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管理部所轄之資訊組，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。

113 年無重大資訊安全事件發生，報告 113/11/12 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.目前已進行異地備份作業，以確保資料的安全與完整性。每日透過連線備份至合作廠商的機房進行數據回存，該機房配有不斷電系統，能有效保障資料在異常情況下的完整性。

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：

正式啟動企業入口網站（EIP）及電子簽核系統(BPM)的導入工作。EIP 系統的實施旨在統一資訊存儲和傳遞管理，透過電子簽核取代傳統紙本流程，實現無紙化的高效作業流程。

1.加強資訊傳遞及外洩防範：透過 EIP 系統的集中管理，資料僅限授權人員存取，降低資料外洩風險。

2.資訊安全與合規：系統具簽核、權限管理及操作紀錄等功能，確保資料的真實性與安全性。

3.流程透明化與操作追溯：審核流程數位化，所有簽核歷程透明度，讓管理層能夠更清楚掌握並快速應對任何異常情況。

4.執行情形：

電子簽呈系統內部會議-3 次（討論企業入口網站（EIP）及電子簽核系統的推行進度與內部規範相關執行方式。）

（七）Active Directory（AD）帳號控管：

所有電腦納入 Active Directory（AD）帳號控管，以進一步加強內部資訊安全及操作規範，保障公司數據資產的安全性。

1.集中化管理：透過 AD 系統統一管理全公司員工的帳號及密碼，方便管理層對使用者權限的即時設定和調整，確保帳號使用符合工作需求並及時更新。

2.提升資料安全：在 AD 系統中，所有電腦均經過身份驗證及授權，未經授權的帳號無法使用公司電腦，避免非公司人員的非法登入，從而減少外部入侵的風險。

3.執行情形：

(1)AD 帳號建置內部會議-2 次（討論 AD 帳號建置及執行流程，帳號系統整合與安全管理方案。）

(2)電子簽呈系統內部會議-3 次（討論企業入口網站（EIP）及電子簽核系統的推行進度與內部規範相關執行方式。）

(3)電子簽呈系統外部會議-2 次（與系統供應商及相關廠商確認技術支援與系統整合的細節。）

（八）異地備份

1.預計每年都將進行資料回存確認作業，今年的資料回存確認預計在 11 月 20 日執行，屆時將於測試機檢查備份資料是否完整。透過此措施，確保在發生意外時，公司能持續穩定運行。

2.執行情形：

(1)異地備份內部會議-2 次（討論異地備份作業流程與應急演練的強化，確保資料安全儲存與恢復能力。）

(2)異地備份外部會議-2 次（與備份合作廠商確認資料傳輸的穩定性及不斷電服務系統（UPS）執行方式。）