財團法人中華經濟研究院資訊安全政策(網站公告版)

1. 本院資訊安全目標為確保重要及核心系統之機密性(Confidentiality)、完整性(Integrity)及可用性(Availability)。並依各階層與職能定義及量測資訊安全績效之量化指標，以確認資訊安全管理系統實施狀況及是否達成資訊安全目標。

2. 為達成本院之任務目標及最高管理階層對資訊安全之期許與要求，確保本院資訊資產之安全，資訊安全政策訂為：

   2.1. 確保本院相關業務資訊之機密性，防止本院機密資訊及個人資料外洩與遺失。

   2.2. 確保本院相關業務資訊之完整性與可用性，以正確執行本院作業與各項業務。

3. 為確保資訊安全管理系統能有效運作，本院已成立資訊安全委員會，統籌資訊安全管理制度之規劃及推動事宜，其組織架構記載於本院「資訊安全政策」與「資訊安全組織及管理審查作業程序書」。

4. 人力資源安全管制：為降低人為因素影響本院資訊安全，本院實施適當之資訊安全教育、訓練及宣導，以提升人員對資訊安全之認知。

5. 資產管理：為保護本院資訊資產安全，本院依照規範建立資訊資產清冊，並訂定資訊資產分類、分級及管控措施作業原則。

6. 存取控制：

   6.1. 為確保資訊處理設備之授權存取，訂定使用者密碼、註冊、變更、刪除及定期審查機制，並訂定辦公桌及電腦螢幕淨空措施。

   6.2. 為維護網路安全，訂定網路服務機制，區隔內部網路與聯外方式，管控遠距工作及行動裝置之使用。

7. 密碼管制：訂定適當與有效使用密碼政策，保護資訊的機密性、鑑別性及完整性。

8. 實體及環境安全管制：為確保機房、辦公處所與相關設備之安全，本院訂定電腦機房門禁、設備檢查與管理原則，並訂定辦公室一般資訊設備使用、管理及報廢原則。

9. 運作及通訊安全：

   9.1. 為確保正確、安全地操作資訊設備，訂定資訊正確使用之規範，防範機密資訊外洩，並建立防範惡意程式碼及可移動程式碼之機制。

   9.2. 為確保資訊資產完整性及可用性，訂定資訊處理設施備份作業及採用外部資訊處理設施服務管控原則。

9.3. 為維護網路安全，訂定網路安全控制機制及監督系統使用狀況軌跡保護原則。

10. 系統獲取、開發及維護：為確保應用系統開發管理、測試、驗收、上線、維護及委外管理作業之安全，本院訂有標準管制程序。
11. 供應者關係：訂定供應者關係與管理，以確保供應者存取、處理及管理本院資訊與資訊處理設施之安全。
12. 資訊安全事件管理：為降低資訊安全事件造成之損害，本院訂有資訊安全通報及處理程序，並加以記錄。
13. 雲端使用安全：在使用雲端服務時，確保資料、應用程式和基礎設施的安全性，防止未授權存取、資料洩露和其他安全風險。
14. 威脅情資：透過蒐集、分析與解釋網路安全威脅相關的資訊，幫助組織預測、識別和應對各種安全威脅，以降低潛在風險並加強防禦措施。
15. 組態管理：管理與維護系統、網路設備、軟體及雲端環境的設定，以確保它們的安全性、一致性和可預測性。
16. 營運持續管理：為確保本院業務持續運作，本院訂有營運持續管理之資訊安全層面控制原則，建立業務持續運作管理流程及架構，並撰寫及實施業務持續運作計畫。
17. 遵循性：為確保資訊安全管理系統之施行符合相關法令、安全政策及最新技術趨勢，本院訂有遵循性確認原則。
18. 員工違反資訊安全相關規定，其應負之資訊安全責任依紀律程序處理。
19. 本政策至少每年經本院資訊安全組織最高主管審閱一次，以符合相關法令、技術及業務等最新發展現況，確保資訊安全實務作業之有效性。
20. 本政策未盡事宜，悉依有關法令及本院相關規定辦理。
21. 本政策經本院資訊安全組織最高主管同意後實施；修正時亦同。