

彰化縣田中鎮公所 【資通安全政策及目標】

一、資通安全政策

為使本機關業務順利運作，防止資訊或資通系統受未經授權之存取、使用、控制、洩漏、破壞、竄改、銷毀或其他侵害，並確保其機密性（Confidentiality）、完整性（Integrity）及可用性（Availability），特制訂本政策如下，以供全體同仁共同遵循：

1. 應建立資通安全風險管理機制，定期因應內外資通安全情勢變化，檢討資通安全風險管理之有效性。
2. 應保護機敏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. 應強固核心資通系統之韌性，確保機關業務持續營運。
4. 應因應資通安全威脅情勢變化，辦理資通安全教育訓練，以提高本機關同仁之資通安全意識，本機關同仁亦應確實參與訓練。
5. 針對辦理資通安全業務有功人員應進行獎勵。
6. 勿開啟來路不明或無法明確辨識寄件人之電子郵件。
7. 禁止多人共用單一資通系統帳號。
8. 使用者需經授權並賦予相關存取權限後，始得使用本機關所提供之各項系統及網路服務，已授權的使用者，僅能在授權範圍內存取系統及網路資源。
9. 落實個人資料保護，合理使用個人資料，避免個人資料外洩。
10. 機密資料檔案的讀取及複製，須符合本機關各業務單位的規定，並經該單位主管或其授權人員核可。
11. 本政策每年應至少評估檢討一次，以反映本機關資訊安全

需求、政府法令法規、外在網路環境變化及資訊安全技術等最新發展現況，以確保其對於維持營運和提供適當服務的能力。

12. 本政策如遇重大改變時應立即審查，以確保其適當性與有效性。必要時應告知相關單位及委外廠商，以利共同遵守。本政策經資通安全長核准，於公告日施行，並以書面、電子或其他方式通知員工及與本機關連線作業之有關機關（構）、委外廠商，修正時亦同。

二、資通安全目標

(一) 量化型目標

1. 核心資通系統可用性達 98.8% 以上。（中斷時數/總運作時數 \leq 1.2%）
2. 知悉資安事件發生，未能於 1 小時內完成通報的次數 \leq 0 次。
3. 電子郵件社交工程演練之郵件開啟率及附件點閱率均低於 8%。
4. 全球資訊網內容遭置換未於 10 分鐘內完成靜態網頁置換次數 \leq 0 次。
5. 發生 3 或 4 級資安事件未於知悉後 36 小時內完成損害控制或復原作業的次數 \leq 0 次。
6. 發生 1 或 2 級資安事件未於知悉後 72 小時內完成損害控制或復原作業的次數 \leq 0 次。

(二) 質化型目標

1. 落實資通安全，強化資訊服務品質：由全體同仁貫徹執行資通安全管理，所有資通作業相關措施，應確保業務資料之機密性、完整性及可用性，免於因外在之威脅或內部人

員不當的管理，遭受洩密、破壞或遺失等風險，選擇適切的保護措施，將風險降至可接受程度持續進行監控、審查及稽核資通安全管理制度的工作，強化服務品質，提升服務水準。

2. 加強資安訓練，符合法令要求規範：督導全體同仁落實資通安全管理工作，每年持續進行適當的資訊安全教育訓練，建立「資通安全，人人有責」的觀念，促使同仁瞭解資訊安全之重要性，促其遵守資通安全規定，藉此提高資通安全認知及緊急應變能力，降低資通安全風險，達持續營運之目標。
3. 合理利用個資、防範個人資料外洩：對個人資料進行分類，以確定保護的需求和防護措施。建立存取控制機制，在個資傳輸和共享方面採用加密和安全措施，以防止個人資料外洩。
4. 適時因應法令與技術之變動，調整資通安全維護之內容，以避免資通系統或資訊遭受未經授權之存取、使用、控制、洩漏、破壞、竄改、銷毀或其他侵害，以確保其機密性、完整性及可用性。
5. 達成資通安全責任等級分級之要求，並降低遭受資通安全風險之威脅。
6. 提升人員資安防護意識、有效偵測與預防外部攻擊等。

三、資通安全政策及目標之核定程序

資通安全政策由本機關行政室簽陳資通安全長核定。

四、資通安全政策及目標之宣導

1. 本機關之資通安全政策及目標應每年透過教育訓練、內部

會議、張貼公告等方式，向機關內所有人員進行宣導，並檢視執行成效。

2. 本機關應每年向利害關係人（例如 IT 服務供應商、與機關連線作業有關單位）進行資安政策及目標宣導，並檢視執行成效。

五、資通安全政策及目標定期檢討程序

資通安全政策及目標應定期監控其執行成效，並於資通安全管理審查會議中檢討其適切性。

修訂日期：112 年 12 月 25 日