萬在工業股份有限公司

資訊安全風險管理架構

資安風險管理架構

1. 資訊安全之權責單位為資訊室，負責規劃、執行及推動資訊安全管理事項，各業務相關單位配合執行，以確認本公司資訊安全管理運作之有效性。
2. 本小組負責制定資通安全管理政策，定期檢討修正。
3. 由稽核室為資訊安全監理之查核單位，若查核發現缺失，立即要求受查單位提出相關改善計劃且定期追蹤改善成效，以降低內部資安風險。

資通安全對象與範圍

對象：包括員工，客戶，供應商和股東以及營運相關資訊軟硬體設備。

範圍：為確保本公司資通安全，制定相關規章制度，應用技術和數據安全標準制定， 並納入管理運作體系，以保障員工，供應商和客戶進行業務接洽時之隱私權保護與資通安全維護。

資訊安全政策

1. 維持各資訊系統永續運作。
2. 防止駭客、各種病毒入侵及破壞。
3. 防止人為意圖不當及不法使用。
4. 防止機敏資料外洩。
5. 避免人為疏失意外。
6. 維護實體環境安全。

資訊安全具體管理方案

1. 電腦設備安全管理
   (1) 本公司電腦主機、各應用伺服器等設備均設置於專用機房，機房保留進出紀錄存查。
   (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；並放置藥劑式滅火器，可適用於一般或電器所引起的火災。
   (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，阻擋駭客非法入侵。
   (2) 同仁由遠端登入公司內網存取 ERP 系統，必須申請 VPN 帳號，透過 VPN 的安全方式始能登入使用，且均留有使用紀錄可稽查。
   (3) 配置上網行為管理與過濾設備，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，由資訊室建立系統帳號，並經各系統管理員依所申請的功能權限做授權方得存取。
   (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，資訊室依人資離職通知，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：建置分地備份系統，採取日備份機制，異地電腦機房各存一份備份資料，且異地建置備援系統，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，再由使用單位書面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：要求同仁定期更換系統密碼，以維帳號安全。
   (2) 資安宣導：提供資訊安全實例文件給同仁參考。

資通安全的資源投入

1. 資通安全由本公司資訊室負責，共設置 2 人，並配置資安專責主管 1 名及 1 名資安專責人員，主係確保資通安全管理制度之運作，鑑別資通安全管理制度之內、外部議題及利害相關團體對本公司之資通安全要求與期望。
2. 持續提升資安人員專業培訓，確保作業人員皆符合資通安全標準。
3. 加入 TWCERT/CC 等資安聯防組織，強化資安聯防體系與威脅情資共享。
4. 本公司 2024 年無重大資通安全危害事件。