台康生技股份有限公司

資通安全及資訊管理報告

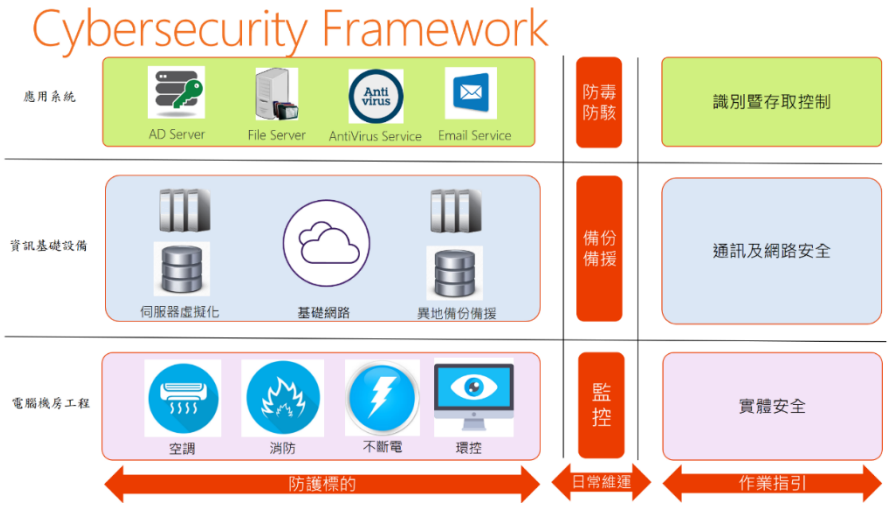
資通安全列入年度稽核項目，定期檢視和評估安全防範措施，並定時更改各項安全設定、更新系統並與外部專業廠商合作來確保資訊及網路安全性。另為確保資訊系統可持續提供穩定之服務，建有各種備援機制及備份系統，並適當地改善相關之流程和提升電腦軟硬體等因應措施。資訊部門經常 Email 各項資安訊息予員工，並加入台灣電腦網路危機處理暨協調中心(TW-CERT)會員，以即時接收資安風險情資(TW-IASC 情資)，資安與資訊系統負責人考量其風險等級、適用性及可行性後，盡速更新或調整內部資通相關設備、架構及作業規範，以降低各種內外部資訊安全風險造成嚴重損害之可能性。 最近期於 113/3/8 董事會報告資安議題。

一、敘明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等：

1. 資通安全風險管理架構

透透過建立資訊安全風險管理架構，降低因內外部資訊環境變遷所帶來未知的資訊安全威脅風險。本公司為降低引進新資訊科技及外在環境變化所帶來的未知資訊安全風險，由資訊部負責統籌資訊安全及相關事宜，擬定相關內部資安計畫，經核准後，依標準作業程序進行資訊安全風險管理，並定期進行內部資訊安全檢查、人員資安意識宣導及資訊安全相關演練。

本公司資通安全框架採分層設計，架構如下所示：



2. 資通安全政策

為達到企業永續經營的目的，確保本公司各資訊系統能有效的運作，以支援各業務之正常運作，確保持續營運，以期將營運損失降到最低。本公司全體員工於使用資訊相關系統時，以此資訊安全管理政策作為管理及遵循之依據。

資訊系統安全政策分為下列數個部分：

(1) 制度及規範：配合相關法令、本公司業務及資訊技術之變化，更新相關資訊安全管理規範、基礎架構、系統、資訊安全防護技術，以維護重要資訊系統的機密性、完整性、可用性，持續保護資訊不受各種威脅，重要資訊系統之權限管理及變更，均應留下紀錄以作為稽核之依據。

(2) 資訊科技的管理：資訊系統即時更新與評估，施行必要之控管措施以確保資料、系統、網路、資訊基礎設施的安全。

(3) 人員與組織：資訊部現有資訊系統安全專家認證(CISSP)一員，負責資訊安全管理相關業務及資訊部同仁的資訊安全技術訓練，再由資訊部向外擴散，對同仁實施資安訓練與宣導，藉此提升內部人員的資安意識與相關專業技術，使其瞭解如何防範常見的網路攻擊。

3. 資通管理方案及投入資通安全管理之資源

本公司積極強化公司整體資訊系統之安全性，自資訊安全規範開始，乃至於資訊基礎之設計、系統維護及升級汰換、專業人員訓練、員工資安意識提昇宣導，均納入資訊安全整體考量範圍，每年進行自我檢視相關制度是否符合環境變遷，並依需求適時調整。本公司於 110 年導入臺灣智慧財產管理規範(Taiwan Intellectual Property Management System，簡稱 TIPS)，以強化本公司機密資料之作業管理。具體施行資通安全管理措施包含如下：

台康生技資通安全管理措施		
類別	說明	作業方式
權限管理	人員及群組帳號及認證方式管理、權限管理、系統管理權限控管	● 人員帳號管理作業，均依作業程序申請及經各權責主管核准後進行使用及變更，使用者離職或職務變更後立即撤銷其使用權限，以防止未經授權之存取 ● 定期審視系統相關權限 ● 系統帳號生命週期及權限帳戶管理 重要系統採行多因數認證及限定登入點方式管制

存取管理	資料流控管及稽核，實體設備存取管理、稽核紀錄及事件調查作業	● 資訊系統資料流之進出修改，設立並保存其存取稽核紀錄 ● 資訊系統主控台之實體安全防護 ● 稽核紀錄之分析與自動異常告警作業 ● 依重要性及風險程度進行資訊安全等級分區處理 重要文件導入數位版權管理技術，用以控管資料流，以避免非經授權的存取
威脅及風險管理	對於內部員工、外部人員、系統潛在弱點所可能帶來的資訊風險進行評級，並施以降低風險之處置	● 使用者電腦預置作業標準化 ● 外部廠商存取本公司資訊系統之作業規範 ● 新技術導入之風險評估作業流程 ● 部屬多品牌多層防火牆及雲端郵件內容過濾，降低外部網路攻擊及釣魚信件的入侵機率 ● 加強端點安全，使用者電腦定期更新並安裝防毒軟體 定期進行人員資訊安全宣導教育，提高資訊安全意識
系統完整性及可用性管理	維護資料與系統之可用性與完整性，發生災害或受破壞時，可回復正常作業	● 主機已完成虛擬化作業，並以叢集方式設計，以提昇系統之可用性 ● 導入大型儲存裝置，並搭配定期自動化本地及異地備份作業，並依計畫進行還原測試，確保系統之完整性與可用性 基礎設施多重備援機制，多套不斷電系統搭配自動發電機，搭配 N+1 及 1+1 精密空調，內外網路線路及設備多重備援，降低資訊服務中斷的機率。

投入資通安全管理之資源與管理：

(1) 113 年資訊安全相關議題的會議及討論共 4 次。

(2) 更新新版資安學習手冊-2024，為所有公司同仁建立並更新資通安全概念。

(3) 本公司亦加入 TWCERT/CC 以進行資安情資分享。

(4) 本公司除每月固定於會議中宣導資安相關議題外，另資訊部門如遇有特殊資安情資，其風險程度有可能影響本公司資訊安全時，即時以通訊軟體及 Email 方式告知內部同仁。

二、列明最近年度及截至年報刊印日止，因重大資通安全事件所遭受之損失、可能影響及因應措施，如無法合理估計者，應說明其無法合理估計之事實：無此情事。

三、科技改變（包括資通安全風險）對公司財務業務之影響及因應措施。

政府近年來積極推動生技產業，其中生技製藥業因具有技術門檻高、研發週期長、專業技術需求及附加價值高等特色，產業進入門檻相對較高，故短時間內不易產生劇烈變化，且本公司擁有高度專業研發能力，對於科技改變及產業變動均能密切掌握並視需要採取適當因應措施。最近年度及截至年報刊印日止，本公司及子公司未因科技改變及產業變化對本公司財務業務造成重大影響。

資訊科技及外部環境的快速改變，為降低外部變化對財務業務之衝擊，本公司與外部專業資訊安全顧問，參照 NIST CSF 網路安全框架及相關同業標準，規劃修訂出適合本公司之相關資訊安全政策，據此分階段施行並定期重新審查調整，做為本公司導入各資訊系統及服務時評估及判斷之基準。

另鑒於新型態偽冒詐騙電子郵件日益增加，已成為企業內部受駭主要管道之一，手法也不斷更新，考量於此，除本公司既有的雲端郵件防護措施外，本年度開始相關大型郵件服務供應商如 Google 及 Yahoo 均開始推動郵件認證協議並計劃強制施行，本公司資訊單位於本年度(2024)第一季底，完成強制郵件認證要求 SPF(寄件者政策框架)，DKIM(網域驗證郵件)及DMAR(網域驗證及報告一致性)協定的導入，以防止偽冒為公司內部人員的釣魚信件發送至內部及外部聯絡人，並對內部使用者加強相關郵件防範宣導，提高郵件使用者的資訊安全意識，降低受駭風險。

對於網路帳號認證方面，由於來自外部的帳號入侵嘗試日益增多，本年度計畫分階段導入多重要素驗證(Multi-Factor Authentication,MFA)，透過多重不同認證方式同時進行登入驗證，避免使用者身分遭冒用，導致重要資訊外洩或偽冒身分進行詐騙等情事。