資通安全

大東電業因應未來強化並提升資訊安全管理，已成立專責資訊安全組織，訂定資安政策，規劃、協調與執行資訊安全防護措施，導入資訊安全管理機制，並持續透過 PDCA 循環作業模式和定期實施員工資訊安全教育訓練，並執行資訊安全風險評鑑與管理，逐年推動資訊安全管理與解決方案，2023 年未發生任何影響公司業務及營運的資訊安全事件。

資安政策與組織

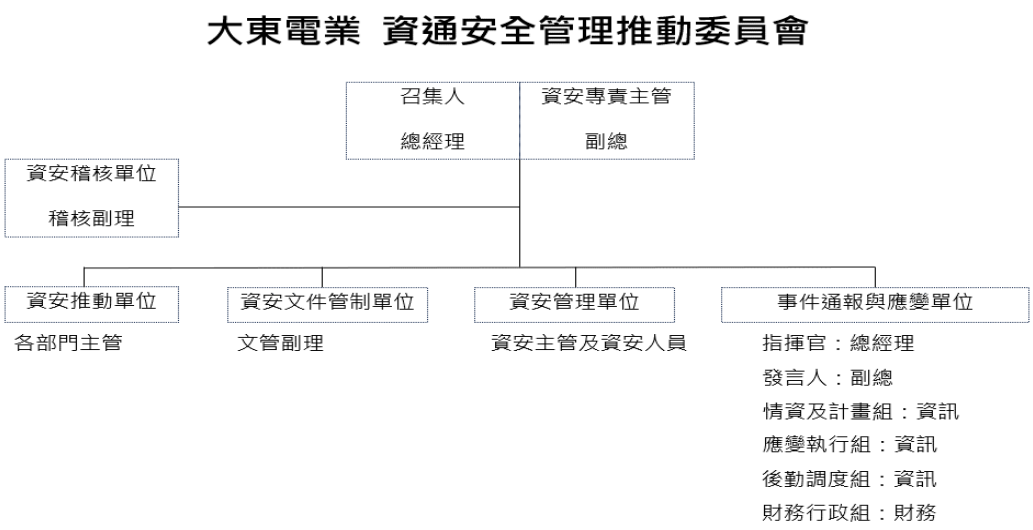
為降低資訊安全事件及營運活動中斷的風險，並保護營運過程不受資訊系統失效影響，聚焦於法令遵循、流程制度、人員訓練及科技運用，強化資料、資訊系統、設備及網路之安全及防護能力，並降低因人為疏失、蓄意或天然災害等導致之資料遭竊、不當使用、洩漏、竄改或破壞等風險，達到保證公司業務持續營運之目的。

大東電業設立資通安全管理推動委員會，督導本公司資訊安全管理制度、技術及維運作業之推行。由總經理當任召集人、副總任資安專責主管 與專責單位主管，訂立「資通安全政策」作為管理依據，以保護員工、客戶、供應商等資訊資料資產之安全，確保企業永續經營。

一.資安政策

為保護大東電業股份有限公司產品與服務之資訊，避免有未經授權之存取、修改、使用揭露，以及天然災害所引起之損失，致力於資通安全管理，以確保本公司重要資訊財產之機密性、完整性及可用性，並符合相關法令法規之要求，保證公司重要業務持續運作。

二. 組織架構



資訊安全管理項目及執行成果

1.成立組織及訂立公司政策

設立大東電業資通安全管理推動委員會及訂定資通安全政策/資通安全目標。

2.配置資安專責人員

配置資安專責主管及資安技術人員。

3.內部資通安全稽核

每年執行內部資通安全和個人資料安全稽核並持續改善。

4.網路防火牆防護

部署次世代防火牆並啟動進階持續性威脅攻擊偵測並進行網路區隔控管存取權限

5.入侵偵測及防禦機制

部署次世代入侵偵測及防禦啟動進階持續性攻擊。

6.強化端點防護

部屬端點防護軟體，防止惡意軟體與勒索軟體攻擊。

7.電子郵件過濾機制

啟用電子郵件過濾/隔離機制。

8.滲透測試

每年執行一次核心系統滲透測試並持續修補弱點漏洞。

9.弱點掃描

每年執行一次核心系統弱點掃描檢測並持續修補弱點漏洞。

10.建置 MDR

導入核心系統 MDR 機制，持續 24 小時監控不中斷。

11.加強備份機制

執行備份 321+1 機制。

12.社交工程演練

每年執行一次社交工程演練，加強員工資安意識。

13.員工資安教育訓練

每年執行員工資安教育訓練，宣導資訊安全，提高員工資識安全意識。

14.災害復原演練

每年排程進行核心系統災害復原演練並確保快速復原，營運不中斷。

15.加入情報安全組織

加入情報安全組織(TWCERT/CC)並提高情資聯防能力。

16.建立資安事件通報機制

已建置資安事件處理標準程序，明定相關流程與措施。

17.資安事件狀況

2023 年無資安事件發生。

18.強化雲端資訊安全管理

透過雲端服務，實現 ESG 數位永續。