大華建設股份有限公司
資訊安全政策及管理方案

一、資訊安全風險架構

本公司資訊安全之權責單位為總經理室所轄之資訊組，於 112 年 10 月 27 日配置專責主管及專責人員各一名，負責統籌資訊安全及相關事宜，並定期進行內部資訊安全檢查及人員資訊安全宣導。

112 年無重大資訊安全事件發生，報告 112/11/10 董事會。

二、資訊安全政策

（一）目的

為強化資訊安全管理，確保資訊資產的機密性、完整性及可用性，以維護資訊系統正常運作，特制定此資訊安全管理政策。

（二）範圍

維持本公司資訊作業正常運作之環境、硬體、軟體、資料及人員。

（三）目標

避免資訊系統遭受來自內、外部人員不當使用或蓄意破壞、或當已遭受不當使用、蓄意破壞等緊急事故時，能迅速應變處置，並在最短時間內回復正常運作，降低該事故可能帶來之公司損失及營運風險。

三、資訊安全管理措施

本公司尚未投保資安險，相關具體預防措施如下:

（一）網路安全管理

1.為確保公司資訊安全，設置防火牆，隔絕網路病毒、防止入侵攻擊、阻擋惡意連線及上網內容過濾避免進入惡意網站。

2.各辦公室連線公司使用應用系統以 VPN 方式連線，避免資料傳輸過程中遭到非法擷取。

（二）系統存取控制:

1.公司內各應用系統的使用，皆透過程式授權書申請，經權責主管核准後，由資訊組建立帳號並依據程式授權書所申請的功能開放權限。

2.人員職務異動或離職時，須會辦資訊組人員，進行各系統權限修正或刪除帳號。

3.每年列印各使用者權限明細表交由各使用單位審查其系統使用權限與職責相符。

（三）病毒防護與管理

1.伺服器與各單位電腦設備皆安裝防護軟體，不可任意關閉或移除，防毒軟體病毒碼自動更新，確保能阻擋最新型電腦病毒。

2.電子郵件服務提供信件掃毒功能及信件過濾功能，防堵病毒或垃圾郵件進入使

用者電腦。

（四）確保系統的永續運作

1.建置備份管理系統，設定每日備份，定期離線備份，一份備份媒體保留在機房，另一份備份媒體異地存放。

2.系統發生異常事件無法運作時，依系統復原程序將系統回復正常運作。

（五）電腦設備安全管理

1.電腦主機，各應用伺服器等設備設置於專用機房內，機房門禁由資訊組人員負責管理，非權責人員進出時須資訊組人員陪同。

2.機房內有獨立空調，以維持電腦設備於適合的溫度環境下運轉。

3.機房內配置不斷電系統以確保供電穩定，以防設備受損造成電腦應用系統無法運作。

(六)企業入口網站導入

1.本公司刻正執行企業入口網站（EIP）及電子簽核系統之導入，冀由 EIP 統籌資訊存儲及傳遞、電子簽核取代傳統紙張作業，俾達資訊指定傳遞及外洩防免之效，並同時確保資料安全性，避免資料遭受不當使用或蓄意破壞。

2.本公司正在確認相關辦法與廠商徵選，2023 年會議次數共 4 次。