管理系統文件

文　件　類　別	第 二 階 文 件	
文　件　編　號	ISMS-P-002	
文　件　名　稱	資訊安全組織與權責管理程序書	
發　行　單　位	文 件 管 制 小 組	
發　行　日　期	108 年 08 月 01 日	
版　　次	C	
訂修廢單位	審　　查	核　　准
資通安全處理小組		

（原版簽名頁保存於文件管制小組）

訂　　修　　廢　　記　　錄		
版次	發行日期	訂 修 廢 內 容 摘 要
A	104/07/06	初版發行
B	107/09/14	新增 5.9.3.2.7 (ISMS 有效性量測表)
C	108/08/01	修訂 5.8.1.1 資訊安全長：由校長指派高階主管一人擔任。

1. 目的

   為促使本校有效推動與管理本校資訊安全管理制度(ISMS)，以確保資訊安全管理制度(ISMS)能持續有效地執行，維護員工及客戶權益，以提升本校服務水準並且達成既定的資訊安全目標，特制訂本程序書。

2. 適用範圍

   凡本校與資訊安全組織架構及相關之權責的管理，均適用本程序書。

3. 參考文件

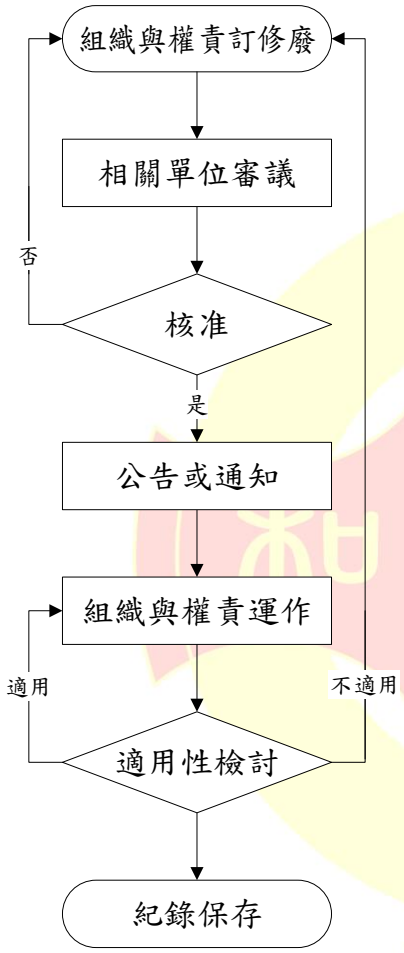
   3.1. ISMS-P-001 文件與紀錄管理程序書。

4. 名詞定義

   無。

5. 作業內容

5.1. 組織與權責管理流程圖

作業流程	權責單位	相關表單
	資通安全處理小組 相關單位主管 資訊安全長 資通安全處理小組 相關單位 資通安全處理小組 資通安全處理小組	資訊安全組織架構圖 會議紀錄單 外部單位聯絡清單 資通安全管理委員會人員名冊

5.2. 組織與權責訂修廢

5.2.1. 資訊安全組織架構圖及權責
在「資訊安全組織架構圖」中，各項職位之權責，由「資通安全處理小組」負責其訂修廢內容之維護。

5.2.2. 各管理程序書之權責
各管理程序書之權責，依照「ISMS-P-001 文件與紀錄管理程序書」之規定，由各項業務之主要承辦人員負責其訂修廢內容之維護。

5.3. 相關小組審議

5.3.1. 「資通安全處理小組」對「資訊安全組織架構圖」、各項職位之權責或各管理程序書之權責於訂修廢時，若需相關單位參與討論與審議時，則由「資通安全處理小組」視需要邀集其他相關單位主管進行會議討論。

5.3.2. 「資通安全處理小組」遇有權責之爭議無法協調，或牽涉到資訊安全組織需進行大變動時，應提交「資通安全管理委員會」決議。

5.4. 組織與權責核准
「資訊安全組織架構圖」、各項職位之權責或各管理程序書之權責之訂修廢內容，應由「資通安全處理小組」之業務承辦人員負責擬案，並依下列規定送呈審核，再依核示意見辦理。

權責 / 類別	訂、修、廢	審查	核准
資訊安全組織架構圖	資通安全處理小組	執行秘書	資訊安全長
各項職位之權責	資通安全處理小組	執行秘書	資訊安全長
各管理程序書之權責	依照「文件與紀錄管理程序書」之規定		

5.5. 公告或通知

5.5.1. 經核准修正後之「資訊安全組織架構圖」應由「資通安全處理小組」負責以適當方式進行公告。

5.5.2. 經核准修正後之各項職位之權責、各管理程序書之權責，應由文件管制人員依據「ISMS-P-001 文件與紀錄管理程序書」之規定，分發通知相關單位。

5.6. 組織與權責運作

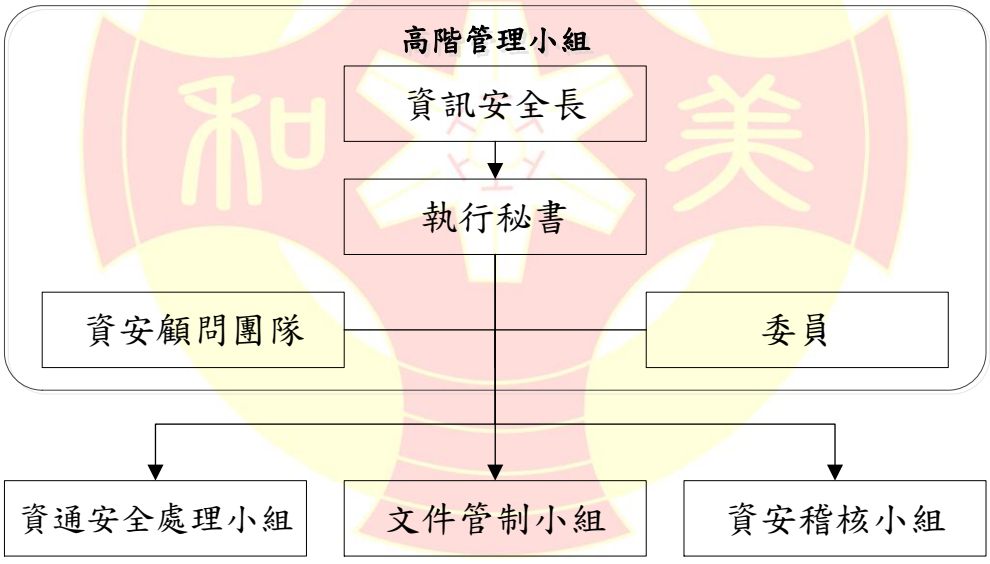
「資通安全處理小組」成員在承辦各項業務時，應依照各項職位之權責或各管理程序書之權責規定執行。

5.7. 適用性檢討

「資通安全處理小組」成員在承辦各項業務時，可隨時進行組織與權責適用性之檢討，若有訂修廢之需求時，依照上述之訂修廢規定辦理。

5.8. 資訊安全管理組織

本校設立「資通安全管理委員會」，明確規範資訊安全管理作業之人員權限與責任，協調事務及推動資訊安全管理事宜，確保資訊安全各項管理規範能有效持續地執行，並達成資訊安全之政策與目標。本管理組織結構如下。



5.8.1. 組織編組

5.8.1.1. 資訊安全長：由校長指派高階主管一人擔任。

5.8.1.2. 執行秘書：由「資訊安全長」指派主管一人擔任。

5.8.1.3. 委　　員：由「資訊安全長」遴選各單位主管擔任。

5.8.1.4. 資安顧問團隊：由「資訊安全長」遴選業界學者專家擔任資

訊安全顧問。

5.8.1.5. 列席人員：視需要指定相關單位人員列席。

5.8.2. 高階管理小組

5.8.2.1. 由資訊安全長、執行秘書、各單位主管及資訊安全顧問團隊所組成。

5.8.2.2. 工作職掌

5.8.2.2.1. 資訊安全管理最高決策組織。

5.8.2.2.2. 核准發行及維護資訊安全管理政策。決定及提供建立、實施、運作及維持管理制度所需之資源。

5.8.2.2.3. 授權小組成員進行資訊安全管理相關事件處置。

5.8.2.2.4. 審理資訊安全管理制度(ISMS)相關事項之計畫及協調溝通。

5.8.2.2.5. 確認資訊安全風險評鑑的時機及審核評鑑報告。

5.8.2.2.6. 召開資訊安全檢討追蹤會議。

5.8.2.2.7. 資訊安全政策與管理文件之審核。

5.8.2.2.8. 審理資訊安全稽核人員之稽核報告。

5.8.2.2.9. 審理資訊安全管理相關之工作報告。

5.8.2.2.10. 其他資訊安全管理相關事宜之決策。

5.8.2.2.11. 承諾遵守與資訊安全相關之法令法規。

5.8.2.2.12. 建立良好遵循實務，落實執行本校「資訊安全管理制度(ISMS)」之政策。

5.8.3. 資訊安全長

5.8.3.1. 工作職掌

5.8.3.1.1. 負責協調相關人員推動資訊安全管理制度(ISMS)。

5.8.3.1.2. 審核本校資訊安全管理制度(ISMS)目標及實施範圍。

5.8.3.1.3. 訂定及檢討本校資訊安全相關政策及規定。

5.8.3.1.4. 監督營運持續演練的辦理，協調資訊安全管理制度(ISMS)執行所需之相關資源分配。

5.8.3.1.5. 審核實施矯正預防措施所需之資源，包括人力、時間及經費。

5.8.3.1.6. 負責定期主持管理審查及各項資訊安全會議，審查資訊安全管理相關事宜。

5.8.4. 執行秘書

5.8.4.1. 工作職掌

5.8.4.1.1. 召集各小組成員參加管理審查及各項資訊安全會議。

5.8.4.1.2. 監督及執行資訊安全管理制度(ISMS)等各項資訊安全工作。

5.8.4.1.3. 協調各小組執行各項資訊安全作業。

5.8.4.1.4. 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。

5.8.4.1.5. 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。

5.8.4.1.6. 對於存取控制管理需定期進行事件紀錄檢核，以及管理程序檢核。

5.8.5. 資訊安全顧問

5.8.5.1. 工作職掌

提供與資訊安全管理與技術領域相關之指導與諮詢建議，確保本校於維運資訊安全管理制度(ISMS)時，能獲得必要之協助與諮詢管道。

5.8.6. 資通安全處理小組

5.8.6.1. 由執行秘書召集業務相關人員若干名組成，成員詳見「ISMS-P-002-01 資通安全管理委員會人員名冊」。

5.8.6.2. 工作職掌

5.8.6.2.1. 制定與維護資訊安全政策、資訊安全目標與各項標準作業程序。

5.8.6.2.2. 界定與檢討資訊安全管理系統之範圍與控制措施。

5.8.6.2.3. 建立與維護業務持續營運計畫。

5.8.6.2.4. 各項資訊安全管理文件與記錄之建立與管制。

5.8.6.2.5. 擬定資訊安全教育訓練計畫及辦理各項資訊安全相關的教育訓練活動。

5.8.6.2.6. 制定風險管理制度，執行風險管理作業。

5.8.6.2.7. 持續不斷的評估與檢討風險管理之具體成效。

5.8.6.2.8. 建立資訊安全事件緊急應變暨復原措施。

5.8.6.2.9. 監控、記錄與調查資訊安全事件。

5.8.6.2.10. 受理資訊安全事件回報與事件處理。

5.8.6.2.11. 執行「資通安全管理委員會」所決議之事項。

5.8.6.2.12. 執行稽核改善建議事項，並追蹤缺失事項之執行情形。執行矯正與預防措施之改善。

5.8.7. 文件管制小組

5.8.7.1. 由執行秘書召集業務相關人員若干名組成，成員詳見「ISMS-P-002-01 資通安全管理委員會人員名冊」。

5.8.7.2. 工作職掌

5.8.7.2.1. 文件發行、回收與銷毀。

5.8.7.2.2. 發行文件之版本管理。

5.8.7.2.3. 紙本文件之保管、借閱。

5.8.7.2.4. 發行文件電子檔之保管。

5.8.7.2.5. 發行文件電子文件公告及更新管理。

5.8.8. 資訊安全稽核小組

5.8.8.1. 由執行秘書召集業務相關人員若干名組成，成員詳見「ISMS-P-002-01 資通安全管理委員會人員名冊」。

5.8.8.2. 工作職掌

5.8.8.2.1. 制定資訊安全內部稽核作業管理程序。

5.8.8.2.2. 負責訂定相關之稽核計畫、內部稽核及協助進行外部稽核作業。

5.8.8.2.3. 負責檢核資通安全業務是否落實。

5.8.8.2.4. 撰寫稽核報告、複查追蹤稽核發現不符合事項之矯正措施。

5.8.8.2.5. 評估與檢討資訊安全內部稽核成效。

5.9. 資通安全管理委員會運作方式

5.9.1. 管理審查會議召開

5.9.1.1. 每年至少召開管理審查會議一次，由「資通安全管理委員會」資訊安全長主持，以確保資訊安全管理制度(ISMS)的適用性和有效性，同時評估改進資訊安全管理制度(ISMS)。

5.9.1.2. 如遇特殊或重大資訊安全事件時得召開臨時會議，討論及決議資訊安全相關事宜，以因應緊急事故。

5.9.2. 管理審查會議參加人員

由「資通安全管理委員會」各個成員參加，必要時可邀請學者或與資訊安全產業相關的專家與會。

5.9.3. 管理審查的重點

5.9.3.1. 審查各項程序和控制措施的執行成效，主要目標如下：

5.9.3.1.1. 快速發現相關程序和控制措施的瑕疵。

5.9.3.1.2. 快速有效的鑑別資訊安全事件。

5.9.3.1.3. 資訊安全活動的實施成效是否符合期望。

5.9.3.1.4. 反應業務優先順序的資訊安全活動。

5.9.3.2. 評估資訊安全管理制度(ISMS)執行的有效性，主要目標如下：

5.9.3.2.1. 執行結果與資訊安全政策是否相符。

5.9.3.2.2. 是否定期更新審查。

5.9.3.2.3. 是否通報給所有相關人員。

5.9.3.2.4. 是否確實執行預防與矯正措施。

5.9.3.2.5. 投入的資源是否足夠。

5.9.3.2.6. 控制措施是否落實執行。

5.9.3.2.7. 為了查核資訊安全控制措施的有效性，各承辦人員須每年依據「ISMS-P-002-04 ISMS 有效性量測表」之項目進行評量，並留下紀錄提交管理審查會議審查。

5.9.3.3. 分析殘餘和可接受風險，以反應下列事項的改變：

5.9.3.3.1. 組織。

5.9.3.3.2. 技術。

5.9.3.3.3. 業務目標和流程。

5.9.3.3.4. 鑑別出的威脅。

5.9.3.3.5. 外部事件，例如法規或社會環境的改變。

5.9.4. 管理審查會議內容

管理審查會議召開前，由「資通安全處理小組」製作「管理審查會議資料」，供會議中進行討論，其資料內容應包括但不限於以下項目：

5.9.4.1. 先前管理審查決議事項之跟催狀況。

5.9.4.2. 有關可能影響 ISMS 的外部與內部問題之變更。

5.9.4.3. 資訊安全的績效回饋，包含下列趨向：

5.9.4.3.1. 不符合事項與矯正措施之執行狀況。

5.9.4.3.2. 監督與量測結果。

5.9.4.3.3. 內部稽核的結果。

5.9.4.3.4. 資訊安全目標的實現。

5.9.4.4. 利害相關團體的回饋。

5.9.4.5. 風險評鑑的結果與風險處理計畫的狀態。

5.9.4.6. 持續改進的機會。

5.9.5. 管理審查會議紀錄

管理審查會議由執行秘書指派特定人員負責將會議結果記錄於「ISMS-P-002-03 會議紀錄單」中，呈資訊安全長核閱後給相關部門傳閱。會議紀錄內容應包括下列事項：

5.9.5.1. ISMS 有效性之改進。

5.9.5.2. 風險評鑑與風險處理計畫之更新。

5.9.5.3. 影響資訊安全之程序與控制之必要時的修改，以回應可能衝擊 ISMS 之內部或外部事件，包括下列事項之變更：

5.9.5.3.1. 各項營運要求。

5.9.5.3.2. 各項安全要求。

5.9.5.3.3. 影響既有各項營運要求之營運過程。

5.9.5.3.4. 法律或法規各項要求。

5.9.5.3.5. 契約的各項義務。

5.9.5.3.6. 風險等級及/或風險接受準則。

5.9.5.4. 資源需求。

5.9.5.5. 控制措施的有效性如何量測之改進。

5.9.5.6. 管理審查為資訊安全管理制度(ISMS)重要之活動，審查會議之紀錄應依「ISMS-P-001 文件與紀錄管理程序書」之規定進行控管。

5.9.6. 決議事項的跟催

會議決議事項列為下次資訊安全內部稽核作業之稽核要項，或由會議中指定專人進行跟催與複查，以確保各項決議事項如期如質地被執行與改善。

5.9.7. 會議記錄陳核

於召開管理審查會議後，由「資通安全處理小組」將會議紀錄彙整並呈報資訊安全長與最高管理階層核閱。

5.10. 內外部溝通事項之管理

5.10.1. 接獲內外部溝通需求

各單位人員接獲內外部聯繫之需求一般有如下時機：

5.10.1.1. 本校頒布新的政策、命令及相關宣導事項時。

5.10.1.2. 本校對外部機關公文往來時。

5.10.1.3. 各單位所承辦業務有新的規定及作法時。

5.10.1.4. 各單位人員與其他單位人員有需協調事宜發生時。

5.10.1.5. 各級主管或同仁發現本校資訊安全管理上之問題時。

5.10.2. 選擇溝通方式

各單位接獲內外部溝通需求時，可選擇如下聯繫方式：

5.10.2.1. E-mail 公告

由欲溝通事項之負責人員，將欲溝通之內容經權責主管同意後，交權責人員以 E-mail 方式傳達給相關同仁。

5.10.2.2. 簽呈

由業務承辦人員將欲簽辦內容，研擬於「簽呈」上，會辦相

關同仁或主管核示意見，並依需要由各級主管針對簽陳內容批示核定意見。

5.10.2.3. 函

由業務承辦人員將欲發函內容，研擬於「函」上，經相關主管審查後，陳權責主管核准，再交由本校收發人員或祕書處辦理發函。

5.10.2.4. 簽到紀錄

與會人員應於會議前於「簽到紀錄」上簽到，由會議主席於會議中指派一位與會者負責記錄，進行各項議決事項追蹤。

5.10.3. 研擬溝通內容及審核

各項內外部溝通欲執行前，由承辦人員視實際需要研擬溝通內容，呈相關主管審閱，經核准後方得發出。

5.10.4. 執行各項溝通事項

由承辦人員依需要執行各項內外部溝通及聯繫事項。

5.10.5. 溝通結果處理

各單位或人員對於各項內外部聯繫事項，若有相關之回饋意見時，可再循各項內外部聯繫方式進行適當溝通，以促使內外部聯繫之溝通目的確實達到為原則。

5.11. 組織間的合作及協調

本校應與外部單位加強合作協調，實施項目如下：

5.11.1. 「資通安全處理小組」應與外部資訊專家或顧問加強協調聯繫，以建立相互合作管道，評估本校面臨資訊安全威脅之處理措施。

5.11.2. 與業務上有密切關係之行政院國家資通安全會報等連結及通信機關，建立及維持適當互動管道，以利發生資訊安全危機時，可獲得外部支援解決問題。

5.11.3. 由「資通安全處理小組」將與本校資訊安全管理制度(ISMS)相關之資訊專家或顧問的聯繫資料紀錄於「ISMS-P-002-02 外部單位聯絡清單」中列管，確保於發生資訊安全事件時能快速聯繫外單

位獲得必要之支援。

5.12. 紀錄保存

相關業務承辦人員應參照如下規範，妥善保存各項紀錄。

編號	表單名稱	保存地點	保存期限
1	資通安全管理委員會人員名冊	資網中心	至少 1 年
2	外部單位聯絡清單	資網中心	至少 1 年
3	會議紀錄單	資網中心	至少 1 年
4	ISMS 有效性量測表	資網中心	至少 1 年

6. 附件

6.1. ISMS-P-002-01 資通安全管理委員會人員名冊。

6.2. ISMS-P-002-02 外部單位聯絡清單。

6.3. ISMS-P-002-03 會議紀錄單。

6.4. ISMS-P-002-04 ISMS 有效性量測表。