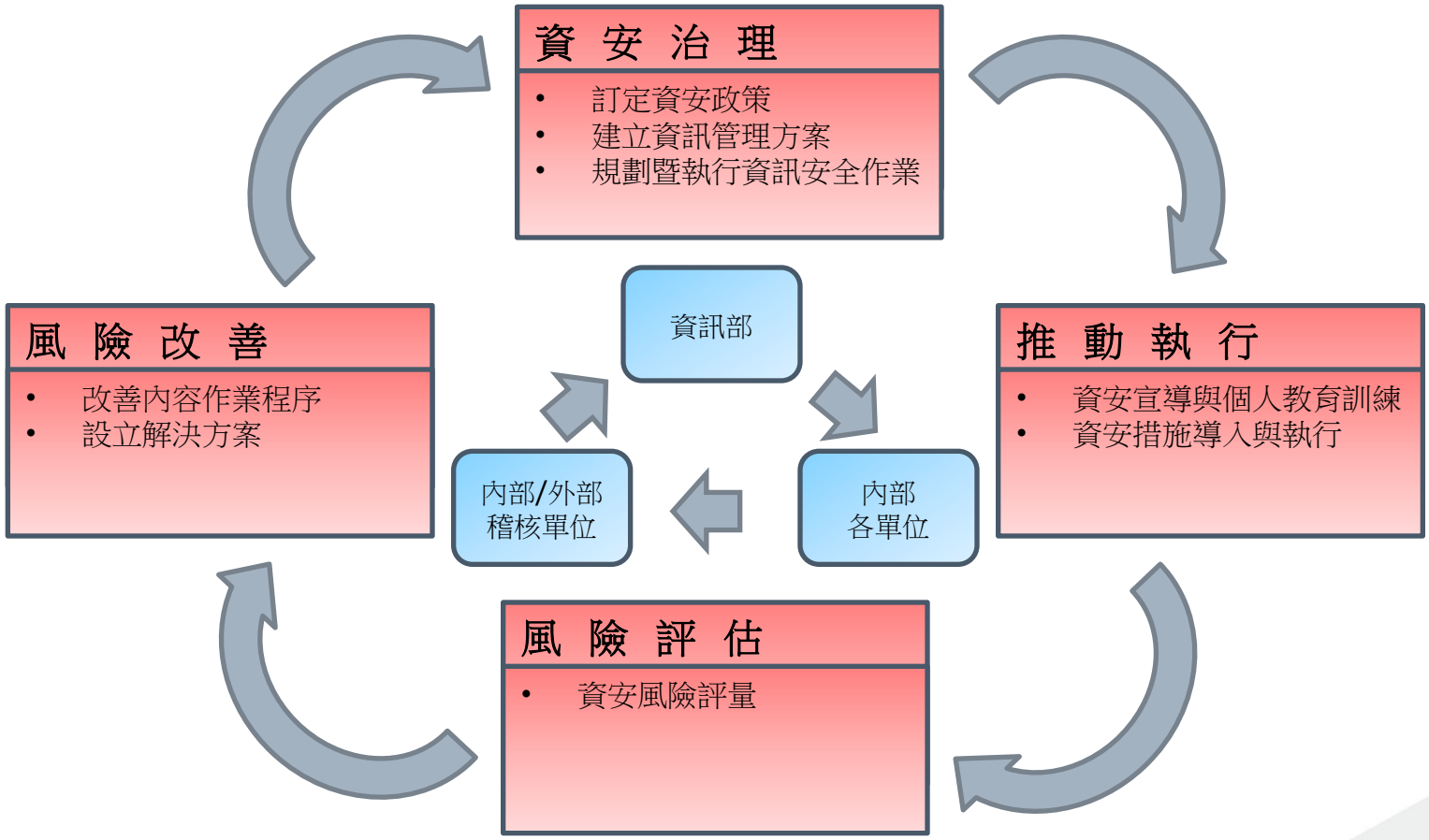
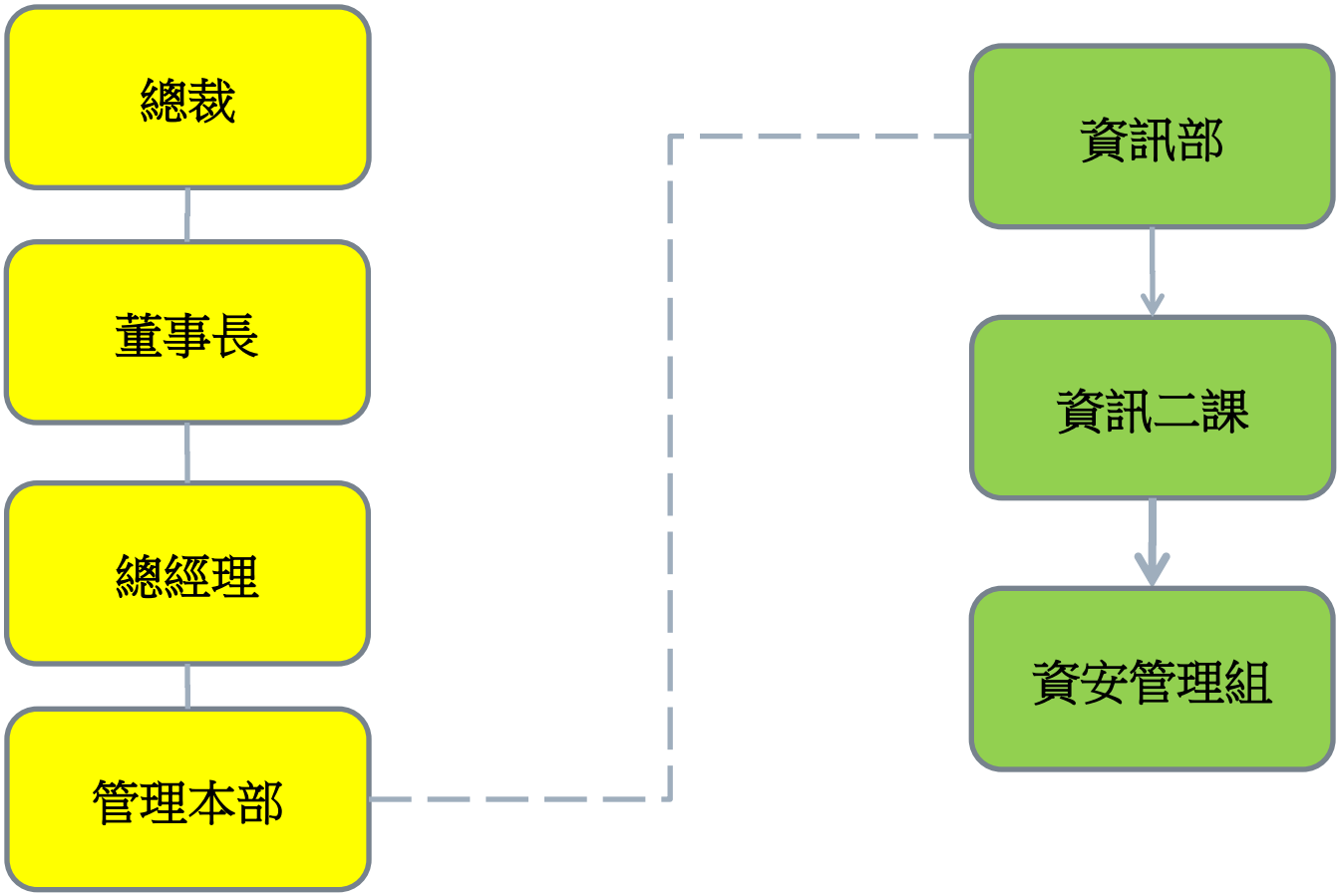
- 資訊安全風險管理架構、安全政策及具體管理方案於2025年08月08日向董事會報告
- 建置資通安全風險管理架構



資通安全組織與架構

- 資通安全組織與架構(成立資安專責單位、設置資安主管)



備註：
2022年/04月 依規定公告申報 資安主管與資安專責人員1名

資通安全政策

- 建大工業資通安全政策：為維護整體資訊安全，強化各項資訊資產之安全管理，確保其具機密性、完整性、可用性，以因應業務運作需要。
  - 遵守政府法令規定：確實遵守各項相關法令規章及資訊安全規範, 致力維護各項資訊之安全，以滿足企業穩定運作。
  - 適時修訂資安管理辦法：透過企業內部與外部的安全威脅與風險評估之過程，適時修訂資安管理辦法，以排除風險。
  - 強化員工資安意識：全面進行資訊安全教育之訓練，強化全員資訊安全能力與認知，建立企業資訊安全之環境。

KENDA

資通安全政策

- 維護電腦資料之機密性、可用性及完整性：完整資料之備援/備份機制，以確保企業內電腦資料，隨時可以有效的使用。
- 掌握或引進最新資安產品：保持與資安廠商聯繫，獲取最新資安防護知識，必要時引進新資安產品，維持企業資安系統與外界技術同步。

資通安全具體管理方案

- 資通安全管理方案
  - 資訊機房安全管理
  - 密碼管理
  - 資訊技術防護
  - 資訊檔案管制
  - 資訊備份/備援與復原
  - 資訊安全管理宣導
  - 違規行為處置
  - 定期稽核

（各項方案說明如下）

資通安全管理方案

- 資訊機房安全管理
  - 資訊機房平時上鎖，門禁管制卡由網路管理員管理，並妥善存放。
  - 資訊人員機房處理的事項，記錄於相關記錄本內，廠外人員因業務需進入時須資訊人員陪同，同時於訪客入出機房記錄，登錄進入機房人員姓名，進出時間及工作摘要。
  - 機房溫度保持28度C以下，濕度保持於30%~65%間，值日生記錄機房溫度、濕度空調設備需有二套，交互替換，內有保全及緊急照明設備，每周檢查一次。

KENDA

資通安全管理方案

- 緊急應變，至少半年一次教育訓練，熟悉操作。
- 員林廠、雲林廠、全球研發總部均設置資訊機房，斗六廠及台北辦公室無設置資訊機房。

資通安全管理方案

密碼管理

- 個人電腦閒置超過15分鐘會自動啟動螢幕保護程式並上鎖，個人電腦禁止將檔案寫出至外接儲存設備，若有業務需求提出MEMO單，經由協理級以上主管同意後，才能將檔案寫出。
- 執行特殊業務或機密性質高的同仁，AD密碼長度設定須達7碼，且強迫英數字，windows密碼90天有效期限到期、UNIX ERP 13周有效期限到期，系統自動提醒。
- 訂定程式及資料存取規定。

KENDA

資通安全管理方案

資訊技術防護

- 本公司資通安全檢查之規定，訂有網路安全的防設程序來防止竄改或修改商業資料：
- 使用網路防火牆(Fire Wall)並專人負責。並開啟下列功能：

1. 網頁過濾：過濾惡意程式網址。
2. 入侵防護：過濾可疑封包，網路傳輸中是否含有惡意攻擊封包。
3. 殭屍網路防護：能透過分析其網路通訊協定而發現惡意軟體。
4. 病毒防護：過濾網路傳輸中是否含有病毒。

KENDA

資通安全管理方案

- 使用郵件防護：使用垃圾郵件主機防堵外部大量信件流量攻擊，並對郵件內容進行檢測與分析，過濾惡意病毒。
- 個人電腦需安裝防毒軟體，並定期更新病毒碼。
- 全面使用防毒軟體，防毒伺服器每小時自動更新病毒碼，並自動部署至每台部署至每台電腦。
- 2022年05月04日加入聯防組織 台灣CERT/CSIRT聯盟，定時取得最新資安訊息。

KENDA

資通安全管理方案

- 資訊檔案管制
  - 敏感性與重要性資訊管理規定
  - 依「公司內標準化規定之流程及保密原則」之機密等級定義管理。
  - 依「資通安全檢查之規定」規定，針對公司各部門的資訊以群組方式規定存放於網路硬碟資源分享，本公司的網路硬碟fileserver、kdfile主機分享。

KENDA

資通安全管理方案

- kdfile 為機密性檔案放置，如下提到為第二類別，fileserver為非機密性檔案放置，如下提到為第三類別，依部門單位分類並管制讀取權限，依文件性質設定唯讀或可讀寫。
- 檔案資料夾則分為三大種類：
  1. 第一類公開唯讀(如:公告、SOP文件、規章守則)。
  2. 第二類部門資料夾同部門同仁可讀寫，其它部門單位則無任何權限。
  3. 第三類部門公用資料夾，主要同部門單位可讀寫，其它部門單位只有讀取權限。

KENDA

資通安全管理方案

- 資訊備份/備援與復原
  - 備份分為機房內的UNIX伺服器、Microsoft伺服器。
  - UNIX伺服器:每天夜間定時備份資料庫，每天備份前一天有修改的程式及檔案二次，每週日備份全部資料庫資料並將磁帶做異地存放，備份訊息須記錄於電腦磁帶記錄。

資通安全管理方案

- Microsoft伺服器:主要為Microsoft SQL資料庫及相關程式，資料庫每日進行備份、伺服器與程式每週二、四、六進行備份，備份情況須紀錄於備份紀錄表。
- 備份資料回復驗證，每半年UNIX伺服器、Microsoft伺服器進行抽測一次，以檢測備份資料之有效性，並將測試狀況記錄於電腦機房記錄。
- 重要Server備援架構建置。

KENDA

資通安全管理方案

資訊安全管理宣導

- 資訊部主管制定資訊安全政策。
- 資訊網管主管每年對員工施予訓練並作成記錄。
- 每年演練一次。

資通安全管理方案

違規行為處置

- 本公司網路使用者需遵守公司網路規定，如有下列情事發生，並經查獲屬實，將予以限制使用網路之處分，再犯、情節重大者，依其情節簽請人評會議處。
- 資訊單位於委外合約中擬定條款，要求委外公司遵守保密規定，與擔負法律上之相關責任。

資通安全管理方案

- 定期稽核
  - 本公司依稽核室年度稽核計畫對資訊系統執行稽核。

投入資通安全管理之資源量化數據

- 定期續約防毒/防火牆軟體與更新

  2025年實際投入費用約74萬(同比去年持平)

  2024年實際投入費用約74萬

  2023年實際投入費用約65萬

- 簽訂重要資訊/網路硬體維護合約

  2025年實際投入費用約85萬(追加機房主機維護)

  2024年實際投入費用70萬

  2023年實際投入費用70萬

KENDA

投入資通安全管理之資源量化數據

- 對全體員工實施「資訊安全教育訓練」

  2025年訓練時數468小時(統計至2025/06月)

  2024年總訓練時數2072小時

  2023年總訓練時數1839小時

- 實施電腦汰換更新

  2025年實際投入費用約145萬(統計至2025/06月)

  2024年實際投入費用約375萬

  2023年實際投入費用約293萬

KENDA

投入資通安全管理之資源量化數據

- 公司重要主機安全性更新(含作業系統、資料庫)
  預計每月更新1台，已更新5台(統計至2025/06月)
- 辦公電腦增加端點防護功能(Defender 0365 P1)
  2025年實際投入費用約35萬/年

未來展望

- 強化資訊安全風險
  - 資安系統盤點:請廠商協助進行公司資安風險評估
  - 資安風險改善:依風險評估報告，進行評估資安系統設備購買
  - 資安弱點掃瞄:公司內部進行資安弱點掃瞄
- 評估透過第三方取得資訊安全管理系統標準認證
- 適度引進資安監控管理設備、資產管理盤點軟體(評估中預計2025-Q3導入）、防火牆硬體更新(預計2025-Q4評估)、 Server主機OS升級

KENDA