美吾華股份有限公司

資訊安全政策

第一條：目的

為維護資訊資產之機密性、完整性、可用性及適法性，資訊系統、設備及網路的安全運作，避免遭受內、外部蓄意或意外之威脅、破壞及盜用，確保公司永續經營，特訂定資訊安全政策作為最高指導原則。

第二條：範圍

凡本公司全體員工、客戶、委外或合作廠商、第三方人員以及所有相關資訊資產之安全管理，應依資訊安全政策處理。

第三條：資安專責單位

本公司由資訊單位負責資訊安全制度之規劃、監控及執行資訊安全管理作業，由資訊單位主管擔任資安專責主管，一名專業資訊人員擔任資安專責人員。

第四條：資訊安全權責與教育訓練

一、依角色及職能為基礎，針對不同層級工作人員，視實際需要辦理資訊安全教育訓練及宣導，促使員工瞭解資訊安全的重要性，各種可能的安全風險，以提高員工資訊安全意識，遵守資訊安全規定。

二、對留職停薪及離職人員，依據人員留職停薪及離職之處理程序辦理，並立即取消各項系統登入及存取權限。

第五條：資訊安全作業及保護

一、建立處理資訊安全事件之作業程序，並賦予相關人員必要的責任，以便迅速有效處理資訊安全事件。

二、建立資訊設施及系統的變更管理通報機制，以免造成系統安全上的漏洞。

三、依據電腦處理個人資料保護法之相關規定，審慎處理及保護個人資訊，不會任意對其他第三者揭露。

四、建立系統備援設施，定期執行必要的資料、軟體備份及備援作業，以備發生災害或儲存媒體失效時，可迅速回復正常作業。

五、每年至少一次審視各項資安漏洞公告，另視事件風險程度不定期審視，如:國家資通安全研究院之漏洞資訊公告網站，評估資安漏洞影響範圍，依據系統變更管理機制，提出並進行相應的系統修正措施。

六、定期對全公司之資訊資產辦理資訊安全風險評鑑如附件，並留存紀錄。

第六條：網路安全管理

一、與外界網路連接之網點，設立防火牆控管外界與內部網路之資料傳輸及資源存取，並執行嚴謹的身分辨識作業。

二、機密性及敏感性的資料或文件，不存放在對外開放的雲端系統中，極機密性文件不以電子郵件傳送。

三、定期對內部網路資訊安全設施與防毒進行查核，並更新防毒系統之病毒碼，及各項安全措施。

第七條：系統存取控制管理

一、視作業系統及安全管理需求訂定通行密碼核發及變更程序並作成記錄。

二、登入各作業系統時，依各級人員執行任務所必要之系統存取權限，由系統管理人員設定賦予權限之帳號與密碼，並定期更新。

第八條：公司資訊安全水準提升

應提升本公司資訊安全管理能力，資安專責主管及人員應每年參加資訊安全訓練課程。

第九條：業務永續運作計畫管理

評估各種人為及天然災害對正常業務運作之影響，訂定ERP、BI系統緊急應變及回復作業程序，並視需要調整更新計畫。

第十條：本辦法經董事長核准實施，修訂時亦同。首次訂定於一〇四年六月十日。第一次修訂於一一〇年六月十日。第二次修訂於一一一年三月二十九日。第三次修訂於一一二年三月一日。第四次修訂於一一二年十一月二十三日。