臺南市政府教育局資訊中心

資訊安全組織程序書

機密等級：一般

文件編號：NC-TN-B-001

版　　次：1.8

發行日期：2018/12/20

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	2012/08/30	封面,1	劉勇炫	修改單位名稱
1.2	2012/10/15	1	劉勇炫	增列 3.權責項目 增列 5.1.4.10 資產交接項目
1.3	2012/11/26	封面,1	劉勇炫	修改單位名稱
1.4	2014/09/19	頁 3,6	劉宜婷	刪除 5.1.4.10 與重複表單
1.5	2016/10/13	頁 1,6	曾卉羽	增加建立資訊安全組織全景與資安目標量測
1.6	2016/12/09	頁 1,6	曾卉羽	修改 5.4.2.4 趨勢與 5.3.2.3
1.7	2016/12/20	頁 2	曾卉羽	修改 5.1.3.1 外部議題與 5.1.3.2 內部議題
1.8	2018/12/20	頁 4	曾卉羽	新增 5.3.3.5 資訊安全官負責作業內容

目錄

資訊安全組織程序書					
文件編號	NC-TN-B-001	機密等級	一般	版本	1.8

1. 目的

促進臺南市政府教育局資訊中心（以下簡稱本中心）資訊安全管理制度執行之有效性，期使本制度達成既定之目標，以增進業務運作之安全。

2. 適用範圍

本中心承辦相關資訊業務作業流程。

3. 權責

資訊安全組織負責本單位資訊安全之維護與落實，權責範圍包括下列各項：

3.1 資訊安全管理制度之審查。

3.2 資訊安全政策之研擬。

3.3 各組資訊安全事項權責分工之協調。

3.4 資訊資產面臨之風險監督。

3.5 應採用之資訊安全技術、方法及程序之協調研議。

3.6 資安事件之檢討及監督。

3.7 矯正預防措施之核准與監督。

3.8 定期舉辦審查會議，討論資訊安全管理制度實施情形，以及相關之預防與矯正措施。

3.9 定期召開資訊安全會議，對期間內所發生之各項資訊安全工作進行討論，並做好工作分配及進度追查。

3.10 確保資訊處理設備的移轉（包含新設備），是經由權責主管人員所進行授權移交，俾使該設備後續運作順利，並賦予接交人之責任所屬。

3.11 其他重要資訊安全事項之協調研議。

4. 名詞定義

無

5. 作業說明

5.1 建立資訊安全組織全景

5.1.1應依據資訊安全定期會議中有關資通訊安全需求決議事項，或上級機關來文要求事項進行評估，並據此建立或調整資通訊安全範圍與目標。

5.1.2應依據決議事項確認與該事項有關之關注方與其要求，並留存文件化紀錄。

5.1.3考量本中心內部、外部議題。依據如下:

5.1.3.1 外部議題：

5.1.3.1.1 為組織尋求達成其目標所處之外部環境，經考量外部利害關係者之目標與關切事項、法令規章要求、利害相關者感知、及特定於風險管理過程範圍之相關風險事項，如:國家、區域、社會文化、法令規章、經濟、技術、環境。

5.1.3.1.2 對組織目標具衝擊之主要推動者與趨勢。

5.1.3.1.3 與外部利害相關者之關係互動與其對於組織之價值。

5.1.3.2 內部議題：

5.1.3.2.1 為組織尋求達成其目標所處之內部環境，可影響組織管理之任何事務，於前後環節進行評估，其組織之專案過程與內容須以組織目標觀點為主要考量，可能產生無法達成目標之機會進而影響組織承諾、信賴與價值觀之事件。

5.1.3.2.2 針對 IT 治理之組織架構與角色執掌、政策目標達成策略、組織支援與知識管理能力、資訊系統與其流程因應。

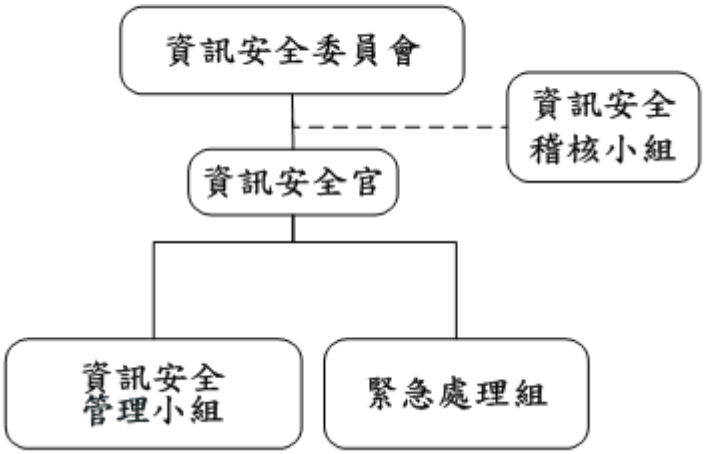
5.1.3.2.3 組織文化與遵循標準、指導綱要、合約關係等模式。

5.2 上述事項之識別與分析應每年至少審查一次，或於本中心組織重大變

更、新業務時重新檢視，並供管理審查時評估管理系統及其適用範圍調整必要性。

5.3 資訊安全組織架構與工作執掌

5.3.1資訊安全組織架構如下圖所示。



5.3.2資訊安全委員會：由資訊安全委員會召集人指派各單位(小組)主管組成，負責資訊安全管理制度相關事項之決議。

5.3.2.1 每年定期或視需要召開會議，審查資訊安全管理相關事宜。

5.3.2.2 視需要召開跨部門之資源協調會議，負責協調資訊安全管理制度執行所需之相關資源分配。

5.3.2.3 資訊安全委員會藉由下列事項，展現對資訊安全管理系統之領導及承諾。

5.3.2.3.1 確保已建立資訊安全政策及資訊安全目標， 並與組織之策略方向相容。

5.3.2.3.2 確保資訊安全管理系統要求事項整合入組織之各項過程。

5.3.2.3.3 確保資訊安全管理系統所需之資源可取得。

5.3.2.3.4 傳達有效之資訊安全管理的重要性，以及符合資訊安全管理系統要求事項之重要性。

5.3.2.3.5 確保資訊安全管理系統達成其預期成果。

5.3.2.3.6 指導及支援人員， 以促進資訊安全管理系統之有效性。

5.3.2.3.7 宣導持續改善。

5.3.2.3.8 當適用其他相關管理角色之責任範圍時， 加以支持以展現其領導權。

5.3.3資訊安全官：由資訊安全委員會指派專人擔任。

5.3.3.1 協調資訊安全管理小組執行資訊安全作業。

5.3.3.2 負責對資訊安全狀況進行預警、監控，並對資訊安全狀況與事件進行處置。

5.3.3.3 對於資訊安全管理之改善提出建議，以及協助執行資訊安全之自我檢核。

5.3.3.4 對於存取控制管理定期進行事件紀錄檢核，以及管理程序檢核。

5.3.3.5 擔任「文管人員」，負責 ISMS 相關文件之發行與管制。

5.3.4資訊安全管理小組：由資訊安全委員會指派人員組成，負責規劃及執行各項資訊安全作業。

5.3.4.1 制定資訊安全管理相關規範。

5.3.4.2 推動資訊安全相關活動。

5.3.4.3 辦理資訊安全相關教育訓練。

5.3.4.4 建立風險管理制度，執行風險管理。

5.3.4.5 建立安全事件緊急應變暨復原措施。

5.3.4.6 執行稽核改善建議事項。

5.3.4.7 執行預防措施之改善。

5.3.4.8 研討新資訊安全產品或技術。

5.3.4.9 執行資訊安全委員會決議事項。

5.3.5緊急處理組：緊急處理組為任務編組。成員相關權責及作業內容分述如下：

5.3.5.1 召集人：

5.3.5.1.1 當重大資安事件發生時，負責聯絡召集緊急處理組。

5.3.5.1.2 協調及督導各關鍵業務流程負責人執行作業，並協調資源之調派使用。

5.3.5.1.3 依據事故評估之結果，得依現況建請資訊安全委員會召集人決議是否宣布災變？是否啟動業務持續計畫？

5.3.5.1.4 當災變發生時，配合救災單位負責搶救人員、物資與設備等及現場指揮工作。

5.3.5.1.5 負責災後協調指揮清理災害現場。

5.3.5.1.6 負責規劃原營運場所之現場復原工作。

5.3.5.2 各關鍵業務流程負責人：

5.3.5.2.1 負責召集相關人員，發展、維護、更新修訂及執行各災害復原程序。

5.3.5.2.2 每年負責召集相關人員進行計劃之測試演練。

5.3.5.2.3 負責原營運場所或異地備援場所之應變、處理、復原及運轉測試工作。

5.3.5.2.4 負責災害現場證據收集,俾利未來訴訟與損害求償事宜。

5.3.5.2.5 災害現場評估損害狀況及執行原營運場所之現場復原工作。

5.3.6資訊安全稽核小組：由資訊安全委員會指派，負責評估資訊安全管理制度之執行情形。

5.3.6.1 擬定資訊安全內部稽核計畫。

5.3.6.2 執行資訊安全內部稽核。

5.3.6.3　撰寫資訊安全稽核報告。

5.3.6.4　追蹤缺失事項之執行情形。

5.3.7資訊安全委員會成員及各小組之人員資訊需由文件管理人員填入「資訊安全組織成員表」並於每年定期更新異動資料。

5.4 管理審查會議

5.4.1資訊安全管理委員會每年應至少召開 1 次「管理審查會議」，必要時得召開臨時會議。

5.4.2管理審查會議審查內容建議包含如下：

5.4.2.1　本中心資訊安全政策。

5.4.2.2　前次管理階層審查議題的處理狀態。

5.4.2.3　與資訊安全管理系統有關的內、外部議題之變更

5.4.2.4　資訊安全管理系統的回饋，包含以下項目之趨勢：

5.4.2.4.1 不符合事項與矯正措施

5.4.2.4.2 審查與量測的結果

5.4.2.4.3 稽核結果

5.4.2.4.4 資訊安全目標執行狀況報告

5.4.2.4.4.1 本中心係以「資訊安全政策」設定之目標為資訊安全目標。

5.4.2.4.4.2 本中心依「資訊安全政策」所列之範圍及目標制定「ISMS 有效性量測表」，並以該表之量測結果做為本

項審查項目之主要討論內容。

5.4.2.4.4.3 資訊安全執行小組應藉由「ISMS 有效性量測表」之量測項目與目標水準建立 ISMS 績效指標，收集各項量測項目之相關資料，據以評估本中心資訊安全目標之達成情形。

5.4.2.5　關注方回饋。

5.4.2.6　風險評鑑結果與風險處理計畫。

5.4.2.7　持續改善的機會。

5.4.3管理審查紀錄

5.4.3.1　管理審查為資訊安全管理制度重要之活動，審查紀錄應依「文件管理程序書」辦理。

5.5　組織間的合作及協調

5.5.1須建立與本資訊安全管理制度相關之「外部單位聯絡清單」。

5.5.2「外部單位聯絡清單」由資訊安全管理小組負責維護更新。

5.6　資訊安全目標的達成計畫與量測方式

5.6.1資訊安全管理小組負責訂定資訊安全目標，資訊安全目標應與資訊安全政策一致並可量測，同時應考量適用之資訊安全要求，以及風險評鑑及處理之結果。並將資訊安全目標與相關事項傳達給本中心人員、委外廠商與資安作業相關單位，且於定期或組之重大變更時進行更新。

5.6.2應定期規劃達成資訊安全目標作業，應包含：

5.6.2.1　相關執行活動或事項；

5.6.2.2　所需投入之人員、預算、設備技術與程序表單等資源；

5.6.2.3　活動或事項負責人員；

5.6.2.4　活動或事項預計完成時間，以及

5.6.2.5　管理目標是否達成之評估方式。

5.6.3完成上述資訊安全目標達成作業規劃並詳列於「ISMS 有效性評量」，由資訊安全管理小組負責維護更新。

5.7　溝通與傳達管理

5.7.1內部溝通與傳達(如管理階層審查會議等)

5.7.1.1　本中心各單位內部如需要溝通與傳達時，可視討論議題，由各單位內自行訂定方式，如：面對面討論、電話、電子郵件與會議等；如以會議方式進行溝通與傳達，則由承辦人員協調開會時間、地點、與會人員，會議完成後應將所討論事項及討論結果記錄在會議紀錄中；如有跟催之必要時則由承辦人員負責追蹤執行狀況。

5.7.1.2　如討論議題需跨單位時，則由承辦人員與權責主管協調後，決定溝通與傳達方式，如各單位權責主管間面對面討論、電話、電子郵件或舉行跨單位會議等方式進行；如以會議方式進行溝通，由承辦人員預約會議場所，以開會通知單通知會議議題、會議時間、會議地點、與會人員。會議完成後應將所討論事項及討論結果記錄在會議紀錄中，如有跟催之必要時則由承辦人員負責追蹤執行狀況，完成後由承辦人員陳報該會議主席，並

由會議主席進行成效評估。

5.7.2外部溝通與傳達

5.7.2.1　外部溝通與傳達由各單位依其工作權責範圍進行，由承辦人員與外部單位人員議定適當溝通與傳達方式，如電話、電子郵件與會議等；溝通完成後，應留下相關紀錄以便日後查閱，如有跟催之必要時則需由承辦人員負責追蹤執行狀況，完成後由承辦人員進行成效評估。

5.7.3媒體溝通與傳達宜由本中心協理核定後，經由電子或紙本文件統一發佈，相關過程應留下溝通相關紀錄，以便日後查閱，如有跟催之必要時則需由承辦人員負責追蹤執行狀況，完成後由承辦人員進行成效評估。

5.7.4資訊安全政策及其它有關本中心資安相關的重大決策，可透過公告或書面的方式進行訊息傳遞，以達到對外溝通與傳達之目的。

5.8 專案管理

5.8.1專案需求分析宜考量資訊安全相關事宜，並列入專案管理工作計畫或合約中。

5.8.2專案啟始時應執行風險評鑑，以評估專案實施階段可能發生的資訊安全風險。

5.8.3專案執行過程中，應對於資訊安全要求進行審查改善。

5.8.4專案管理應對專案相關人員進行角色界定與責任配置。

5.9 行動裝置及遠距工作

為確保本中心遠距工作與行動裝置使用之安全，應訂定作業管理規範，以降低遠距工作與行動裝置使用時的風險，相關程序與方法請參閱「NC-TN-B-007 通信與作業管理程序書」。

6. 相關文件

6.1 文件管理程序書

6.2 資訊安全組織成員表

6.3 外部單位聯絡清單

6.4 ISMS 有效性評量

6.5 利害關係者與議題一覽表