美吾華股份有限公司
資訊安全風險管理架構

本公司資訊安全之權責單位為資訊部，依據專業分工編制有資訊安全專責主管及資訊安全專責人員共2人，負責訂定內部資訊安全政策、規劃暨執行資訊安全作業與資安政策推動與落實。

稽核室依據「公開發行公司建立內部控制制度處理準則」規定，將「資通安全檢查之控制」納入年度稽核計劃，並依所排定期程進行查核作業，進行資訊安全稽核工作，包含內部稽核與外部稽核。若有發現缺失／風險，即請受查單位及協同作業單位進行檢討，提出具體改善計劃及時程，定期追蹤改善進度，以落實公司資訊安全政策。

本公司目前資訊安全相關具體執行措施如下：

項目	具體管理方式
防火牆及入侵防禦	●防火牆設定連線規則。 ●自動偵測駭客入侵行為並即時攔阻 ●如有特殊連線需求，需提出電腦作業需求申請單開放。 ●監控分析防火牆數據報告。
使用者上網控管機制	●使用者上網需經過身份驗證 ●使用自動網站防護系統控管使用者上網行為。 ●自動過濾使用者上網可能連結到有木馬病毒、勒索病毒或惡意程式的網站。
防毒軟體	●使用知名防毒軟體，並自動更新病毒碼，降低病毒感染機會。
作業系統更新	●作業系統透過 WSUS 自動更新，並定期追蹤更新情況，因故未更新者，由資訊部協助更新。
郵件安全管控	●具備郵件掃描威脅防護機制，在使用者接收郵件之前，事先防範不安全的附件檔案、釣魚郵件、垃圾郵件，及擴大防止惡意連結的保護範圍。 ●個人電腦接收郵件後，防毒軟體也會掃描是否包含不安全的附件檔案。
網站防護機制	●定期進行弱點掃描，並定期更新網站主機系統，修補主機漏洞，防止駭客入侵。
資料備份機制	●重要資訊系統資料庫皆設定每日完整備份、每小時差異備份，主機作業系統每週完整備份。
異地存放	●伺服器與各項資訊系統備份檔，分開存放於分公司。
重要檔案存放	●公司內各部門重要檔案上傳 NAS 存放，由資訊部統一備份保存。
系統監控	●網管系統集中監控機房設備及網路連線運作狀況，發現異常時通知資訊人員。

本公司每季進行一次資安漏洞檢視，並將檢視結果呈報總經理，資安事件通報流程如下：