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：1.3

發行日期：2012/11/26

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

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	1.3

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	1.3

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。

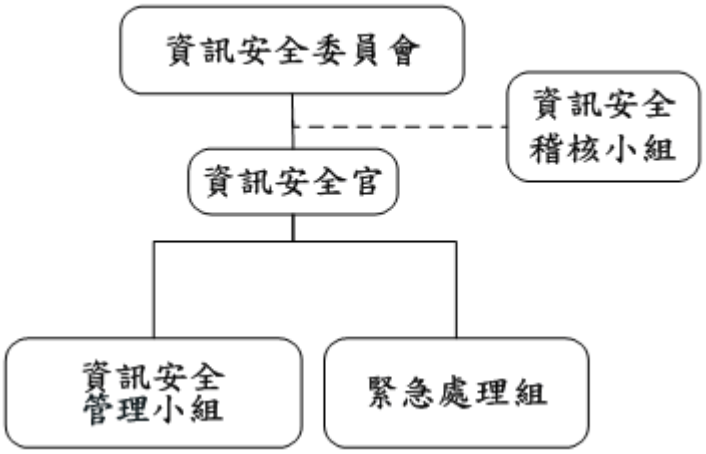
4. 名詞定義

無

5. 作業說明

5.1 資訊安全組織架構與工作執掌

5.1.1資訊安全組織架構如下圖所示。



5.1.2資訊安全委員會：由各單位(小組)主管組成，負責資訊安全管理制度相關事項之決議。

5.1.2.1 每年定期或視需要召開會議，審查資訊安全管理相關事宜。

5.1.2.2 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。

5.1.3資訊安全官：由資訊安全委員會指派專人擔任。

5.1.3.1 協調資訊安全管理小組執行資訊安全作業。

5.1.3.2 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。

5.1.3.3 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。

5.1.3.4 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。

5.1.4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。

5.1.4.1 制定資訊安全管理相關規範。

5.1.4.2 推動資訊安全相關活動。

5.1.4.3 辦理資訊安全相關教育訓練。

5.1.4.4 建立風險管理制度，執行風險管理。

5.1.4.5 建立安全事件緊急應變暨復原措施。

5.1.4.6 執行稽核改善建議事項。

5.1.4.7 執行預防措施之改善。

5.1.4.8 研討新資訊安全產品或技術。

5.1.4.9 執行資訊安全委員會決議事項。

5.1.4.10 執行資訊資產交接之管理。

5.1.5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：

5.1.5.1 召集人：

5.1.5.1.1 當重大資安事件發生時，負責聯絡召集緊急處理組。

5.1.5.1.2 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。

5.1.5.1.3 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？

5.1.5.1.4 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。

5.1.5.1.5 負責災後協調指揮清理災害現場。

5.1.5.1.6 負責規劃原營運場所之現場復原工作。

5.1.5.2 各關鍵業務流程負責人：

5.1.5.2.1 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。

5.1.5.2.2 每年負責召集相關人員進行計劃之測試演練。

5.1.5.2.3 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。

5.1.5.2.4 負責災害現場證據收集，俾利未來訴訟與損害求償事宜。

5.1.5.2.5 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。

5.1.6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。

5.1.6.1 擬定資訊安全內部稽核計畫。

5.1.6.2 執行資訊安全內部稽核。

5.1.6.3 撰寫資訊安全稽核報告。

5.1.6.4 追蹤缺失事項之執行情形。

5.2 管理審查會議

5.2.1資訊安全委員會每年應召開一次「管理審查會議」，必要時得召開臨時會議。

5.2.2管理審查會議審查內容建議包含如下：

5.2.2.1 資訊安全稽核結果及建議改善事項。

5.2.2.2 員工、上級指導單位及第三方單位等利害相關團體的建議。

5.2.2.3 新資訊安全產品或技術導入之審查。

5.2.2.4 矯正及預防措施檢討。

5.2.2.5 風險評鑑適切性審查。

5.2.2.6 前次管理審查會議決議執行狀況。

5.2.2.7 影響資訊安全制度之任何變更事項。

5.2.2.8 資訊安全組織成員所提出之改善建議。

5.2.2.9 資訊安全目標執行狀況報告。

5.2.3管理審查會議之結論建議包含：

5.2.3.1 資訊安全制度執行之各項改進措施。

5.2.3.2 更新風險評鑑與風險處理計畫。

5.2.3.3 針對可能影響資訊安全制度之內外部事件，修正資訊安全管理流程與控制措施。內外部事件包括：

5.2.3.3.1 營運需求的變更。

5.2.3.3.2 安全需求的變更。

5.2.3.3.3 影響現行營運需求的業務程序變更。

5.2.3.3.4 管理或法規需求的變更。

5.2.3.3.5 契約要求的變更。

5.2.3.3.6 可接受風險等級或標準的變更。

5.2.3.4 針對資訊安全制度之需要，協調所需之資源。

5.2.3.5 控制措施有效性評量方式的改善。

5.2.4管理審查紀錄

5.2.4.1 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。

5.3 組織間的合作及協調

5.3.1須建立與本資訊安全管理制度相關之「外部單位聯絡清單」。

5.3.2「外部單位聯絡清單」由資訊安全管理小組負責維護更新。

6. 相關文件

6.1 資訊安全組織成員表

6.2 文件管理程序書

6.3 外部單位聯絡清單

6.4 人員職掌清冊

6.5 資訊資產交接清冊