名軒開發股份有限公司

資訊安全政策

修訂日期：112年10月30日

本公司資通安全之權責單位為資安管理室，負責訂定公司資通安全政策，規劃資訊安全措施，並執行相關之資訊安全作業，資安管理室設置資訊安全專責主管一位並由資訊課主管擔任，資安管理室下轄資安執行組及資安稽核組分別設資訊安全專責人員一名由資訊課工程師擔任，稽核專責人員由稽核室主管擔任。

一、資訊安全管理目標

1.維持各資訊系統持續運作

2.防止駭客、各種病毒入侵及破壞

3.避免人為疏失、防止人為意圖不當及不法使用

4.防止機敏資料外洩 ，機敏資料包含客戶個資及公司人員個資。

二、資訊安全設施與管理方式

1.電腦設備安全管理

(1)本公司系統主機、各應用伺服器等設備均設置於專用機房。

(2)機房內部備有獨立空調，維持電腦設備於適當的溫度環境下運轉。

(3)機房主機配置不斷電與穩壓設備，避免台電意外瞬間斷電造成系統當機，或確保臨時停電時不會中斷電腦應用系統的運作。

2.網路安全管理

(1)與外界網路連線的入口，配置企業級防火牆，並搭配中華電信資案艦隊防護服務，阻擋駭客非法入侵。

(2)各案現場與公司點對點的連線作業，使用VPN資料加密的方式，避免資料傳輸過程遭受非法擷取。

(3)配置上網行為管理與過濾之資安系統，控管網際網路的存取，可屏蔽訪問有害或政策不允許的網路位址與內容，強化網路安全並防止頻寬資源被不當占用。

3.病毒防護與管理

(1)伺服器與同仁終端電腦設備內均安裝有端點防護軟體，病毒碼採自動更新方式，確保能阻擋最新型的病毒，同時可偵測、防止具有潛在威脅性的系統執行檔之安裝行為。

(2)電子郵件伺服器配置有郵件防毒、與垃圾郵件過濾機制，防堵病毒或

垃圾郵件進入使用者端的PC。

4.系統存取控制。

(1)同仁對各應用系統的使用，透過公司內部規定的系統權限申請程序，經權責主管核准後，由資訊課建立系統帳號，並依所申請的功能權限開放授權存取；其包含員工個人資料之鼎新人力資源管理系統及存有客戶個資的高益AHM業務系統。

(2)帳號的密碼設置，規定適當的強度、字數，並且必須文數字、特殊符號混雜，才能通過。

(3)同仁辦理離(休)職手續時，必須會辦資訊課，進行各系統帳號的刪除作業。

5.確保系統的永續運作。

(1)系統備份：備份資料於電腦機房及銀行保險箱均另各存一份複本，以確保系統與資料的安全。

(2)災害復原演練：各系統每年實施一次演練，選定還原日期基準點後，由備份媒體回存於系統主機，再確認回復資料的正確性，確保備份媒體的正確性與有效性。

(3)租用電信公司兩條數據線路，透過頻寬管理設備，兩線路並聯互為備援使用，確保網路通訊不中斷。

6.資安宣導與教育訓練

(1)提醒宣導：每月一次不定期以電子郵件方式通知全體員工最新資安資訊及提醒注意事項，系統設定自動要求同仁到期更換系統密碼，以維帳號安全。

(2)講座宣導：每年對內部同仁實施資訊安全相關的教育訓練課程。