資通安全管理

台灣神隆為一國際性原料藥公司，致力於建立合規完善的資訊安全系統，來保護公司重要的研發技術、智財專利，並確保營運、製造與品質保證等企業功能運作在安全保護下同時符合 GMP 規範要求。

一、 管理架構

台灣神隆的資訊安全，由行政管理中心轄下的資訊技術處負責，資訊技術處統籌資訊安全相關政策制定、執行、風險管理與遵循查核，定期向總經理報告執行情形；本公司有設一名資安專責主管和一名資安人員，以強化公司資通安全管理。

在整體的資通安全管理上，每年定期檢視資安事件、資安政策並進行改善，同時持續關注並投入資金推動新的資安服務，加強與更新企業資安防護網，以使公司持續穩健運作；並且與時俱進更新汰換不合時宜的措施與設備；導入新科技資安服務進行保護與防禦；規範、查核及嚴格限制裝置存取與人員存取行為；透過稽核機制追蹤與查核各項異常活動；並建置各種備份與災難復原機制，以確保資料符合 GMP 合規性。

二、 資通安全政策

本公司內部控制制度訂有「使用電腦化資訊系統作業」，並關注主管機關最新資安相關法令動態以檢視制度符合主管機關之要求，強化公司資訊安全管理機制。

透過 PwC 資誠聯合會計師事務所作為 ISO27001:2022 導入顧問單位，並藉由 ISO 國際認證落實資安自理與管控，確保資訊安全管理制度符合國際標準，提升整體資安治理成熟度。

三、 具體管理方案

面對許多新型態多變的資安威脅，如僵屍網路、零時差攻擊、勒索病毒等等，本公司導入次世代防火牆(Next Generation Firewall)、入侵預防系統(IPS) 、網站過濾(URL Filtering)、防毒牆(Anti-Virus Wall) 、郵件安全系統(Anti-Spam)以增強能力應對，防範駭客入侵和破壞；實施網路分割與多層次網路隔離的縱深防禦機制，防止攻擊長驅直入內部網路；限制遠端連線存取範圍，同時啟用流量側錄與稽核，監控網路異常，事先找出威脅加以阻絕，避免災害發生與擴大、降低風險與損失。

隨著數位科技蓬勃發展及辦公模式的改變，端點安全威脅也隨之提升。在終端電腦設備上，本公司實施設備存取控管、個人帳號權限與特權帳號的分級管理，建置次世代防毒系統、增強密碼強度與採用多重因素驗證，來防範及降低受惡意軟體與勒索軟體感染的可能性；同時持續進行程式及裝置的修補和安裝更新、使用合法軟體與符合資訊安全規範的系統；導入文件加密防止資料外洩。

因應國家資安主管機關近期發布之「生成式 AI 語言模型」相關風險警示，並為強化公司整體資訊安全及資料保全，調整並實施生成式 AI 工具使用規範，明確界定使用範圍與資料輸入限制，避免敏感資訊外洩或誤用，並要求員工遵循內部指引，確保生成式 AI 技術的應用符合資安政策與法規要求。

除此之外，建置多種類型的備份與復原機制，並且定期還原演練，以符合當前藥廠法規規範的資料完整性(Data Integrity)。為有效落實本公司資訊安全政策，員工需參與資訊安

全教育訓練，強化資安觀念與識別資安威脅。協同外部資安公司建構資訊安全聯絡網，協助企業及時處理資安問題，有利於第一時間進行阻絕避免災害擴大。

運用新科技來提升營運效率之餘，同時也需預防其帶來的網路資訊安全威脅，本公司採用以下措施來保護公司重要智慧資產，並依循 PDCA 的循環管理來達到資安目標持續改善。

1. 使用符合資訊安全規範的雲端服務平台。
2. 啟用多因素認證來強化密碼保護。
3. 限定網域伺服器(DC)登入管理。
4. 限定遠端服務連線設備與存取範圍。
5. 限定 GPO 派送。
6. 限定 USB 使用。
7. 定期災害還原(DR)演練。
8. 不定期公告案例宣導強化員工資安意識。
9. 加密網路傳遞與資料存取
10. 採用多層次網路架構主動進行防堵與隔離來保護實驗室與生產線設備。
11. 佈署次世代防毒軟體保護辦公室和實驗室電腦。
12. 建構安全防護偵測機制如 DDI (Deep Discovery Inspector)、Deep Security、XDR(延伸式偵測及回應)，並且由第三方專業廠商進行監控。

四、 投入資通安全管理之資源

針對公司近期所投入的資通安全管理資源，主要包括以下方面：

(1).軟體盤點：每年一次；確保合法使用授權軟體與更新風險識別資料庫資訊。

(2).資料恢復演練：核心系統定期災難復原演練每年一次。

(3).特權帳戶與遠距辦公強化管理：

- 核心系統之伺服器特權帳號登入採用雙因素帳戶認證。
- 強化特權認證安全系統消除特權帳號管理和存取控制過程中常見的複雜性和耗時流程，降低人為疏失。
- 強化遠距辦公人員帳戶雙因素認證措施。

(4).與第三方雲端監控中心合作：

- 與第三方雲端監控中心合作，建置多層次的偵測及回應資安防護系統。對公司重要資訊系統進行全面監控，並能夠對各種異常行為進行及時的檢測與回應。

(5).加強情報與資安培訓：

- 加入 TW-ISAC 成員，享有該組織的情資分享，並不定期對內部公告資安防範措施與攻擊手法說明以強化同仁資安意識。
- 加入科學園區資安資訊分享與分析中心(SP-ISAC)的資安聯防，定期交換業界資安風險情資，有利於隨時掌握整體資安新技術及攻擊威脅。
- 114 年度資訊同仁除參與六場外部資安相關研習活動，並有三位資安同仁通過財團法人台灣金融研訓院所舉辦(AI 對資訊安全的影響及因應)、(資安攻防技術及事後處理與補救措施)與(駭客攻擊手法及防禦要點)共計 6 小時訓練，了

解到最新的資安威脅和攻擊手法從而降低資訊安全風險，而採取更有效的防範措施。

(6).資安防範措施與攻擊手法說明以強化同仁資安意識：

- 不定期內部公告全體同仁發布資安防範措施和攻擊手法說明，從而提高同仁的資安意識和安全素養。
- 新進同仁須於到職後完成新生訓練課程並取得通過資格，其中課程內容包含「資訊安全-IT 相關義務」，以提升新進同仁對資訊安全之義務。
- 每季舉辦實體資訊安全通識教育訓練課程，提高同仁資訊安全素養。
  114 年度資訊技術處透過內部 e-Learning 線上課程提供「資訊安全教育訓練」，課程時數約 0.5 小時。另透過社交工程演練強化資安觀念和識別資安威脅，全體員工參與人數約 755 位；並不定期對內部公告資安防範措施與攻擊手法說明，114 年共發布 27 則。

五、 取得第三方認證

本公司於 115 年 03 月 24 日通過 SGS 台灣檢驗科技股份有限公司的第三方驗證且取得證書，依據 ISO 27001:2022 對於資訊安全、網宇安全及隱私保護進行相關查驗作業，認證效期為 115/03/24 至 118/03/24。(檢附相關證書資訊。)