格遵循內部政策以及各國法規，如歐盟一般資料保護規範（GDPR）、藥品優良臨床試驗規範（GCP）、赫爾辛基宣言、臺灣的「人體研究倫理政策指引」、「醫療法」等，以完善我們對於個人資料保護之責任。2022年無任何侵犯客戶隱私或遺失客戶資料的投訴。

全球資安策略 – 美國資安專欄

治理權責

- 聘請超過20年IT管理經驗之IT總監為資訊與網路安全最高主管，直接報告給VP of Business Operations
- 由資深營運經理申請「國際資訊安全經理人認證（Certified Information Security Manager, CISM）
- 預計2023年3月前設立相關的管理流程與作業辦法

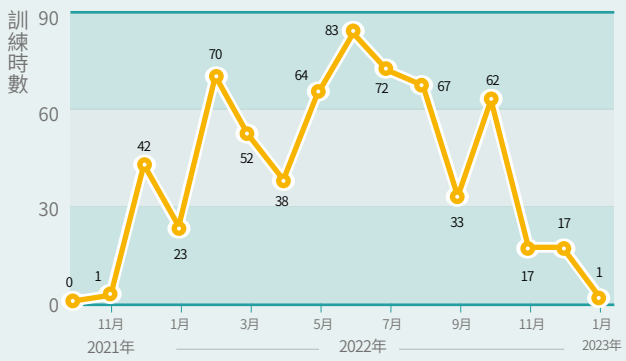
風險防範

- KnowBe4系統具備警示功能，若員工發現異常情況，可於系統進行回報並阻絕潛在釣魚信件。如果員工認為帳號有資安風險之虞，可以直接立即尋求IT支援
- 交由第三方資安監測公司進行IT審查管理以預防駭客或釣魚攻擊，並合作逐步改善管理，進行更加完善的政策文與管理流程建置，包含自攜電子設備相關政策（BYOD Policy）、合理使用政策（Acceptable Use Policy）、資安資產管理（Asset Management）、安全與隱私管理政策（Security and Privacy）、變更管理工作流程（IT Change Management）等
- 目前為止並無受到任何資安或網路攻擊

管理措施

- **管理辦法**：目前已有內部作業辦法(SOP-IT-001)，此辦法不僅管理資安風險，也針對其它可能導致企業持續營運具有風險的事件進行管理說明
- **教育訓練**：對所有員工進行相關政策與管理辦法說明，宣導資訊安全的重要性。針對使用的KnowBe4系統，規範所有員工必須定期完成相關訓練課程。2022年總訓練時數達599小時。

訓練時數



各訓練項目時數