資通安全風險管理-114 年度

1 資通安全管理策略及架構：

1.1 企業資訊安全治理組織，慧智基因股份有限公司設立「資訊工程處」，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，並已加入台灣電腦網路危機處理暨協調中心並進行資安聯防，隨時更新及接收最新安全情資並隨時進行安全防控，且由 總經理每半年向董事會彙報資安管理成效、資安相關議題及方向。慧智基因股份有限公司資訊工程處肩負監督治理企業資訊安全之責，由 總經理及資訊工程處主管監督評核公司資訊與網路安全管理機制及方向。公司為執行資訊安全組織訂定的資安策略，確保內部遵循資安相關準則、程序與法規，由 總經理及資訊工程處主管負責稽核、監督、檢視及決議資訊安全與資訊保護方針及政策，並由資訊工程處轄下之資訊服務部、系統維運部執行並落實資訊安全管理措施的有效性。

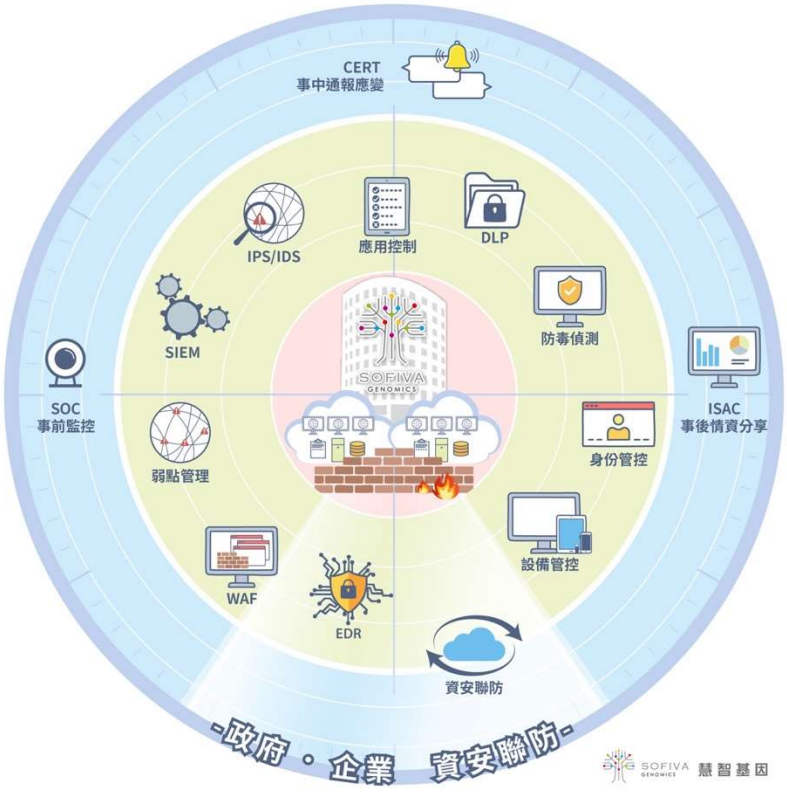
1.2 資訊安全管理策略與架構，公司為有效落實資安管理，由資訊工程處，定期召開例行會議，依據規畫、執行、查核與行動(Plan-Do- Check-Act, PDCA)的管理循環機制，檢視資訊安全政策適用性與保護措施，並定期與 總經理回報執行成效。「規畫階段」著重資安風險管理，建立完整的資訊安全管理系統(Information Security Management System, ISMS)，從系統面、技術面、 程序面降低企業資安威脅，建立符合客戶需求、最高規格的機密資訊保護服務。「執行階段」則建構多層資安防護，持續導入將資安防禦創新技術，將資安控管機制整合內化 於軟硬體維運、供應商資安管理等平日作業流程，系統化監控資訊安全，維護慧智基因股份有限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，並透過定期模擬演練資安攻擊進行資訊安全成熟度評鑑。「行動階段」則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，依據資安違規處理流程進行處置，並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，確保慧智基因股份有限公司重要機密資訊不外洩。

2　資通安全風險與因應措施：

2.1　資訊技術安全之風險及管理措施 慧智基因股份有限公司已建立全面的網路與電腦相關資安防護措施，但無法保證其控管或維持公司製造營運及會計等重要企業功能之電腦系統能完全避免來自任何第三方癱瘓系統的網路攻擊。這些網路攻擊以非法方式入侵慧智基因股份有限公司的內部網路系統，進行破壞公司之營運及損及公司商譽等活動。在遭受嚴重網路攻擊的情況下，慧智基因股份有限公司的系統可能會失去公司重要的資料，營運上也可能因此停擺。慧智基因股份有限公司透過持續檢視和評估其資訊安全規章及程序，以確保其適當性和有效性，但不能保證公司在瞬息萬變的資訊安全威脅中不受推陳出新的風險和攻擊所影響。網路攻擊也可能企圖竊取公司的營業祕密及其他機密資訊，例如客戶或其他利害關係人的專有資訊以及慧智基因股份有限公司員工的個資。惡意的駭客亦能試圖將電腦病毒、破壞性軟體或勒索軟體導入慧智基因股份有限公司的網路系統，以干擾公司的營運、對慧智基因股份有限公司進行敲詐或勒索，取得電腦系統控制權，或窺探機密資訊。這些攻擊可能導致公司因延誤或中斷訂單而需賠償客戶的損失;或需擔負龐大的費用實施補救和改進措施，以加強公司的網路安全系統;也可能使慧智基因股份有限公司因涉入公司對其有保密義務之員工、客戶或第三方資訊外洩而導致的相關法律案件或監管調查，而承擔重大法律責任。慧智基因股份有限公司過去曾經因遭受勒索病毒攻擊，未來也可能面臨類似的攻擊。為了預防及降低此類攻擊所造成的傷害，慧智基因股份有限公司落實相關改進措施並持續更新，例如建置機器設備安全防護機制以防止內含惡意軟體的機器設備進入公司;強化網路運用虛擬化切分各級網段及內、外網之使用，員工不得使用私人之設備連接公司內部網路及禁止遠端桌面使用，若需由外部連線進入公司系統需申請、審核透過安全之 VPN 連線使用，並區隔主機、系統及使用者互相連結及防護，以避免惡意之連結與入侵，而在內部網路以內部防火牆與網路控管以防止惡意軟體跨機器設備及跨區擴散，對外網路之提供相關資訊服務主機連結使用外部防火牆控管防止惡意入侵，並加以運用全球資安情資分析防禦系統防護公司，以降低及減少外來之資安威脅、駭客攻擊、惡意連線及自動阻擋惡意軟體之入侵；依電腦類型建置端點防毒/護措施；導入先進的解決方案以偵測與處理惡意軟體;設計開發資安強化個人電腦供員工使用；以虛擬化建立公司私有雲並加強系統、異地資料備份以防遭受不當攻擊或損害時可及時恢復系統運作與資料正確存取，將公司損傷降至最低狀態；導入新技術加強資料保護；加強釣魚郵件偵測；所有之網路及相關系統連結之封包、訊息均予與監控及記錄以防止及及時防護公司之資訊安全；系統、機器設備均以統一以 Active Direrory 集中式目錄服

務做身份驗證與授權進行權限使用控管以達統一及易於管控，防止人員非法使用之入侵，增加 DLP 系統防止有心人士或無心之錯，所造成之機敏性資料外洩，以增加資料文件之安全性，導入 EDR 系統、SIEM 及建置 SOC 中心以 7*24 方式進行與第三方及政府進行資安聯防防制及監控並分析其有心人士之不正當電腦行為及時防範、制止並進行安全性處置；且因應行動裝置設備越加趨增使用以 MDM 系統加以控管、監測相關之設備使用與安全防護並做相關之安全處置；以縱向、橫向方式進行 360 度安全無死角之防護網並建立一個整合的自動化 資安維運平台，並定期執行員工警覺性測試及委託外部專家執行資安評鑑。

2.2 整體資安架構如下圖所示



3　科技改變及產業變化對公司財務業務之影響及因應措施：

3.1　本公司針對相關產業之科技脈動均能適時掌握並加以分析利用，並未因科技改變而有重大影響財務業務之情形。

3.2　資安風險評估分析：

3.2.1 資訊安全政策：

3.2.1.1 確保本公司資料、系統、設備及網路通訊安全，阻絕外界之入侵、破壞。

3.2.1.2 確保系統資訊帳戶存取權限與系統之變更均經過公司規定程序授權處理。

3.2.1.3 落實銷毀程序，已報廢之電腦儲存媒體應加以銷毀避免資料意外暴露外流。

3.2.1.4 監控資訊系統之安全狀態與活動紀錄，有效掌控並處理資訊安全事件。

3.2.1.5 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。

3.2.1.6 資安網路架構本公司資訊單位專責資訊安全，定期向資訊主管會報資安管理運作情形。公司之內部系統皆位於虛擬網路之中，外部網路受隔離無法直接進入，並且採用多重網路安全防禦系統，位於網路前端之防火牆、入侵防禦連線篩檢系統、郵件內安全控管系統負責過濾網路進出連線的內容，能防禦外部網路攻擊，並即時封鎖最新惡意軟體、有害之網路連結、垃圾電子郵件等威脅。位於內部之主機及端點皆由中控台佈署防毒軟體、EDR 及建置 SOC 中心，隨時更新病毒碼與即時辨識惡意行為特徵，能即時攔截病毒木馬蠕蟲、勒索軟體、文件夾帶之惡意程式等，有效降低被駭客功擊損害之風險且以 DLP 用以防範有心人士進行機敏性資料存取及外洩。

3.2.1.7 系統帳號生命週期管理與權限帳號管理依各業務範圍、職權分別設定使用者之帳號及權限，資料之存取皆需透過簽核流程經各權責主管申請並核准後始能使用與變更。使用者一旦離開原職務，立即撤銷該使用者之帳號與權限，以防範未經授權之使用。

3.2.1.8 資料存取紀錄稽核備存能紀錄系統檔案文件存取之軌跡記錄、往來郵件等資料，進行歸檔保存。報廢程序完成之電腦均執行硬碟拆解破壞以符合法規遵循的管理制度及資安政策。

3.2.1.9 資訊系統持續運作系統與文件皆採取每日、每週及每月之本地備份，每月之備份資料再傳輸到異地做異地備份，並每年定期執行系統資料復原測試演練，以確保資訊系統之正常運作及資料保全，可降低無預警天災及人為災害造成之資料損失風險。

3.2.1.10 資訊部門執行作業依本公司規定程序均能落實執行，確保資料完成性與安全性，風險評估結果尚屬良好，科技改變對公司資訊安全並無重大不利影響且無重大營運風險。

3.3 本公司近年投入資通安全管理之費用項目，請參考附件檔案。