國立花蓮女子高級中學

資訊安全組織程序書

機密等級：限閱

文件編號：HLGS-ISMS-B-001

版 次：1.0

發行日期：100.10.11

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	100.10.11		主管會報	初版
1.1	111.04.27	1、2、4、5、6	資訊安全委員會	

目錄

資訊安全組織程序書					
文件編號	HLGS-ISMS-B-001	機密等級	限閱	版次	1.1

1 目的

確保國立花蓮女子高級中學（以下簡稱「本校」）資訊安全管理制度之資訊安全責任，落實資訊安全政策之推行，並符合下列「教育體系資通安全暨個人資料管理規範」之控制目標：

1.1 為確保本校內部資訊安全管理事項之推動，應建立適當管理架構，以審核資訊安全政策、分配安全責任，並協調本校各項資訊安全措施之實施。

1.2 建立與外部資訊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

本校承辦之資訊安全相關業務作業流程。

3 權責

無。

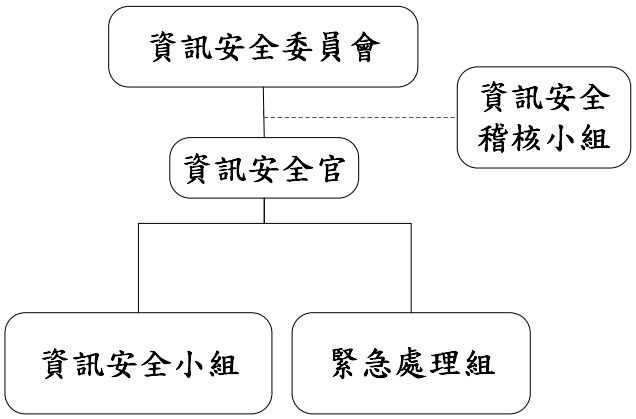
4 名詞定義

無。

5 作業說明

5.1 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，資訊安全組織成員應填寫於「資訊安全組織成員表」，若遇人員異動應加以更新。



5.1.2資訊安全委員會：由本校校長擔任召集人，各業務部門主任或代表一名為委員會委員，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：由資訊安全委員會召集人指派專人擔任。

5.1.3.1 負責協調資訊安全小組與緊急處理組執行資訊安全相關作業。

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資訊安全小組：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 鑑別資訊安全相關之法規。

5.1.4.11 資訊安全小組應針對本校所提供之資訊服務，識別資訊安全相關法令、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。

5.1.5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：

5.1.5.1 緊急處理組組長：

5.1.5.1.1 當重大資安事件發生時，負責聯絡及召集緊急處理組。

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。

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，以及現場指揮工作。

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員：

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業務永續運作計畫之測試演練。

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：由資訊安全委員會召集人指派，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 撰寫資訊安全內部稽核報告。

5.1.6.4 追蹤不符合事項之改善執行情形。

5.2 建立資訊安全組織全景

5.2.1應依據行政管理會議（如主管會報、行政會議或校務會議等）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。

5.2.2應依據決議事項確認與該事項有關之利害相關團體與其要求，並留存文件化紀錄。

5.2.3上述事項之識別與分析應每年至少審查一次，或於組織重大變更、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 管理審查會議

5.3.1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。

5.3.2管理審查會議審查內容建議如下：

5.3.2.1 過往管理審查之議案的處理狀態。

5.3.2.2 資通訊安全或個資管理要求的變更，如上級機關要求、最高行政管理會議決議事項。

5.3.2.3 管理目標與指標量測結果。

5.3.2.4 內外部稽核結果。

5.3.2.5 資安事故與不符合項目之矯正情形。

5.3.2.6 風險評鑑結果及風險處理計畫執行進度。

5.3.2.7 持續改善之機會。

5.3.3管理審查會議之決議事項建議如下：

5.3.3.1 資訊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，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 針對資訊安全制度之需要，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

管理審查會議為資訊安全管理制度重要之活動,「資訊安全管理審查會議紀錄」應依「文件管理程序書」辦理。

5.4 組織間的合作及協調

須建立與資訊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。

5.4.1為確保資訊安全事件發生時，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...；並建立與組織資訊安全管理制度相關之「外部單位聯絡清單」。

5.4.2應隨時與資訊安全技術相關團體維持聯繫，獲取資訊安全技術及產品資訊與知識，以及處理資訊安全事件或執行系統修補資訊等，並將資訊建立於「外部單位聯絡清單」,由資訊安全小組負責維護更新。

5.5 資訊安全目標的達成計畫與量測方式

5.5.1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校人員、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。

5.5.2應定期規劃達成資訊安全目標作業，應包含：

5.5.2.1 相關執行活動或事項

5.5.2.2 所需投入之人員、預算、設備技術與程序表單等資源

5.5.2.3 活動或事項負責人員

5.5.2.4 活動或事項預計完成時間

5.5.2.5 管理目標是否達成之評估方式

5.5.3完成上述資訊安全目標達成作業規劃並詳列於「ISMS 有效性量測

表」。

6 相關文件

6.1 資訊安全政策。

6.2 文件管理程序書。

6.3 資訊安全組織成員表。

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 資訊安全管理審查會議紀錄。