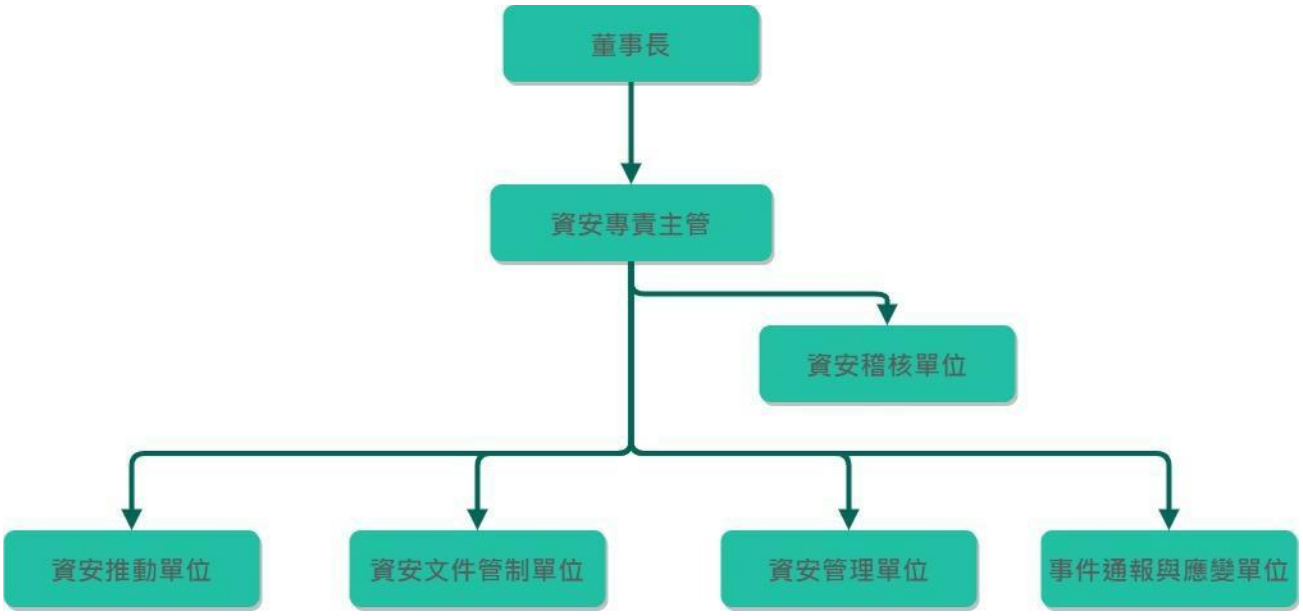
# 資通安全具體管理暨執行情形

（一） 資通安全風險管理架構、資通安全政策、具體管理方案及投入資通安全管理之資源。

1. 企業資訊安全治理組織：




2. 資通安全政策：

為有效推行資訊安全管理制度，以確保資料、系統、設備及網路安全，本公司訂定有資訊應用相關之電腦軟硬體管理規定、系統主機管理規定及資通安全相關辦法，做為資訊安全管理工作之執行與評估，以確保本公司各資訊系統可持續性運作、資訊之完整性、有效性、可用性、及安全性，並落實遵守資通安全相關法律及規定。

3. 資通安全具體管理方案：

（1） 資訊系統帳號密碼管理

- 帳號每 90 天變更一次密碼，密碼需有英文大小寫加上數字，長度需大於 8 碼，輸入錯誤 3 次將鎖定帳號，需由 IT 人員進行驗證才能解鎖，密碼到期前一週會透過系統通知使用者進行密碼變更。

（2） 資訊系統備份

- 每日資訊系統於本機進行第一備份，並透過 NAS 或磁帶機等備份設備進行第二備份、透過網路進行第三異地備份。

（3） 資訊系統安全保護

- 所有資訊安全設備需安裝防毒軟體，隨時確認防毒軟體更新至最新版本及最新特徵碼。

（4） 資訊機房及伺服器管理

- IT 人員進出機房需刷卡進行驗證，非 IT 人員進出機房需填寫機房進入申請單並由 IT 人員陪同。

(5) IT 人員教育訓練要求

- IT 人員行為準則及系統操作準則透過線上考核系統進行教育訓練及測驗，需通過測驗後才能執行相關動作。

(6) 工廠 GMP/IT 相關

- 依據 GMP 相關規定定時進行儀器校時、實驗資料備份及人員權限檢視。

(7) 定期安排社交工程演練或資安弱掃

- 定期安排進行 Email 社交工程演練，並持續進行。
- 定期安排資安弱掃，確保資訊系統弱點項目均受控制

(8) ERP 災害還原中心

- 建置 ERP 災害還原中心，每年定期演練。

(9) GDPR 個資管理程序

- 就 GDPR 相關之臨床試驗個資，建立相關防護 SOP。

(10) 加入資安資訊分享與分析中心(ISAC)

- 加入 ISAC 以了解資安預警、資安威脅、與弱點資訊。

(11) 加入科學園區資安資訊分享與分析中心

- 加入科學園區資安資訊分享與分析中心強化及共享第一手資安訊息。

(12) 防火牆檢視及維護

- 專人定期檢視防火牆的警示與紀錄檔。
- 定期封鎖有疑慮之 IP、網路行為及程式。

(13) 落實 VPN 管控

- 依照申請權限開放可使用之系統。
- 每一季整理未登入之 VPN 帳號並停用權限。

4. 投入資通安全管理之資源：

(1) 投入人員總數：企業資訊安全治理組織及資訊部門全體。

(2) 相關會議召開次數：

- 每週：IT 會議檢討。
- 每月：公司層級重大事項報告。
- 每季：企業資訊風險專案報告。

（二）截至民國113年11月30日止，本公司無重大資通安全事件。並已提報113年12月26日友霖生技董事會中報告。