和益化學工業股份有限公司

資訊安全管理計畫

壹、目的

為確保本公司資訊處理、傳送、儲存及流通之安全作有效之管制，擬訂本計畫規範資訊安全管理措施。

貳、通則

本計畫所定資訊安全措施，綜合考量各項資訊資產之重要性與價值，及因人為疏失、蓄意破壞或自然災害等風險，致本公司資訊資產遭不當使用、洩漏、竄改、破壞等情事，影響及危害業務之程度，採行與資訊資產價值相稱及具成本效益之管理、作業及技術等安全措施。

參、就下列項目訂定資訊安全管理計畫實施，並定期評估實施成效：

一、資訊安全政策訂定

(一)所訂定之資訊安全管理政策，以書面、電子或其他方式告知本公司暨所屬員工及提供資訊服務之廠商共同遵行。

(二)資訊安全管理政策實施後，資訊安全專責單位須不定期評估，以反映公司規定、技術及業務等最新發展現況，確保資訊安全實務作業之有效性。

(三)每年應鑑別應遵守之法令及契約要求。

(四)遵循上市上櫃公司資通安全管控指引。

二、資訊安全權責分工

(一)資訊安全政策、計畫及技術規範之研議、建置及評估等事項，由資訊安全專責單位負責辦理。

(二)資訊機密維護及稽核使用管理事項，由督導單位會同相關單位負責辦理。

(三)資訊安全推動組織定期向董事會或管理階層報告資訊安全執行情形。

三、人員管理及資訊安全教育訓練

(一)對資訊相關職務及工作人員，應進行安全評估，並依其任務之適任性進行必要之考核。

(二)對可存取機密性與敏感性資訊或系統之人員，及因工作需要須配賦系統管理權限之人員，應加強評估及考核。

(三)資訊安全專責單位得依業務及資訊等不同工作類別，視實際需要定期辦理資訊安全教育訓練及宣導，建立員工資訊安全認知，提升資訊安全水準。

(四)負責資訊安全之主管及人員，每年接受資訊安全專業課程訓練。
(五)對負責重要資訊系統之管理、維護、設計及操作之人員，應妥適分工，分散權責，並視需要建立人力備援制度。
(六)各組督導人員,須負責督導所屬員工之資訊作業安全,防範不法及不當行為。

四、電腦系統安全管理

(一)辦理資訊業務委外作業,須以契約與廠商約定資訊安全責任及保密規定,要求廠商遵守並定期考核。
(二)對於系統變更作業或更新功能,由資訊單位執行控管並詳細記錄,以備查考。
(三)各系統伺服器所存放之機房須由資訊單位管理，並嚴禁無關人員進出。

五、網路安全管理

(一)各系統伺服器與外界網路連接之網點,須設立防火牆以控管外界與內部網路之資料傳輸及資源存取,必要時應以代理伺服器等方式提供外界存取資料。
(二)開放外界連線作業，須由資訊單位事前與連線單位簽訂契約或協定，限制系統可運作之權限，並明定應遵守之資訊安全規定、程序及應負之責任。

六、系統存取控制管理

(一)登入各作業系統時，依各級人員執行工作所必要之系統存取權限，由資訊單位系統管理人員設定應賦予權限之帳號與密碼,並按照「密碼變更管理原則」管理。
(二)對離(休)職人員,立即取消使用各項資訊資源所有權限,並列入人員離（休）職之必要手續。
(三)對於資料存取落實職責分工，僅提供相關負責人員必要之系統存取權限。
(四)僅允許使用者依據各部門分派任務與業務之功能需要,授權資料存取行為。

七、系統發展及維護安全管理

(一)開發或委外發展系統，須在系統開發初期階段，即將資訊安全納入考量；系統之維護、更新、上線執行及版本異動作業,應予安全管制,避免不當軟體、暗門及電腦病毒等危害系統安全。
(二)對合作夥伴之軟硬體系統建置及維護人員,應規範及限制其可接觸之系統與資料範圍，並嚴禁資訊單位核發長期性之系統辨識碼及通行密碼。
(三)對合作夥伴或系統維護人員基於實際作業需要,資訊單位得核發短期性及臨時性之系統辨識及通行密碼供使用。但使用完畢後應立即取消其使用權限。
(四)因應個資法，個人資料做必要之權限控管或加密處理(詳參第十二條)。
(五)系統應記錄監控影響個人資料機密性的事件供稽核、檢視分析，以發現不當或不尋常的活動跡象，並採取適當措施。

八、資訊資產安全管理

(一)為防斷電時造成系統毀視或資料流失，主機房須配置不斷電系統因應斷電時，有足夠時間做存檔與正常關機。

(二)不使用來源不明之磁片或隨身碟。

(三)不使用非經許可之軟體程式光碟。

(四)電腦設備須裝置防毒軟體（如 Sophos），並開啟於即時掃描狀態。

(五)個人重要文件如與個資及公司營業秘密有關者，存檔或需分享時，須養成加密碼保護習慣。

(六)資訊設備辦理移轉異動前應將機密性、敏感性資料及授權軟體予以移除或實施安全性覆寫。資訊設備報廢前，應將儲存之資料及軟體移除後並做實體破壞。

(七)定期辦理設備、系統元件、資料庫系統及軟體安全性漏洞修補。

(八)資訊系統開發及維護相關文件資料，定期彙整備份保管。

(九)定期盤點資訊系統，並建立核心系統資訊資產清冊，依據資產清冊辦理資訊安全風險評估。

九、實體及環境安全管理

(一)資訊單位就系統伺服器主機設備安置於主機房，並由資訊單位專責管理，並管制非相關人員隨意進出。

(二)主機房須設置空調控制。

(三)若非資訊單位人員或維修人員，不得自行拆卸電腦機殼及更換內部零組件。

十、作業永續運作計畫管理

(一)為因應各種人為及天然災害造成業務運作受影響，資訊人員須於每星期三、五定期作完整備份，並每日作異動資料之備份。(所作之完整備份資料須異地存放)。

(二)各單位人員所建立之資料檔須定期存放於伺服器中並由資訊人員作備份。

(三)設置備援電腦於第二場所，在緊急狀況時，即時啟動。

(四)各單位人員在發生資訊安全事件時，應依據資訊安全事件通報程序通報。

(五)若資訊安全事件判斷為重大事件,依據資訊安全事件應變處置及通報作業程序發布重訊。

十一、個人電腦使用辦法

(一)為尊重智慧財產權，不得使用非法軟體及光碟。

(二)禁止任意下載或安裝來路不明、違反法律（如版權、智慧財產權等）或與業務無關的電腦軟體。

(三)使用外來檔案及隨身碟，應先掃毒。

(四)禁止於上班時間閱覽不當之網路（如暴力、色情、賭博、駭客、惡意網站、

釣魚詐欺、傀儡網路等）及瀏覽非公務用途網站，亦不可利用網路資源進行與工作內容無關之串流媒體、MP3、圖片、檔案等網路上的傳輸。

(五)電腦內重要資料文件應定期備份，避免資料毀損。

(六)為確保資訊安全，禁止使用公司電腦收取個人郵件。

(七)下班時，應先行關機始得離去，電腦關機應依正常程序操作。

十二、電腦處理個人資料保護控制作業

個人資料檔案件建置在個人電腦硬式磁碟機上者,資料保有單位應在該個人電腦設置開機密碼、螢幕保護程式密碼及相關安全措施。

十三、罰則

若發現同仁違反上述相關規定，資訊管理單位將逕行限制該同仁之使用範圍，包括但不限於限制連結部分網站、鎖定電子郵件信箱、取消即時通訊軟體使用之權限等，並呈報上級主管及總經理。情節重大者，由公司進行懲戒，若造成公司損害，將追究違反者法律責任。

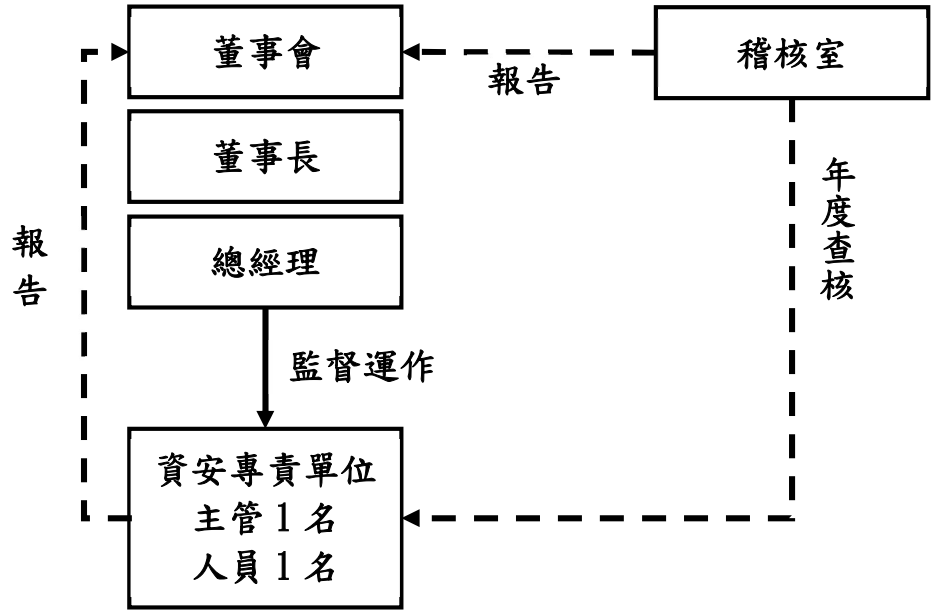
十四、本計畫經董事會核准後實施，修正時亦同。

十五、本計畫於 103 年 10 月訂定實施，第一次修訂於 109 年 9 月，第二次修訂於 112 年 11 月，第三次修訂於 114 年 11 月 12 日。

附件:

1. 資安組織架構及執掌
2. 資訊安全事件通報程序

1.資安組織架構



資訊安全業務職掌

1.擬訂資訊安全計畫、執行資訊安全作業。
2.負責與推動資訊安全之資訊資產風險評鑑與風險處理計畫。
3.確認資訊資產皆有適當的管理，同時符合風險管理的政策與程序。
4.負責規劃及實施全體同仁資訊安全宣導教育。
5.對資訊安全管理狀況進行預警、防禦、監控等規劃。
6.負責監督資訊安全維護計畫、資訊安全事件通報及應變管理程序。
7.提供年度成果與建議予董事會。

2. 資訊安全事件通報程序