三發地產股份有限公司
資訊安全風險管理

111 年 11 月 8 日董事會報告

資訊安全風險管理架構

本公司資訊安全之權責單位為總經理室/資訊組，負責規劃與制訂資訊安全政策並推動執行相關事務，同時向員工宣導資訊安全重要性以提升資安意識。

本公司稽核室為資訊安全執行之督導查核單位，定期進行資訊安全查核，如發現缺失則立即要求受查單位提出改善計畫，且定期追蹤改善成效，以確保公司資訊安全之有效性，同時每年向董事會報告執行狀況。

資訊安全政策

- 建立安全且穩定的網路架構
- 維持資訊系統永續運作
- 確保系統與資料之機密性與完整性
- 資訊人員參與資訊安全相關培訓課程
- 定期辦理資安宣導與教育訓練

資訊安全具體管理方案

- 資訊機房安全管理
  - 設置門禁指紋機管制僅資訊人員得進出機房；非資訊人員進出機房需填寫「機房進出管制表」並由資訊人員陪同
  - 設置不斷電系統以確保機房設備不會因供電異常造成不正常關機，進而導致系統與資料損毀之風險；且安裝網管卡提供機房伺服主機關機自動化機制，避免斷電時間過長備用電力耗盡或夜間無人值守時發生未預警斷電之情況
  - 除大樓空調系統外，機房內部備有獨立空調，維持資訊設備於適當溫度環境下運作
- 網路安全管理
  - 定期進行防火牆設備韌體及阻擋政策設定之更新，防止外部惡意入侵與破壞
  - 各項網路資訊服務均依據資訊安全政策予以監控
  - 每日透過「機房工作日誌」記錄並監控內外部異常活動
  - 同仁於遠端欲存取公司內部資源，須透過「應用系統權限申請單」申請 VPN 帳號，透過 VPN 的安全連線後始能登入使用，所有連線均留有紀錄可供稽查

- 內控與流程管理
  - 新進人員填寫「網路帳號申請單」經權責主管核准後交付資訊組開設帳號並告知郵件使用之規定。員工離職時均依離職程手續會辦資訊單位，資訊單位將離職人員帳號刪除。
  - 使用資訊系統及網路儲存伺服器需提出「應用系統權限申請單」申請，經權責主管核准後交付資訊組設定權限後始可操作存取，防止未經授權修改或使用
  - 資訊人員異動或離職時，各系統管理密碼均需立即進行更換，確保系統資訊安全
  - 定期彙整各資訊系統及檔案之人員存取權限向權責主管進行報告並評估檢討合適性
  - 定期由稽核室進行資訊循環、資訊安全查核，確保資安管理措施之落實度並持續精進
  - 定期向董事會報告資訊安全管理計畫之執行情況，並檢討改進

- 病毒防護與管理
  - 伺服器與同仁終端電腦內均安裝有防毒軟體，病毒碼採自動更新方式，確保能偵測並阻擋最新型的病毒入侵，同時透過雲端控制台管理所有內容與監控
  - 電子郵件伺服主機配置有郵件防毒、與垃圾郵件過濾機制，防堵病毒或垃圾郵件進入使用者端電腦中

- 資安宣導與教育訓練
  - 提醒宣導：要求同仁定期更換系統密碼，以維帳號安全
  - 資安宣導：每年不定期對內部同仁實施資訊安全相關的教育訓練課程

風險管理措施

- 系統備份

  建置異機與異地之差異與完整備份計畫,對於每日重要之資訊服務建置 High Availability 即時備援機制，以確保系統與資料的安全並提供不中斷資訊服務

- 災害復原演練

  透過備用虛擬伺服主機進行災難復原測試與演練，選定系統及資料庫還原日期基準點後，將備份媒體回存於備用虛擬伺服主機，再由使用單位確認回復資料的正確性，確保備份媒體的正確性與有效性

執行情況

本公司目前無重大資安事件導致營業損害之情事，將持續落實資訊安全管理政策目標並持續精進。