興國學校財團法人臺南市興國高中
資通安全政策

113.01.25 校務會議通過

1. 本校資訊安全管理制度(ISMS)資通安全政策之目的
    1. 確保本校之主機、網路設備及網路通訊安全，有效降低人為疏失、蓄意或天然災害等而導致資訊資產遭竊、不當使用、洩漏、竄改或破壞等風險，並建立資通安全管理規範。
    2. 確保本校各處室業務資訊之機密性、完整性與可用性。
        1. 機密性：確保被授權之人員才可使用及取得資料。
        2. 完整性：確保資訊正確無誤、未遭竄改。
        3. 可用性：確保被授權之人員能取得所需資訊。
2. 依據
    1. 資通安全管理法及其子法
    2. 個人資料保護法及其子法
3. 適用範圍
    1. 本校資訊安全管理制度（ISMS）所涵蓋範圍皆適用之。
    2. 資訊安全管理涵蓋 14 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，對本校帶來各種可能之風險及危害。管理事項如下：
        1. 資通安全政策之制定及評估
        2. 資訊安全組織之職責與分工
        3. 人力資源安全
        4. 資訊資產管理

5. 存取控制
6. 密碼措施
7. 實體與環境安全
8. 作業安全
9. 通訊安全
10. 資訊系統獲取、開發及維護
11. 供應商關係
12. 資通安全事故管理
13. 營運持續管理之資訊安全層面
14. 遵循性。

4. 資通安全政策內容
    1. 組織全景之鑑別

        (1)本校應決定與本校營運目的相關，且會影響 ISMS 預期成果之內部與外部議題，鑑別出與本校所提供服務相關之利害關係者，以及這些利害關係者對本校之需求與期望，並讓資通安全長知悉以取得共識，用以客觀決定本校 ISMS 之範圍。

        (2)應系統化地鑑別本校之核心業務與核心業務相關之利害關係者，並判別若無法達到利害關係者之需求與期望，會對本校造成何種程度之衝擊，並將上述評估及分析結果供資通安全長用以決策 ISMS 之導入及驗證範圍。
    2. 本校各項資訊安全管理規定必須遵守政府相關法規（如：資通安全管理法、刑法、國家機密保護法、專利法、商標法、著作權法、個人資料保護法等）之規定。
    3. 成立資訊安全管理組織負責資訊安全制度之建立及推動事宜。

4. 定期實施資通安全教育訓練，宣導資訊安全政策及相關實施規定。
5. 建立主機及網路使用之管理機制，以統籌分配、運用資源。
6. 新設備建置前，須將風險、安全因素納入考量，防範危害系統安全之情況發生。
7. 建立資訊機房實體及環境安全防護措施，並定期施以相關保養。
8. 明確規範網路系統之使用權限，防止未經授權之存取動作。
9. 訂定資訊安全管理制度內部稽核計畫，定期檢視本校推行資訊安全管理制度範圍內所有人員及設備使用情形，依稽核報告擬訂及執行矯正預防措施。
10. 訂定營運持續管理規定並實際演練，確保本校業務持續運作。
11. 本校所有人員負有維持資通安全之責任，且應遵守相關之資通安全管理規範。
12. 資訊安全管理制度文件應有明確之管理規範。
13. 委外廠商在執行本校委外業務時若有複委託之需求，應評估複委託業務相關之資安風險。並要求委外廠商依資訊安全管理制度(ISMS)等相關規定對複委託廠商進行適當之監督與管理。
14. 對內部及外部專案管理的過程中，應明訂及陳述與專案相關之各項資訊安全要求，並由風險評鑑之結果用以決定及實作資訊安全控制措施，確保內部及外部專案資訊之機密性、完整性及可用性，降低機敏資訊(含個人資料)外洩及違反法令之風險。
15. 應制定可攜式資訊設備(包含智慧型移動裝置)及可攜式儲存媒體之管理程序，要求同仁落實執行，並定期針對可攜式資訊設備(包含智慧型移動裝置)及可攜式儲存媒體進行風險評鑑，依據風險評鑑之

結果選擇適切之控制措施，定期對同仁執行查核作業，確保使用可攜式資訊設備及儲存媒體之風險受到監控，降低機密資料外洩之風險。

16.組織內有效溝通

應決定及建立與資訊安全管理制度（ISMS）相關的內部與外部溝通之需求及準則(如下表所示)，確保資訊安全管理制度（ISMS）各項業務在內部適度的溝通與傳達，以利資訊安全管理制度（ISMS）之推動與管理

內外部溝通	溝通時機	溝通對象	溝通內容、方式	由誰溝通
外部溝通	不定期會議、有可能造成資安事件	委外廠商	本校資通安全政策	權責主管或資訊組
外部溝通	客訴事件發生	利害關係者	透過電話、電子郵件、書面或親自拜訪等方式，向相關人員進行處置說明，並取得諒解	權責主管或業務承辦人員
外部溝通	採購作業	相關供應商	採購作業相關事宜與資訊安全要求	權責主管或資訊組
內部溝通	每年至少一次	所有利害關係者	資通安全政策(含對內外公告)	資通安全長
內部溝通	每年管理審查會前	所有員工、相關利害關係者	管理審查相關輸入事項	資通安全長
內部溝通	每年內外稽核之後	相關人員、委外廠商	稽核缺失改善作業	權責主管或資訊組

5. 資訊安全目標

本校執行資訊安全管理擬達成之資訊安全目標如下:

(一)量化型目標

1.資通系統可用性達 99.0%以上。(中斷時數/總運作時數≤ 0.1%)。

2.知悉資安事件發生後，於規定的時間完成通報、應變及復原作業的比率為 100%。

3.電子郵件社交工程演練之郵件開啟率低於 8%。

4.電子郵件社交工程演練之郵件附件點閱率低於 8%。

5.辦理資安及社交工程教育訓練(1 次)。

6.資通系統發生資料外洩之資通安全事件(≦2 次/年)。

7.「全球資訊網」發生資料遭竄改之資通安全事件(≦2 次/年)。

8.帳號權限管理未授權事件(≦1 件/年)。

9.辦理滲透測試及弱點掃瞄作業 1 次。

10.辦理本校資訊安全稽核 1 次。

(二)質化型目標：

1.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。

2.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。

3.強化委外廠商之選任、監督、管理，嚴格審視委外契約，建構安全服務通道，確保供應鏈關係之資通安全。

4.提升人員資安防護意識、有效偵測與預防外部攻擊等。

6. 資訊安全責任

1. 本校資訊安全管理委員會應建立及審查本政策。

2. 本校資訊安全管理委員會應指派專人訂定、修正及實施資通安全維護計畫，每年呈報上級主管機關執行情況。
3. 資訊安全管理者透過適當的標準和程序以實施本政策。
4. 所有人員與合約供應商均須依照程序以維護資訊安全政策。
5. 所有人員有責任報告安全事件，和任何已鑑別出的弱點。
6. 任何蓄意違反資訊安全的行為將受到相關規範或法律行動。

7. 資安政策之評估與審查

本政策應至少每年評估及審查一次，以反映政府資通安全管理政策、法令、技術及本校業務等之最新發展現況，確保本校資訊安全管理制度的可行性及有效性，以維持營運和提供適當服務的能力。

8. 實施

本政策經資訊安全管理委員會核准，於公告日施行，並以書面、電子或其他方式通知本校全體及與本校連線作業之有關機關（構）、廠商，修正時亦同。