台灣中油股份有限公司

資通安全政策

（摘自本公司資訊管理政策彙編）

4.資通安全政策

4.1.為確保本公司資通系統機密性，完整性，可用性符合公司營運需求，特制定資通安全政策如下：

（一）目的

為使本公司資通訊作業安全及營運持續穩定,確保資訊或資通系統之機密性、完整性及可用性，並符合政府資通安全政策及相關法令之規定，制訂「資安認知人人有責，資安管理人人做到」政策，供全體同仁共同遵循。

（二）範圍

本政策適用於本公司同仁、提供各項服務或接觸本公司業務之委外廠商與第三方人員。

（三）策略

(1)建立資通安全風險管理機制，定期檢檢討風險管理之有效性，採取適當之防護措施。

(2)保護資訊及資通系統之機密性與完整性，避免未經授權的存取與竄改。

(3)強化核心資通系統之韌性，確保公司業務持續營運。

(4)辦理資通安全教育訓練，提高同仁之資通安全意識。

(5)完善委外管理程序，確保資訊安全及品質。

(6)建立資通安全稽核制度，確認資訊安全管理制度之有效性。

(7)落實資通安全事件通報作業，強化事件應變、損害控制與復原之能力。

(8)依「各機關對危害國家資通安全產品限制使用原則」辦理資通產品之購置。

4.2.資通安全定義：將安全保護措施的規則應用於電腦系統，並使電腦系統可正常無誤的運作。

4.3.資通安全範圍：

4.3.1.資通安全政策。

4.3.2.資通安全之組織。

4.3.3.人力資源安全。

4.3.4.資產管理。

4.3.5.存取控制。

4.3.6.密碼學。

4.3.7.實體與環境安全。

4.3.8.運作安全。

4.3.9.通訊安全。

4.3.10.系統取得、開發及維護。

4.3.11.供應者關係。

4.3.12.資通安全事故管理。

4.3.13.營運持續管理之資通安全層面。

4.3.14.遵循性。

4.4.資通安全之原則、標準：

4.4.1.國家機密保護法及本公司機密業務資料管理實施要點。

4.4.2.行政院及所屬各機關資通安全管理要點及規範。

4.4.3.經濟部標檢局資訊技術-安全技術-資通安全管理系統-要求。

4.4.4.行政院金融監督管理委員會公開發行公司建立內部控制制度處理準則。

4.4.5.個人資料保護法。

4.5.員工應負的一般性及特定的資通安全責任，並遵守下列事項

之要求及規定：

4.5.1.政府法令及契約對機關資通安全之要求及規定。

4.5.2.台灣中油股份有限公司工作規則。

4.5.3.資通安全教育及訓練。

4.5.4.電腦病毒防範。

4.5.5.業務永續運作計畫。

4.6.資通安全工作之組織、權責及分工：

4.6.1.本公司成立資通安全推動小組，負責督導、推動及協調資通安全相關政策、計畫及措施。

4.6.2.資通安全管理之分工原則：

(1)資通安全相關政策、計畫、措施及技術規範之研議，以及安全技術之研究、建置及評估相關事項，由資訊單位負責辦理。

(2)資料及資訊系統之安全需求研議、使用管理及保護等事項，由業務單位負責辦理。

(3)資訊機密維護由政風單位會同相關單位負責辦理。

(4)稽核使用管理事項由稽核單位會同政風單位辦理。

(5)未設置資訊及政風單位者,由機關首長指定適當的單位及人員負責辦理資通安全管理事項。

4.7.資通安全事件發生時依據「資通安全事件緊急應辦計畫及作業處理程序」處理。

4.8.資通安全之評估：採用 PDCA（Plan，Do，Check，Act）過程模式定期進行獨立及客觀的評估，以反映政府資通安全管理政策、法令、技術及機關業務之最新狀況，運用新興科技或處理新型態資安威脅之程序，確保資通安全實務作業確實遵守資通安全政策，以及確保資通安全實務作業之可行性及有效性。資通安全評估的對象如下：

4.8.1.資訊設施及系統提供者。

4.8.2.資訊及資料擁有者。

4.8.3.使用者。

4.8.4.管理者。

4.8.5.系統維護者。

4.8.6.其他有關人員。

4.9.資通安全風險評鑑機制:針對資產價值,弱點產生之衝擊性、威脅發生機率評鑑風險值，產生風險評鑑報告，由管理審查會議決定風險可接受程度，各單位提報風險處理計畫與控制

措施，將風險值降低至風險可接受程度內。

4.10. 資通安全政策及規定之宣達：需以書面、電子或其他方式通知員工及與本公司連線作業之公私機構及提供資訊服務之廠商共同遵行。

4.11. 本資通安全政策經資通安全推動小組核准後實施，修訂時亦同。