晟德大藥廠股份有限公司

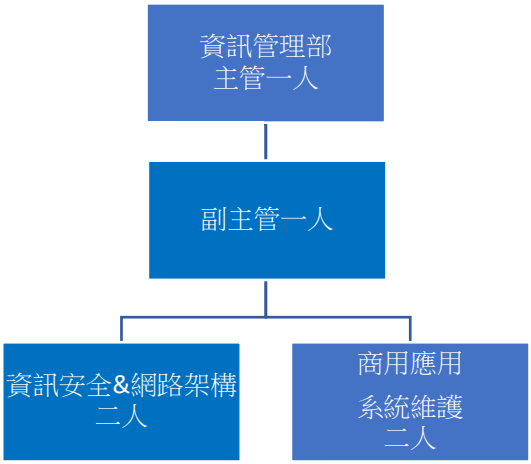
資通安全管理準則

(一) 資通安全風險管理架構

1.企業資訊安全治理組織

晟德大藥廠股份有限公司(以下簡稱本公司)，設有資訊管理部，負責統籌資訊安全及保護相關政策制定、執行、風險管理與遵循度查核，由資訊管理部最高主管每年向董事長彙報資安管理成效、資安相關議題及方向。

2.本公司資訊管理部組織架構



(二) 資通安全政策

1. 企業資訊安全管理策略與架構

企業資訊安全組織為有效落實資安管理以涵蓋各廠區，每季召開例行會議，依據規畫、執行、查核與行動（Plan-Do-Check-Act, PDCA）的管理循環機制，檢視資訊安全政策適用性與保護措施，每年向董事長回報執行成效。

- ◆「規畫階段」: 著重資安風險管理，建立完整的資訊安全管理系統（Information Security Management System, ISMS)，從系統面、技術面、程序面降低企業資安威脅，建立符合公司需求、最高規格的機密資訊保護服務。
- ◆「執行階段」: 建構多層資安防護，持續導入資安防禦創新技術，將資安控管機制整合內化於軟、硬體維運等平日作業流程，系統化監控資訊安全，維護本公司重要資產的機密性、完整性及可用性。
- ◆「查核階段」: 積極監控資安管理成效，依據查核結果進行資安指標衡量及量化分析。
- ◆「行動階段」: 以檢討與持續改善為本，落實監督、稽核確保資安規範持續有效；當員工違反相關規範及程序時，視違規情節進行人事處分(包括員工當年度考績或採取必要的法律行動)；此外，亦依據績效指標及成熟度評鑑結果，定期檢討及執行包含資訊安全措施、教育訓練及宣導等改善作為，確保本公司重要機密資訊不外洩。

2. 具體管理方案

(1) 網路安全

- 網路安全導入先進技術執行電腦掃描及系統與軟體更新。
- 強化網路防火牆與網路控管，防止電腦病毒跨機台及跨區擴散。

(2) 裝置安全

- 建置電腦設備皆列管，防止未被授權或內含惡意軟體的設備進入公司。
- 依電腦類型設置端點防毒措施，強化惡意軟體行為偵測。

(3) 應用程式安全

- 制定開發流程應用程式安全自檢表、評核標準及改善目標。
- 持續強化應用程式控管安全控管機制，並整合於開發流程及平台。

(4) 資料安全

- 透過文件機密分類，控管資料夾存取權限。
- 各項重要資料皆進行定期備份，並遵守３２１備份原則。
- 定期傳達公司最新資安規定及注意事項。

3. 評估與審查

本政策由董事長核定，每年度至少評估一次，或組織內有重大變更時，依作業、組織異動重新評估。依相關法律、技術、業務之發展，予以合適修訂。

4. 公告實施與宣達

本政策經董事長核定通過實施，修正時亦同。