大江生醫資訊安全政策

本公司以 ISO 27001 與 BS7799 為參考標準，並依據公司內部實際管理需求制定資訊安全政策。主要之資訊安全管理需求為建置基準，以戰略數據中心提供的相關資訊服務，以及公司相關部門為主要範圍。

為了維護公司競爭優勢，所有員工均應依照公司所頒布的相關資訊保護辦法做好自我管理，並具備資安意識。除了資訊系統所提供服務之資訊安全控管措施，更著重保護重要個人及交易資料等資訊之機密性、完整性及可用性。同時強化資訊安全管理，確保資料、系統、設備及網路等軟硬體資訊安全，營造健康的資訊環境，部署創新的資訊安全防護技術，落實推動資訊安全管理作業，以提升大江生醫集團安全的服務品質。

為達成此政策，制定相關資訊安全規範，確認資訊安全管理運作之有效性。

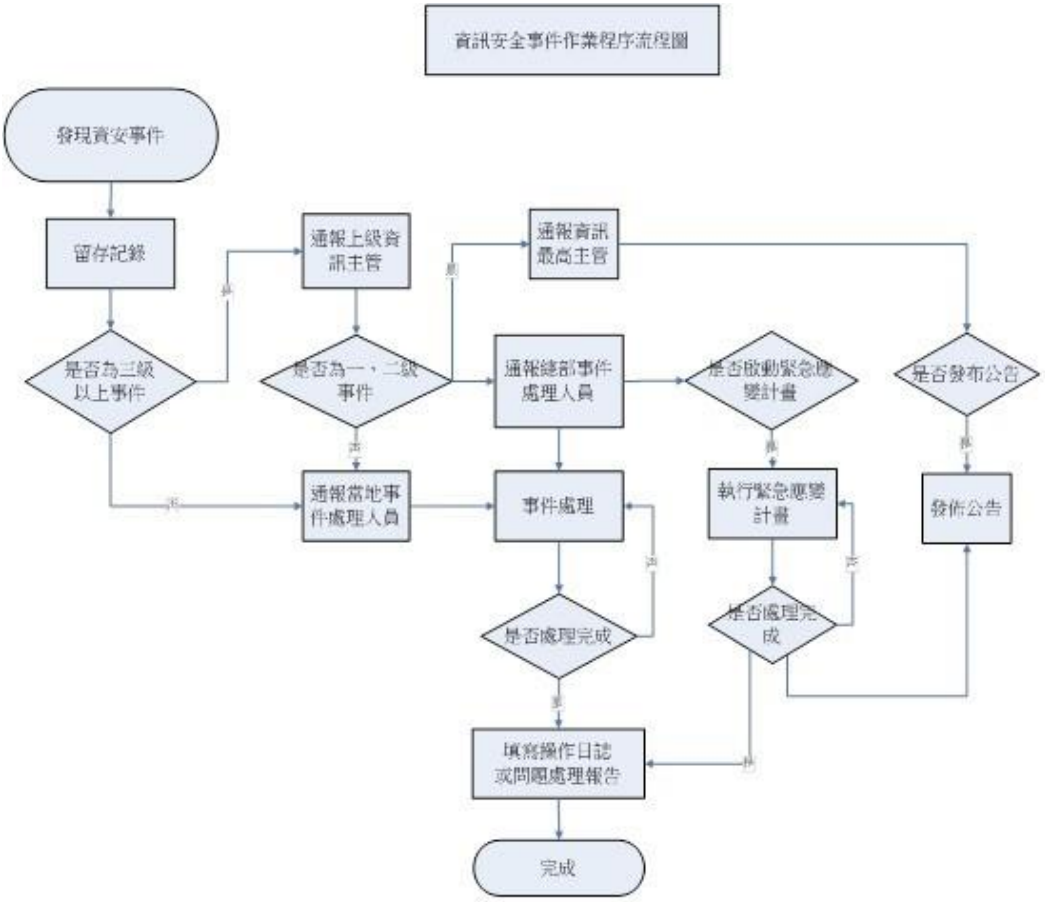
- 戰略數據中心各單位均建立相關資訊資產清單，並明定擁有者，依資訊資產等級差異，執行風險評鑑作業，針對高於可接受水準之風險應進行風險管理，以有效降低風險，並持續落實各項管控措施。
- 相關人員錄用應進行必要之考核並簽署相關作業規定文件，異動或離職時應歸還其資訊資產、新進與現任同仁均須參與資訊安全教育訓練並以提昇資訊安全防護之認知觀念。
- 進出實驗室及資訊安全管制區域應落實相關門禁管控及物品攜出入規定。
- 嚴禁同仁私自架設網路設備串接外部網路與公司內部網路，內外部網路均設置防火牆、非武裝區（DMZ）、及必要之安全設施保護之，重要設備應建置適當之備援或監控機制，維持其可用性。同仁之個人電腦應安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軟體。
- 同仁個人持有之帳號、密碼與權限應善盡保管與使用責任、管理人員應定期清查覆核，重要系統運作資料應定期備份並執行回復測試。
- 系統開發應於初始階段考量安控機制之建置、委外開發部分應強化控管及契約資訊安全之要求，評估系統的控管要求可採取必要之控管。
- 同仁遇有資訊安全事件，應立即通報，並依照資訊安全事件處理程序處理，避免事件擴大，並配合權責部門共同解決。
- 同仁日常作業應落實確認覆核機制，維持資料準確性，主管人員應督導資訊安全遵行制度落實情況，強化同仁資訊安全認知及法令觀念。

- 本公司定期檢視資訊安全政策，以反映政府法令、技術及業務等最新發展現況，確保資訊安全實務作業之有效性。

資訊安全管理方案

公司除了成立資安管理委員會負責統籌、管理、督導集團所有資安業務，並有專屬資安工程師專責處理資安工作、並定期進行弱點掃描、社交工程演練、防護系統有效性查核...等相關資安檢測，提供相關資安宣導及教育訓練課程，雖暫無購買資安險，但透過資安委員會的運作及資安政策的執行，仍可提供安全無虞的資安環境，保障公司各項服務的資訊安全。後續目標則是完備各廠資安專家系統，以強化集團資安防護網，建立資安聯防機制。未來除了資安人才的擴充外，計畫進行培訓及認證工作，讓公司的資訊安全在人力、能力上能更加完善，值得信賴。

資安事件通報程序



2021 年執行情形

依循管理方案執行 2021 年無重大資訊安全事件及風險

行動方案	單位	2021 年行動計劃	執行成果
資訊安全防禦	大江生醫	透過數據分析有效發現異常事件並提供相關單位即時處理	持續分析與處理資訊安全事件，主動阻擋異常連線及可疑電子郵件，降低駭客攻擊與資料外洩風險
		持續優化資訊安全管理平台與進階持續性滲透攻擊(APT)防護系統及事件分析調查能力	
		成立資安專責單位，與資安單位聯合運作，以強化資安聯合防禦	已成立資安專責單位，強化資訊治理
		提升端點防護機制、端點管理功能並搭配端點惡意程式偵防作業，強化縱深防禦能力	強化個人電腦以及伺服器防毒提升作業，分析可疑程式與行為
		定期針對系統執行滲透測試	已完成透過發動之實戰測試，在服務承載程度以及應變通報及時狀況以符合資安要求
		持續針對系統定期弱點掃描	已完成透過已公開之系統弱點進行定期弱點掃描與修復
		持續不定時針對系統漏洞提供相關修補管理	已完成針對系統重大安全性之漏洞補丁提供不定時的系統修補