2.4 資料安全與隱私保護

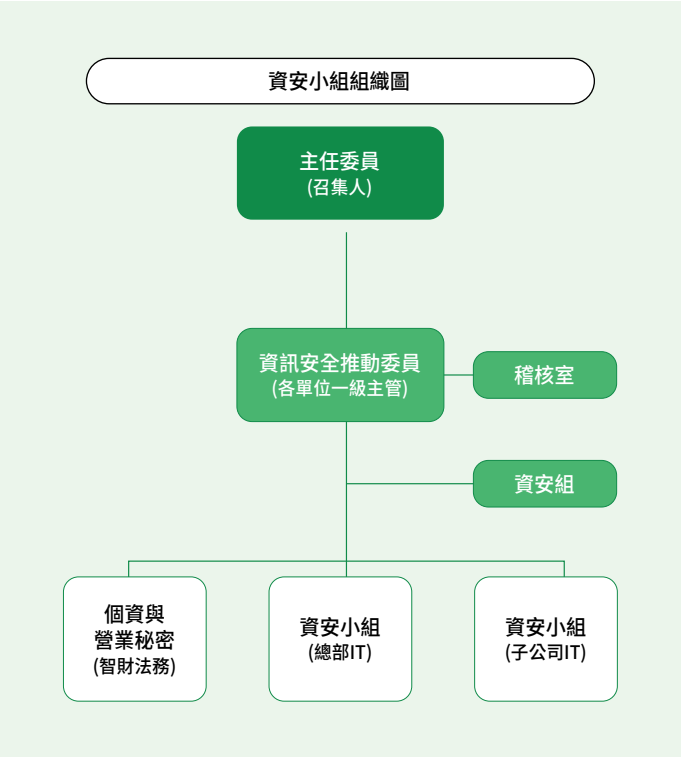
▶ 資訊安全管理制度

藥華醫藥為強化資通安全防護及管理機制，配合臺灣「公開發行公司建立內部控制制度處理準則」之修正及「上市上櫃公司資通安全管控指引」之增訂，本公司持續修訂資通安全政策與辦法，於2022年董事會通過增訂《資通安全管控辦法》及成立資安推動小組並公告於官網，內容涵蓋建置資通安全推動組織、訂定資安政策、舉辦人員訓練、鑑別重要核心業務、盤點及發展資通系統並辦理資安風險評估、執行資通安全防護及控制措施、資通安全事件應變通報及持續精進資通安全管理等事項，並由資安主管每年定期向董事會進行業務報告，最近一次於2025年2月完成資通安全報告，說明近期資安管理實際落實情形及改善事項。

▶ 資訊安全管理小組

為有效推動資訊安全工作，本公司設置資訊安全管理小組(以下簡稱「資安小組」)，統籌資訊安全的推動、治理及監督等。本公司資安小組召集人由執行長或總經理指定高階主管一人擔任，資安小組成員包含總管理處資訊主管、CEO Office Biostatistics主管、總管理處智財主管、法務主管、永續發展中心主管、公司治理主管、QA/QC/PROD/Engineering主管、總管理處人力資源主管等，並由稽核室列席，召集人得依實際需要指派主管擔任委員。另本公司資安小組設立以下推動小組，由召集人指派，負責掌理各項任務之協調、規劃及執行。

1. **個人資料保護與營業秘密管理推動小組：**負責建置個人資料保護體系、執行並督導個人資料保護，以及統籌管理本公司營業秘密相關事宜。涵蓋對象為公司內部員工與對外廠商、CRO臨床資料與泛泰資料等
2. **資訊系統安全維護小組：**負責資訊系統安全管理之規劃與實施
3. **稽核室：**負責資訊安全相關作業之稽核



藥華醫藥總部2023年10月導入ISO 27001：2022資訊安全管理系統，並於2024年4月通過稽核審查、7月9日正式取得認證。導入ISO 27001後，公司的資訊安全從被動防禦轉向主動管理，建立更健全的資安管理架構，強化資訊安全防護能力，不僅符合法規要求，也增強國際競爭力，提升員工資安意識。未來，短期內我們期待能填補資安人力缺口或尋求外部資安顧問協助，並將部署SASE、SIEM及SOC視為長期目標，強化公司整體資安防護能力。


Certificate TW24/00000563
The management system of
PharmaEssentia Corp.
has been assessed and certified as meeting the requirements of
ISO/IEC 27001:2022
For the following activities
The provision of development and operation of Enterprise Resource Planning system(ERP), network and server room facility maintenance via Information Technology Department in accordance with the Statement of Applicability version 1.0.
This certificate is valid from 09 July 2024 until 08 July 2027 and remains valid subject to satisfactory surveillance audits.
Issue 1. Certified since 09 July 2024
SGS
IAF

ISO 27001 認證通過

資訊安全相關訓練

為提升員工的資訊安全意識，於2024年舉辦2場資訊安全教育訓練以及2場ISO 27001的教育訓練，共計289人參與，總時數約334小時。同時並培育9名員工參與ISO/IEC 27001：2022主導稽核員課程，每人共6小時，並已取得主導稽核員認證。我們規劃從臺灣總部開始，未來將要求美國、日本等子公司逐步導入。此外，我們也指派1名IT部門主管參與多樣主題的資訊安全研討會，進一步瞭解現在資安趨勢與因應做法。

美國子公司雖未導入ISO 27001資訊安全管理系統，但已經開始資安課程教育訓練，規範所有員工必須每月完成網絡安全主題培訓，2024年總計參與人數157人及總參與時數593小時，且IT部門每月亦對全體美國子公司及PIRC員工進行模擬釣魚攻擊測試，提升同仁的資訊安全意識。

課程名稱	課程內容	場次	參與人數	教育訓練時數/人	總教育訓練時數
資訊安全教育訓練	1. 資訊安全政策宣導 2. 社交工程防駭實務	2	280	1	280
ISO 27001：2022教育訓練	1. ISMS內部稽核訓練 2. ISMS程序教育訓練	2	9	6	54
資訊安全研討會	1. CIO Taiwan智慧醫療研討會 2. Menlo Security企業瀏覽器的全新世代 3. CIO Taiwan企業上雲(多雲管理下的關鍵應用) 4. 企業AI知識管理系統 5. 宏碁資訊舉辦的AI引領未來 6. CIO數位轉型與AI創新	6	1	40.5	40.5

個資保護 GRI 418-1

資訊安全與隱私保護的對象除公司內部員工外，也包括醫療保健專業人員、醫療機構、委外合作機構以及臨床試驗患者。在患者隱私安全的部份，無論是藥華醫藥的委外研究機構或臨床試驗醫院端參與的醫護人員，均須嚴格恪守隱私保護政策，並符合國外及國內法規要求，例如：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、臺灣人體研究倫理政策指引與醫療法等，以落實我們對於個人資料保護之責任。2024年藥華醫藥全球各公司皆無發生員工或顧客資料保護與隱私權申訴之事件，也無遺失客戶資料的投訴事件。