臺南市政府教育局資訊中心

資訊安全政策

機密等級：一般

文件編號：NC-TN-A-001

版　　次：1.7

發行日期：2024/09/02

修　訂　紀　錄				
版次	修訂日期	修訂頁次	修訂者	修訂內容摘要
1.0	2007/12/3			初版
1.1	2012/08/29	1	劉勇炫	修改單位名稱
1.2	2012/11/26	1	劉勇炫	修改單位名稱
1.3	2016/10/13	1;2	曾卉羽	為符合 ISO 27001:2013 要求，增加資安目標與領域
1.4	2016/12/09	1;2	曾卉羽	文審後增加 CIAL 各項目標
1.5	2018/11/28	2	曾卉羽	增加管理階層之領導與承諾
1.6	2019/12/26	1	曾卉羽	修正適用範圍
1.7	2024/09/02	1~4	曾卉羽	因應 ISO27001:2022 改版，修改適用範圍

資訊安全政策					
文件編號	NC-TN-A-001	機密等級	一般	版本	1.7

目錄

資訊安全政策					
文件編號	NC-TN-A-001	機密等級	一般	版本	1.7

1. 目的

確保臺南市政府教育局資訊中心（以下簡稱本中心）所屬之資訊資產機密性、完整性及可用性，並符合相關法規之要求，使其免於遭受內、外部的蓄意或意外之威脅。

2. 適用範圍

本中心承辦相關資訊業務作業流程，包含臺南市政府教育局資訊中心 TANet 骨幹連線、「認證」系統與機房維運作業。

涵蓋 4 類控制措施、93 項管理事項，避免因人為疏失、蓄意或天然災害等因素，導致資料不當使用、洩漏、竄改、破壞等情事發生，對本中心帶來各種可能之風險及危害。管理事項如下：

（1）組織控制措施：

- 資訊安全政策。
- 資訊安全之角色及責任。
- 職務區隔。
- 管理階層責任。
- 與權責機關之聯繫。
- 與特殊關注群組之聯繫。
- 情資威脅。
- 專案管理之資訊安全。
- 資訊及其他相關資產之清冊。
- 可接受使用資訊及其他相關聯資產。
- 資產之歸還。
- 資產之分類分級。
- 資訊之標示。
- 資訊傳送。
- 存取控制。

- 身分管理。
- 鑑別資料。
- 存取權限。
- 供應者關係中之資訊安全。
- 於供應者協議中闡明資訊安全。
- 管理 ICT 供應鏈中之資訊安全。
- 供應者服務之監視、審查及變更管理。
- 使用雲端服務之資訊安全。
- 資訊安全事故管理規劃及準備。
- 資訊之評鑑及決策。
- 對資訊安全事故之回應。
- 由資訊安全事故中學習。
- 證據之蒐集。
- 中斷期間之資訊安全。
- 營運持續之 ICT 備妥性。
- 法律、法令、法規之契約要求事項。
- 智慧財產權。
- 紀錄之保護。
- 隱私及個人可識別資訊(PII)保護。
- 資訊安全之獨立審查。
- 資訊安全政策、規則及標準的遵循性。
- 書面紀錄之運作程序。

(2) 人員控制措施：

- 篩選。
- 聘用條款及條件。
- 資訊安全認知、教育和訓練。
- 獎懲過程。

- 聘用終止或變更後之責任。
- 機密性或保密協議。
- 遠端工作。
- 資訊安全事件通報。

（3）實體控制措施：

- 實體安全周界。
- 實體進入。
- 保全辦公室、房間及設施。
- 實體安全監視。
- 防範實體及環境威脅。
- 於安全區域內工作。
- 桌面淨空及螢幕淨空。
- 設備安置及保護。
- 場所外資產之安全。
- 儲存媒體。
- 支援公用服務事業。
- 佈纜安全。
- 設備維護。
- 設備汰除或重新使用之保全。

（4）技術控制措施：

- 使用者終端設備。
- 特殊存取權限。
- 資訊存取限制。
- 對原始碼之存取。
- 安全識別。
- 容量管理。
- 防惡意軟體。

- 技術脆弱性管理。
- 組態管理。
- 資料刪除。
- 資料遮蔽。
- 資料洩漏預防。
- 資料備份。
- 資訊處理設施之備援。
- 日誌紀錄。
- 監視活動。
- 鐘訊同步。
- 具特殊權限共用程式之使用。
- 對運作中系統之軟體安裝。
- 網路安全。
- 網路服務的安全性。
- 網路區隔。
- 網頁過濾。
- 加密技術之使用。
- 開發生命週期之安全。
- 應用程式安全要求。
- 安全系統架構及工程原則。
- 安全程式設計。
- 開發和驗收中的安全測試。
- 委外開發。
- 開發、測試及運作環境之區隔。
- 變更管理。
- 測試資訊。
- 稽核測試期間的資訊系統保護。

3. 政策

「維護本中心資訊機密性、完整性與可用性，保障使用者資料隱私」

4. 目標

・保護本中心學術網路資訊，避免機敏資料外洩。

・避免本中心發生資料遭未經授權的竄改。

・建立資訊業務永續運作計畫，本中心關鍵業務系統因資通安全事件、異常事件、其他安全事故造成系統、主機異常而中斷營運服務之情事，每次最長不得超過 8 工作小時，確保本中心業務永續運作。

・本中心業務執行須符合相關法令及法規之要求。

5. 責任

・本中心的管理階層建立及審查此政策。

・資訊安全管理者透過適當的標準和程序以實施此政策。

・本中心管理階層應提供對政策之支持，以及持續改善之領導與承諾。

・所有人員和合約供應商均須依照程序以維護資訊安全政策。

・所有人員有責任報告資訊安全事件，和任何已鑑別出的弱點。

・任何蓄意去危及資訊安全的行為將受到相關懲罰或法律行動。

6. 審查

本政策應至少每年評估一次，以反映政府法令、技術及業務等最新發展現況，以確保它對於維持永續運作和提供學術網路相關服務的能力。

7. 實施

・資訊安全政策配合管理審查會議進行資訊安全政策審核。

・本政策經「資訊安全委員會」核定後實施，修訂時亦同。