國立彰化高級中學

資通安全組織程序書

機密等級：一般

文件編號：CHSH-ISMS-B-001

版 次：1.0

發行日期：112.05.30

修　訂　紀　錄				
版次	修訂日期	修訂頁次	修訂者	修訂內容摘要

目錄

資通安全組織程序書					
文件編號	CHSH-ISMS-B-001	機密等級	一般	版次	1.0

1 目的

確保國立彰化高級中學（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「教育體系資通安全管理暨個人資料保護規範」之控制目標：

1.1 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。

1.2 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。

2 適用範圍

本校承辦之資通安全制度相關業務作業流程。

3 權責

無。

4 名詞定義

無。

5 作業說明

5.1 建立組織全景

5.1.1 應依據行政管理會議(如主管會報、行政會議或校務會議等校內行政管理會議)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。

5.1.2 應依據相關法令要求、行政院及教育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、行政會議或校務會議等)，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。

5.1.3 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。

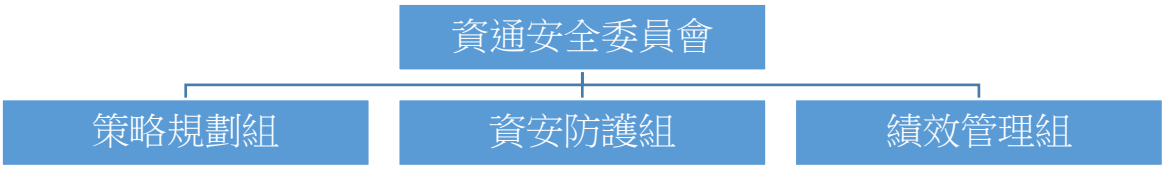
5.1.4 上述事項之識別與分析應每年至少審查一次，或於發生下列事件後重新檢視，並供管理審查時評估管理制度及其適用範圍調整之必要性。

5.1.4.1 組織重大變更後三月內。

5.1.4.2 新業務建立前或執行後一個月內。

5.2 資通安全組織架構與工作執掌

5.2.1資通安全組織架構如下圖所示，資通安全組織成員應填寫於「資通安全組織成員表」，若遇人員異動應加以更新。



5.2.2資通安全委員會：由本校校長擔任資通安全長，各單位一級主管為委員會委員，負責資通安全管理制度相關事項之決議。

5.2.2.1 每年定期或視需要召開會議，審查資通安全管理相關事宜。

5.2.2.2 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。

5.2.3策略規劃組：由資通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。

5.2.3.1 資通安全政策及目標之研議。

5.2.3.2 訂定學校資通安全相關規章與程序、制度文件，並確保相關

規章與程序、制度合乎法令及契約之要求。

5.2.3.3　依據資通安全目標擬定學校年度工作計畫。

5.2.3.4　傳達學校資通安全政策與目標。

5.2.3.5　其他資通安全事項之規劃。

5.2.4資安防護組：由資通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：

5.2.4.1　資通安全技術之研究、建置及評估相關事項。

5.2.4.2　資通安全相關規章與程序、制度之執行。

5.2.4.3　資訊及資通系統之盤點及風險評估。

5.2.4.4　資料及資通系統之安全防護事項之執行。

5.2.4.5　資通安全事件之通報及應變機制之執行。

5.2.4.6　其他資通安全事項之辦理與推動。

5.2.5績效管理組：由資通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。

5.2.5.1　辦理資通安全內部稽核。

5.2.5.2　提報資通安全事項執行情形，以利教育部稽核審查使用。

5.3　管理審查會議

5.3.1資通安全委員會應每年至少召開二次管理審查會議，必要時得召開臨時會議。

5.3.2管理審查會議審查內容建議如下：

5.3.2.1　資通安全稽核結果及建議改善事項。

5.3.2.2　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。

5.3.2.3　新資通安全產品或技術導入之審查。

5.3.2.4　矯正及預防措施檢討。

5.3.2.5　風險評鑑適切性審查。

5.3.2.6 前次管理審查會議決議執行狀況。

5.3.2.7 影響資通安全制度之任何變更事項。

5.3.2.8 資通安全組織成員所提出之改善建議。

5.3.2.9 資通安全目標執行狀況報告。

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。

5.3.3管理審查會議之結論建議如下：

5.3.3.1 資通安全制度執行之各項改進措施。

5.3.3.2 更新風險評鑑與風險改善計畫。

5.3.3.3 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：

5.3.3.3.1 營運需求的變更。

5.3.3.3.2 安全需求的變更。

5.3.3.3.3 影響現行營運需求的業務程序變更。

5.3.3.3.4 管理或法規需求的變更。

5.3.3.3.5 契約要求的變更。

5.3.3.3.6 可接受風險等級或標準的變更。

5.3.3.4 針對資通安全制度之需要，協調所需之資源。

5.3.3.5 控制措施有效性評量方式的改善。

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。

5.3.4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」辦理。

5.4 權責機關、特殊利害相關團體的聯繫

5.4.1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」。

5.4.2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」。

5.4.3「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。

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

5.5 法規遵循性

5.5.1識別適用之法令、法規

「資通安全小組」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」。

5.5.2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。

5.5.3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。

5.5.4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。

6 相關文件

6.1 資通安全政策。

6.2 文件管理程序書。

6.3 資通安全組織成員表。

6.4 外來文件一覽表。

6.5 外部單位聯絡清單。

6.6 ISMS 有效性量測表。

6.7 資通安全管理審查會議紀錄。