興國學校財團法人臺南市興國高中
資通安全組織程序書

112.12.05 校務會議通過

一、目的

確保興國高中 (以下簡稱「本校」) 資通安全管理制度之資通安全責任，落實資通安全政策之推行，並符合下列「資通安全管理暨個人資料保護規範」之目標：

1. 為確保本校內部資通安全管理事項之推動，應建立適當管理架構，以審核資通安全政策、分配安全責任，並協調本校各項資通安全措施之實施。
2. 建立與外部資通安全專家之聯繫管道，以利於安全事件處理及專家意見徵詢。

二、適用範圍

本程序適用範圍涵蓋興國高中，以下簡稱本校。

三、權責

無

四、名詞定義

無

五、作業說明

(一)、建立組織全景：

1. 應依據行政管理會議(如：主管會報、行政會議或月會等本校內部會議)中有關資訊安全暨個人資料保護需求決議事項，或上級機關來文要求事項進行評估，並據此建立或調整管理範圍與目標。
2. 應依據相關法令要求、行政院主管機關所下達之重要決定或指導(包括主管機關之行政指導、重要會議決議事項等)、組織透過相關會議所做成之決議(包括主管會報、行政會議或月會等)，針對管理制度之維護需求進行評估，並據此建立或調整相關之管理範圍與目標。
3. 應依據決議事項確認與該事項有關之利害相關團體及其要求，並留存文件化紀錄。
4. 上述事項之識別與分析應每年至少審查一次，或於發生下列事件後重新檢視，並供管理審查時評估管理制度及其適用範圍調整之必要性。

   (1) 組織重大變更後三月內。

   (2) 新業務建立前或執行後一個月內。

(二)、資訊安全組織架構與工作執掌：

1. 資訊安全組織成員如下列 2~6 項所列。
2. 資訊安全委員會：由本校校長擔任召集人，各單位主任以上職為委員會委員，負責資訊安全管理制度相關事項之決議。

   (1) 每年定期或視需要召開會議，審查資通安全管理相關事宜。

(2) 視需要召開跨單位之資源協調會議，負責協調資通安全管理制度執行所需之相關資源分配。

3. 資通安全長：由資訊通安全委員會召集人指派專人擔任。

(1) 負責協調策略規劃組與資訊防護組(緊急處理組)執行資訊安全相關作業。

(2) 負責對資訊安全狀況進行預警、監控，並對資通安全狀況與事件進行處置。

(3) 對於資通安全管理之改善提出建議，以及協助執行資通安全之自我檢核。

(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。

4. 策略規劃組：由資訊安全委員會召集人指派人員組成，負責規劃及執行各項資通安全作業。

(1) 制定資訊安全管理相關規範。

(2) 推動資訊安全相關活動。

(3) 辦理資訊安全相關教育訓練。

(4) 建立風險管理制度，執行風險管理。

(5) 建立安全事件緊急應變暨復原措施。

(6) 執行稽核改善建議事項。

(7) 執行預防措施之改善。

(8) 研討新資通安全產品或技術。

(9) 執行資通安全委員會決議事項。

(10) 鑑別資通安全相關之法規。

A.資策略規劃組應針對本校所提供之資訊服務，識別資通安全相關法令、法規及相關要求，明確定義至「外來文件一覽表」中，並定期檢討與更新。

5. 資訊防護組(緊急處理組)：緊急處理組為任務編組，由資訊安全委員會召集人指派人員組成。成員相關權責及作業內容分述如下：

(1) 資訊防護組組長：

A. 當重大資安事件發生時，負責聯絡及召集資訊防護組。

B. 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。

C. 依據事件評估之結果，得依現況建請資訊安全委員會召集人決議是否宣布災變並啟動業務永續運作計畫。

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

E. 負責災後協調、指揮清理災害現場。

F. 負責規劃原營運場所之現場復原工作。

6. 資訊安全稽核小組：由資訊安全委員會召集人指派，負責評估資通安全管理制度之執行情形。

(1) 擬定資通安全內部稽核計畫。

(2) 執行資通安全內部稽核。

(3) 撰寫資通安全內部稽核報告。

(4) 追蹤不符合事項之改善執行情形。

(三)、管理審查會議：

1. 資訊安全委員會應每年至少召開一次管理審查會議，必要時得召開臨時會議。
2. 管理審查會議審查內容建議如下：

(1) 資訊安全稽核結果及建議改善事項。

(2) 上級指導單位、內部同仁及外部單位等利害相關團體的建議。

(3) 新資訊安全產品或技術導入之審查。

(4) 矯正及預防措施檢討。

(5) 風險評鑑適切性審查。

(6) 前次管理審查會議決議執行狀況。

(7) 影響資訊安全制度之任何變更事項。

(8) 資訊安全組織成員所提出之改善建議。

(9) 資訊安全目標執行狀況報告。

(10) 本校依據「資通安全政策」所列之範圍及目標制定「ISMS 有效性量測表」，並以該量測結果做為評估本校資通安全目標達成情形。

3. 管理審查會議之結論建議如下：

(1) 資訊安全制度執行之各項改進措施。

(2) 更新風險評鑑與風險改善計畫。

(3) 針對可能影響資通安全制度之內、外部事件，修正資通安全管理流程與控制措施，包括：

A. 營運需求的變更。

B. 安全需求的變更。

C. 影響現行營運需求的業務程序變更。

D. 管理或法規需求的變更。

E. 契約要求的變更。

F. 可接受風險等級或標準的變更。

(4) 針對資訊安全制度之需要，協調所需之資源。

(5) 控制措施有效性評量方式的改善。

(6) 應每年檢視「ISMS 有效性量測表」之量測結果與執行情形，並檢討量測項目與目標水準是否需進行調整之必要，做成改善決議。

(7) 管理審查紀錄：

管理審查會議為資通安全管理制度重要之活動，「資通安全管理審查會議紀錄」應依【文件管理程序書(ZH-ISMS-2-001)】辦理。

4. 權責機關、特殊利害相關團體的聯繫：

(1) 為確保資訊安全、個人資料保護事件發生時，儘速執行事件處理，須與權責或外部單位隨時保持聯繫，例如：主管機關、資通安全會報、消防單位等；並建立與管理制度相關之「外部單位聯絡清單」。

(2) 應隨時與資訊安全、個人資料保護技術相關團體維持聯繫，獲取相關之技術及產品資訊與知識，以及處理相關事件或執行系統修補資訊等，亦將資訊建立於「外部單位聯絡清單」。

(3)「外部單位聯絡清單」由各單位自行建立與保管，或以任何可行之方式保存之。

(4) 須建立與資通安全管理制度相關之「外部單位聯絡清單」，並由資訊安全小組負責維護及更新。

5. 法規遵循性：

(1) 識別適用之法令、法規：「資訊安全小組」應定期識別管理制度適用之法令、 法規，並彙整或修訂於「外來文件一覽表」。

(2) 智慧財產權：員工應遵守智慧財產權等相關法令，並依據本校軟體管理相關規定辦理。為確保員工均遵守智慧財產權，於稽核時，將一併查核軟體使用情形。

(3) 個人資訊的資料保護與隱私：員工應遵守個人資料保護法、行政院所屬各機關資訊安全管理要點及相關規定。

(4) 組織紀錄的保護：紀錄依紀錄型式進行分類(例如：變更紀錄、資料庫紀錄、錯誤 日誌、稽核日誌和運作程序)，訂定保存期間和儲存媒

體型式(例 如：紙張、磁片、磁帶、硬碟或光碟片等儲存媒體)。並應依據資訊等級進行適當地處置與保護。