

資訊安全具體管理方案

➤ 網路活動檢視

- 一、網路活動皆透過委外資安中心 24 小時持續偵測，針對重大資安風險立即進行處理，每季提供中低風險資安事件進行改善。
- 二、設置防火牆與安全加密連線通道(SSL VPN)，管制設備網路介面卡不允許非法設備網路連線。

➤ 裝置安全

- 一、公司個人電腦與伺服器均安裝防毒軟體，一人一帳號，並利用網域伺服器(Active Directory) 管控認證，每三個月強制更換密碼。
- 二、架設 Windows Server 更新服務(WSUS)進行公司個人電腦與伺服器軟體自動更新。

➤ 資料安全

- 一、公司個人電腦 USB 埠預設關閉，開放需另外申請核准。
- 二、電腦機房進出均有門禁管制，重大系統定期備分，資料庫每年進行災難復原演練。

➤ 郵件管控與社交工程演練

- 一、郵件系統皆透過垃圾郵件伺服器進行過濾，並設定黑白名單機制。
- 二、不定時配合集團進行郵件釣魚測試，並依嚴重性提報改善。
- 三、每年舉辦資安教育訓練，不定期進行資安公告，提升員工資訊安全觀念。

資通安全風險與因應措施

- 加強例行性資安維運工作及採購新的軟硬體資安設備。
- 強化資安事件偵測監控與通報機制，導入外部轉業資安顧問協助，成立資訊安全委員會定期召開會議。
- 每季實施資訊安全教育訓練，每月實施電子郵件社交工程演練。

- 五大資訊安全管理措施：

- 一、辨識(Identify)

- 審視資訊環境及關鍵資源、系統與服務，建構符合日常營運的風險管理策略，包括資訊資產盤點及風險評鑑，並透過內部稽核及外部稽核以發現可能潛在之風險進而改善。

- 二、防禦措施(Protect)

- 建置相應的防禦措施，確保關鍵資源、系統與服務不受資安事件影響，包括身分與存取管理、端點/防毒防護與防火牆等。

- 三、偵測威脅(Detect)

- 建置資安事情即時偵測與告警機制，包括垃圾郵件管理系統、入侵偵測系統、資安監控中心(Security Operations Center, SOC)

- 四、事件應變(Respond)

- 制定資通安全事件通報及應變管理，當事件發生時期能迅速完成損害控制或復原作業，降低資訊安全事件對中鋼構公司之衝擊影響。

- 五、災後復原(Recover)

- 資訊處有完整的備份 SOP，當發生資料損毀時，可由備份程序執行災難還原。在預計的時間內，將資料還原至前一個的備份點，將生產製程的影響降至最低。