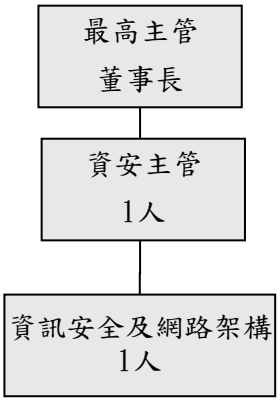
晟德大藥廠股份有限公司

113 年資通安全管理情形

一、資訊安全風險管理架構：

本公司資訊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，為更進一步強化資安防護及管理，112年起設置資訊安全主管1名及資訊安全人員1名，負責資訊安全制度之規劃、監控及執行資訊安全管理作業、資訊安全事件應變處理等，並定期召集會議檢討資安政策，及每年至少一次向董事會彙報資安策略方向及資安管理成果，最近一次提報日期為114年1月10日。。

本公司資安組織架構如下：



二、資訊安全政策：

本公司資訊安全單位為有效落實涵蓋各廠區之資安管理，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。

- 「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。

三、具體管理方案：

1.網路安全

(1)網路安全導入先進技術執行電腦掃描及系統與軟體更新。

(2)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

(1)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。

(2)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

(1)制定開發流程應用程式安全自檢表、評核標準及改善目標。

(2)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

(1)透過文件機密分類，控管資料夾存取權限。

(2)各項重要資料皆進行每天定期備份，並遵守 321 備份原則，即至少 3 份資料備份、存放 2 種不同儲存媒介與至少 1 份異地備份，對公司資料安全進行全面保護。

(3)定期傳達公司最新資安規定及注意事項。

5.資訊安全訓練

對公司員工進行資安意識與防範教育，及進行社交工程演練資安防駭訊息電子郵件，提供員工資安事件資訊及防範因應措施。

四、投入資通安全管理之資源：

1.定期資安會議：本公司以風險導向的角度，定期每季召開資訊安全會議，針對資訊安全風險管理、威脅情資管理（於 112 年加入 TWCERT 資安聯盟）、資訊安全控管、委外及依賴關係管理、資安事件管理與回應等面向，確認營運整體風險，採取適當之因應措施，以維持網路及資訊安全強度。113 年已召開 4 次資訊安全會議。

2.教育訓練：113 年員工資通安全教育訓練總時數為 25 小時，執行 196 次電子郵件社交工程釣魚郵件演練，另提供新進人員資安教育訓練 58 人次。

3.資安公告：113年總計已發出3則資安相關公告，傳達資安防護重要規定與注意事項。

五、資訊安全措施執行成果：

113 年本公司無發生資通系統、官方網站或內部文件檔案遭駭客攻擊入侵，或有個資、內部文件檔案資料外洩、遺失等重大資安事件，資訊安全措施執行成果良好。