資通安全維護計畫訂定

國教署資安業務輔導團

國立華南高商　圖書館主任　劉耀明

現職及經歷：

1. 國立華南高級商業職業學校圖書館主任

2. 教育機構資安驗證中心(ISCB)稽核員(2013至今)

3. 網路管理經驗25年(1997至今)

4. 行政院資安處資通安全專案稽核委員。

5. 教育部部署機關資通安全實地稽核及專案稽核委員

6. 國教署資安業務輔導團輔導委員、社群輔導員、實地稽核訪視委員。

專業證照：

1. ISO/IEC 27001:2013 Information Security Management System(ISMS) Lead Auditor（ISO/IEC 27001:2013資通安全管理制度(ISMS)主導稽核員）

2. BS10012:2017 / ISO 29100:2011 Personal Information Management System(PIMS) Lead Auditor（BS10012:2017 / ISO 29100:2011個人資訊管理系統(PIMS)主導稽核員）

3. ISO/IEC 27701:2019 Privacy Information Management System Lead Auditor（ISO/IEC 27701:2019隱私資訊管理系統主導稽核員）。

為何需要資通安全維護計畫?

資通安全維護計畫撰寫參考依據

維護計畫考量的面向

政策面	• 核心系統盤點 • 資安政策及組織 • 專責人力及經費
管理面	• 資產盤點及風險評估 • 委外管理 • 持續精進與績效管理
技術面	• 安全防護與控制措施 • 資通系統發展及維護安全 • 資通安全通報

維護計畫實施的方式


Act
改善
Plan
計畫
Check
考核
Do
執行
• 針對目標、有效性量測、內稽、外稽、資安事件缺失進行改善
• 進行風險評估、制定資通安全維護計畫、組織及人力
• 檢討計畫執行(內部稽核、管理審查委員會)
• 依據計畫進行相關程序及實作

資通安全相關法規、辦法、制度

- 資通安全法及六子法。
- 學校財團法人及所設私立學校內部控制制度實施辦法
- 高級中等學校學生學籍管理辦法
- 臺灣學術網路各級學校資通安全通報應變作業程序
- 教育體系資通安全暨個人資料管理規範
- ISO 27001資通安全管理(ISMS)

資通安全法第十條

- 公務機關應符合其所屬資通安全責任等級之要求，並考量其所保有或處理之資訊種類、數量、性質、資通系統之規模與性質等條件，訂定、修正及實施資通安全維護計畫。

學校財團法人及所設私立學校內部控制制度實施辦法

第 10 條

學校應就營運事項，訂定管理規章及設計作業程序與內部控制點；其內容包括下列事項：

一、教學。

二、學生。

三、總務。

四、研究發展。

五、產學合作。

六、國際交流及合作。

七、資訊處理。

八、其他學校營運事項。

高級中等學校學生學籍管理辦法

- 第 27 條

學校應就學生學籍資料，依個人資料保護法及其相關法規規定蒐集、處理及利用。

- 第 28 條

學校承辦學籍管理人員違反本辦法規定者，除依法規規定予以懲處外，其涉及刑事責任者，並移送司法機關辦理。

- 第 29 條

各該主管機關得派員檢查及輔導學校學生學籍管理作業，並視辦理情形予以獎懲。

資通安全法施行細則第6條

資通安全法第十條、第十六條第二項及第十七條第一項所定資通安全維護計畫，應包括下列事項：

一、核心業務及其重要性。

二、資通安全政策及目標。

三、資通安全推動組織。

四、專責人力及經費之配置。

五、公務機關資通安全長之配置。

六、資訊及資通系統之盤點，並標示核心資通系統及相關資產。

資通安全法施行細則第6條(續)

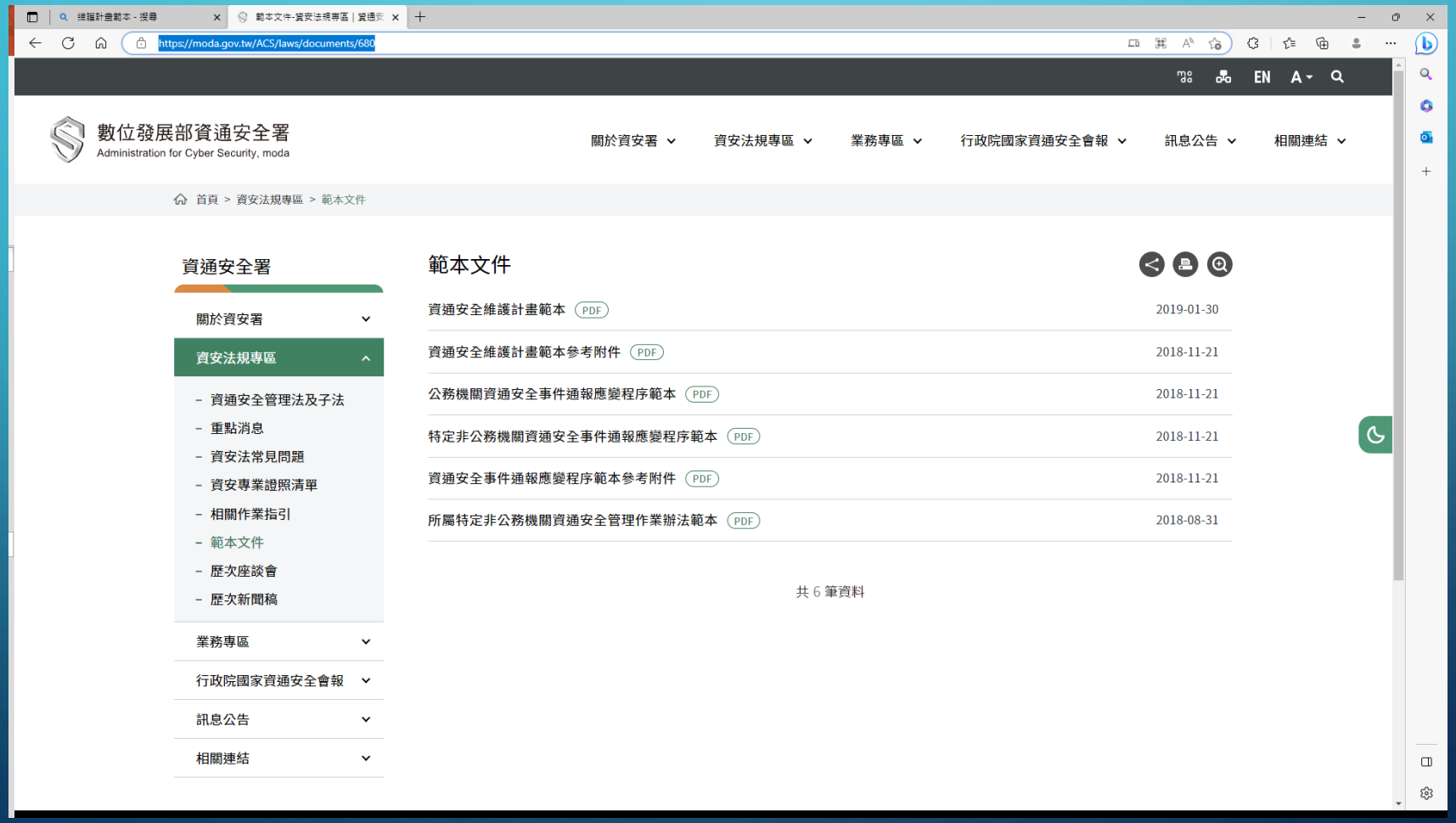
七、資通安全風險評估。
八、資通安全防護及控制措施。
九、資通安全事件通報、應變及演練相關機制。
十、資通安全情資之評估及因應機制。
十一、資通系統或服務委外辦理之管理措施。
十二、公務機關所屬人員辦理業務涉及資通安全事項之考核機制。
十三、資通安全維護計畫與實施情形之持續精進及績效管理機制。

資通安全維護計畫(範本)

- 壹、依據及目的
- 貳、適用範圍
- 參、核心業務及重要性
- 肆、資通安全政策及目標
- 伍、資通安全推動組織
- 陸、專職(責)人力及經費配置
- 柒、資訊及資通系統之盤點
- 捌、資通安全風險評估
- 玖、資通安全防護及控制措施
- 壹拾、資通安全事件通報、應變及演練相關機制
- 壹拾貳、資通系統或服務委外辦理之管理
- 壹拾參、資通安全教育訓練
- 壹拾肆、機關所屬人員辦理業務涉及資通安全事項之考核機制
- 壹拾伍、資通安全維護計畫及實施情形之持續精進及績效管理機制
- 壹拾陸、資通安全維護計畫實施情形之提出
- 壹拾柒、相關法規、程序及表單

數位發展部資通安全署範本文件

- https://moda.gov.tw/ACS/laws/documents/680



資通安全維護計畫撰寫說明

壹、依據及目的

- 基於本校資通安全推動之依循要求，訂定、修正及實施本資通安全維護計畫(以下簡稱本計畫)。其目的為因應上級主管單位之要求，以符合法令規定並落實本計畫之資通安全作業。

貳、適用範圍

- 本計畫適用範圍涵蓋學校全機關

參、核心業務及重要性(核心業務)

核心業務	核心資通系統	重要性說明	業務失效影響說明	最大可容忍中斷時間	資通系統分級
校務學生資料管理	校務系統	□為主管機關指定之關鍵基礎設施 □為主管機關核定資通安全責任等級A級或B級機關所涉業務 ■為本校依組織法執掌，足認為重要者	違反法遵義務：依個人資料保護法應善盡個人資料保護責任，如違反該法致產生損害他人者將依受罰。 影響校務運作	○小時	中

核心業務

- 資通安全法施行細則第 7 條

  前條第一項第一款所定核心業務，其範圍如下：

  一、公務機關依其組織法規，足認該業務為機關核心權責所在。

  二、公營事業及政府捐助之財團法人之主要服務或功能。

  三、各機關維運、提供關鍵基礎設施所必要之業務。

  四、各機關依資通安全責任等級分級辦法第四條第一款至第五款或第五條第一款至第四款涉及之業務。

  前條第一項第六款所稱核心資通系統，指支持核心業務持續運作必要之系統，或依資通安全責任等級分級辦法附表九資通系統防護需求分級原則之規定，判定其防護需求等級為高者。

- 防護需求等級為高者多數為牽涉個資法法遵性或涉及國家機密問題的系統。

校內常見之核心系統(教育部資科司認定)

- 校務系統(教務、學務、輔導)
- 校園資訊網(官網)
- DNS(Domain Name Server)
- 公務使用之Mail Server
- 學生學習歷程系統

參、核心業務及重要性(非核心業務)

非核心業務	業務失效影響	最大可容忍中斷時間	資通系統分級
公文交換	電子公文無法即時送達機關，影響機關行政效率	○小時	普
校務基金系統	影響機關行政效率	○小時	普
財管系統	影響機關行政效率	○小時	普

常見的非核心系統

- 財務管理系統、公文管理系統、監控系統
- 校務基金系統、主計系統
- 人事差勤系統、教師甄選系統
- 播客系統(IGT)、彈性學習平台系統
- 圖書館管理系統、電子看板系統
- 其它(如:合作社系統等等)。

檢討目前系統的必要性，租賃或買斷，系統應符合向上集中之架構

肆、資通安全政策及目標

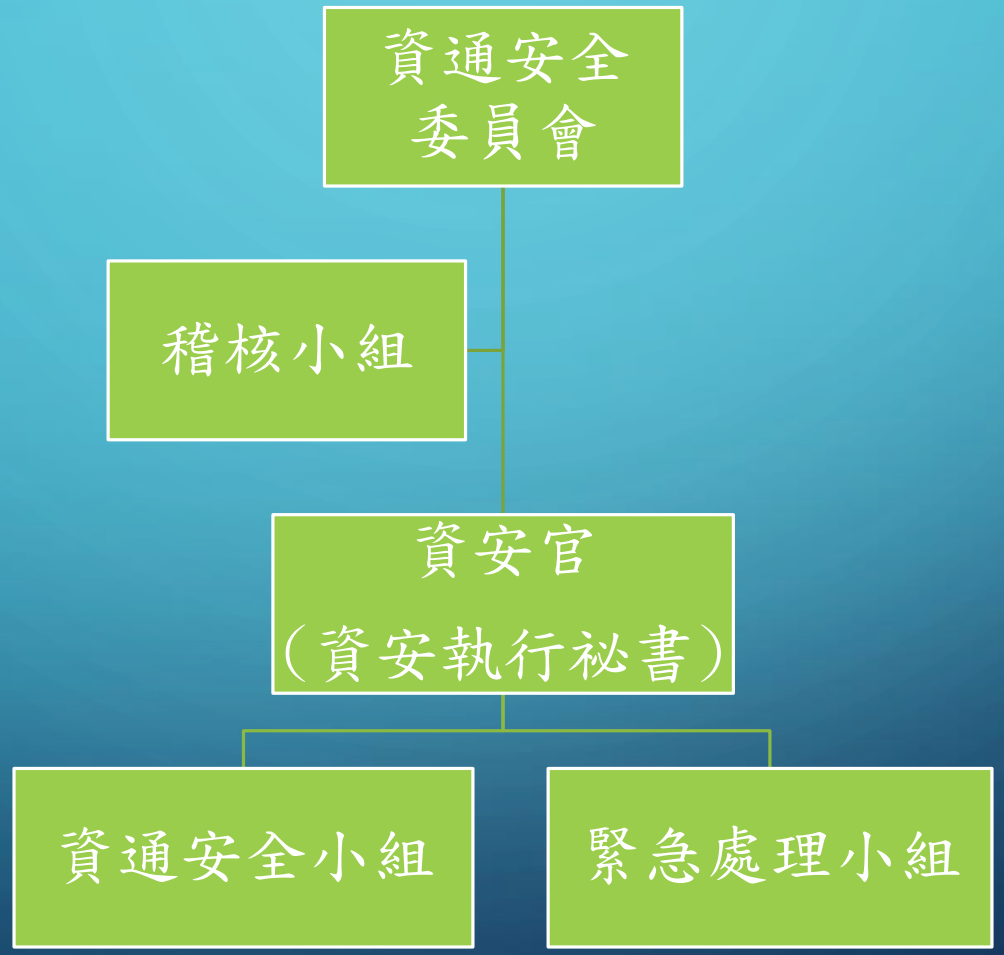
- 本章包含政策內容、目標、核定程序、宣導程序、定期檢討程序等節，機關如已有規定及程序者，可直接引述內部文件編號及名稱。
- 注意事項：

  1. 量化指標及質性指標，是學校能力所及。並明確的定義出量測區間及方法。
  2. 簽陳資通安全長核定
  3. 政策宣導方式
  4. 資通安全政策及目標定期檢討程序

伍、資通安全推動組織

- 資通安全(暨個人資料保護)委員會
  1. 可以和個人資料保護委員會結合
  2. 成員通常為校長及各業務單位一級主管。
  3. 通常設有資安長(校長)、資安官或資通安全執行祕書(資安單位主管)、資安小組（負責實務面工作）。
  4. 定期召開資通安全管理審查會議(一年至少一次)
  5. 校內若無專業人員可以外聘諮詢委員(如:顧問公司、資安輔導團委員或輔導員、區縣市網路中心人員)協助。
  6. 資通安全長，由機關首長指派副首長或適當人員兼任，負責推動及監督機關內資通安全相關事務。

資通安全委員會組織



陸、專職(責)人力及經費配置

- 各校至少1名專責人員
  (1)資通安全管理面業務，負責推動資通系統防護需求分級、資通安全管理系統導入、內部資通安全稽核及教育訓練等業務之推動。
  (2)資通系統安全管理業務，負責資通系統分級及防護基準、安全性檢測、業務持續運作演練等業務之推動。
  (3)資通安全防護業務，負責資通安全防護設施建置及資通安全事件通報及應變業務之推動。
  (4)資通安全管理法法遵事項業務，負責本機關對所屬公務務機關或所管特定非公務機關之法遵義務執行事宜。
- 專責人員鼓勵能擁有資通安全專業證照及職能證書，且建議至少參與12小時專業研習(C級機關、第三類機關）。

陸、專職(責)人力及經費配置

4.機關負責重要資通系統之管理、維護、設計及操作之人員，應妥適分工，分散權責， 若負有機密維護責任者，應簽屬書面約定並視需要實施人員輪調，建立人力備援制度。

5.本機關之首長及各級業務主管人員，應負責督導所屬人員之資通安全作業，防範不法及不當行為。

6.專業人力資源之配置情形應每年定期檢討，並納入資通安全維護計畫持續改善機制之管理審查 。

柒、資訊及資通系統之盤點

- 包含資訊及資通系統之分類及盤點之程序
- 參考行政院及所屬各機關資訊安全管理規範之「捌、資訊資產之安全管理」一節
- 每年辦理資訊及資通系統資產盤點
- 資訊及資通系統盤點結果，製作「資訊及資通系統資產清冊」

捌、資通安全風險評估

- 參考行政院國家資通安全會報頒布之最新「資訊系統風險評鑑參考指引」。
- 每年針對資訊及資通系統資產進行風險評估。
- 每年依據資通安全責任等級分級辦法之規定，分別就機密性、完整性、可用性、法律遵循性等構面評估自行或委外開發之資通系統防護需求分級。(系統分級:普、中、高)

捌、資通安全風險評估

核心資通系統	資訊資產	核心資通系統主要功能	最大可容忍中斷時間
校務系統	1. 網站前台主機計1台 2. 網站後台主機計1台 3. 骨幹網路交換器 4. 管理人員、操作人員 5. 資料庫、系統軟體	學籍管理、學生修課、出缺席、輔導狀況資料。	○小時

玖、資通安全防護及控制措施

- 資訊及資通系統之管理
  1. 資訊及資通系統之保管
  2. 資訊及資通系統之使用
  3. 資訊及資通系統之刪除或汰除
- 存取控制與加密機制管理
  1. 網路安全控管(含有線及無線)
  2. 資通系統權限管理
  3. 特權帳號之存取管理
  4. 加密管理

玖、資通安全防護及控制措施(續)

- 作業與通訊安全管理
  1. 防範惡意軟體之控制措施
  2. 遠距工作之安全措施
  3. 電子郵件安全管理
  4. 確保實體與環境安全措施
  5. 資料備份
  6. 媒體防護措施
  7. 電腦使用之安全管理
  8. 行動設備之安全管理
  9. 即時通訊軟體之安全管理

玖、資通安全防護及控制措施(續)

- 系統獲取、開發及維護

  資通系統應依「資通安全責任等級分級辦法」附表九之規定完成系統防護需求分級，依分級之結果，完成附表十中資通系統防護基準

- 業務持續運作演練

  每二年辦理一次核心資通系統持續運作演練。

玖、資通安全防護及控制措施(續)

- 執行資通安全健診

  每二年應辦理資通安全健診，至少應包含下列項目：網路架構檢視、網路惡意活動檢視、使用者端電腦惡意活動檢視、伺服器主機惡意活動檢視、安全設定檢視。

- 資通安全防護設備

  1. 防毒軟體、網路防火牆、電子郵件過濾裝置，軟、硬體之必要更新或升級。
  2. 資安設備定期備份日誌紀錄。(log紀錄至少留存6個月)

壹拾、資通安全事件通報、應變及演練相關機制

- 為即時掌控資通安全事件，並有效降低其所造成之損害，學校應訂定資通安全事件通報、應變及演練相關機制，詳資通安全事件通報應變程序
- 以目前教育部資安通報程序為主(臺灣學術網路各級學校資通安全通報應變作業程序)。(1小時內完成通報)
- 演練包含資安通報演練及社交工程演練。

壹拾壹、資通安全情資之評估及因應

- 本章為機關接受情資後應採取之評估及因應措施，其內容包括情資分類及情資因應。
- 適時公佈相關情資：如協力廠商、網路新聞、區網及Tacert預警。

壹拾貳、資通系統或服務委外辦理之管理

- 機關辦理資通系統或服務委外時應注意之事項，其內容包括委外前之選任及委外後之監督 。
- 資安法施行細則第4條中除已規範應注意事項外，學校亦可參考最新版本之《資訊作業委外安全參考指引》調整相關內容，並於資訊委外各階段，訂定具體安全需求。

資安法施行細則第4條

各機關依本法第九條規定委外辦理資通系統之建置、維運或資通服務之提供（以下簡稱受託業務），選任及監督受託者時，應注意下列事項：

一、受託者辦理受託業務之相關程序及環境，應具備完善之資通安全管理措施或通過第三方驗證。

二、受託者應配置充足且經適當之資格訓練、擁有資通安全專業證照或具有類似業務經驗之資通安全專業人員。

三、受託者辦理受託業務得否複委託、得複委託之範圍與對象，及複委託之受託者應具備之資通安全維護措施。

四、受託業務涉及國家機密者，執行受託業務之相關人員應接受適任性查核，並依國家機密保護法之規定，管制其出境。

資安法施行細則第4條(續)

- 五、受託業務包括客製化資通系統開發者，受託者應提供該資通系統之安全性檢測證明；該資通系統屬委託機關之核心資通系統，或委託金額達新臺幣一千萬元以上者，委託機關應自行或另行委託第三方進行安全性檢測；涉及利用非受託者自行開發之系統或資源者，並應標示非自行開發之內容與其來源及提供授權證明。

  六、受託者執行受託業務，違反資通安全相關法令或知悉資通安全事件時，應立即通知委託機關及採行之補救措施。

  七、委託關係終止或解除時，應確認受託者返還、移交、刪除或銷毀履行契約而持有之資料。

  八、受託者應採取之其他資通安全相關維護措施。

  九、委託機關應定期或於知悉受託者發生可能影響受託業務之資通安全事件時，以稽核或其他適當方式確認受託業務之執行情形。

壹拾參、資通安全教育訓練

- 資安專責人員每年至少1名人員建議接受12小時以上之資安專業課程訓練或資安職能訓練。(鼓勵參加資安證照及資安職能證書訓練)
- 一般使用者與主管，每人每年接受3小時以上之一般資通安全教育訓練
- 資通安全認知宣導及教育訓練之內容得包含

  1. 資通安全政策(含資通安全維護計畫之內容、管理程序、流程、要求事項及人員責任、資通安全事件通報程序等)。
  2. 資通安全法令規定。
  3. 資通安全作業內容。
  4. 資通安全技術訓練。

壹拾肆、機關所屬人員辦理業務涉及資通安全事項之考核機制

- 所屬人員之平時考核或聘用，公務機關依據公務機關所屬人員資通安全事項獎懲辦法、各校教職員獎懲實施要點及各相關規定辦理之。
- 私校可依學校訂定之相關獎懲辦法或法規之規定。

壹拾伍、資通安全維護計畫及實施情形之持續精進及績效管理機制

- 為落實安全維護計畫，使資通安全管理有效運作，各相關單位於訂定各階文件、流程、程序或控制措施時，應與本校之資通安全政策、目標及本安全維護計畫之內容相符，並應保存相關之執行成果記錄。
- 至少每二年一次內部稽核作業，並完成稽核改善報告。(資安稽核作業人員需包含有取得專業稽核人員證照、或受過相關稽核訓練之人員)。
- 資通安全委員會定期(每年至少一次)召開資通安全管理審查會議，確認資通安全維護計畫之實施情形，確保其持續適切性、合宜性及有效性。

管理審查會議題應包含下列討論事項

- 過往管理審查議案之處理狀態。
- 與資通安全管理系統有關之內部及外部議題的變更，如法令變更、上級機關要求、資通安全推動小組決議事項等。
- 資通安全維護計畫內容之適切性。
- 資通安全績效之回饋，包括：
  - 資通安全政策及目標之實施情形。
  - 資通安全人力及資源之配置之實施情形。
  - 資通安全防護及控制措施之實施情形。
  - 稽核結果。
  - 不符合項目及矯正措施。
- 風險評鑑結果及風險處理計畫執行進度。
- 重大資通安全事件之處理及改善情形。
- 利害關係人之回饋 。
- 持續改善之機會。

壹拾陸、資通安全維護計畫實施情形之提出

- 依據資通安全法第12條之規定，每年度應向上級或監督機關，填報「資通安全維護計畫實施情形」，使其得瞭解本校之年度資通安全計畫實施情形。
- 目前私校依署內要求。

壹拾柒、相關法規、程序及表單

- 一、相關法規及參考文件
- 二、附件表單

附件表單

附件一：資訊安全政策

附件二：資訊安全組織

附件三：資訊安全組織成員表

附件四：保密切結書

附件五：資訊資產管理

附件六：風險評鑑與管理

附件七：資訊資產異動作業

附件八：存取控制管理

附件九：實體安全管理

附件十：通信與作業管理

附件表單

附件十一：系統開發與維護

附件十二：資通安全事件通報及應變程序

附件十三：委外廠商執行人員保密切結書

附件十四：委外廠商執行人員保密同意書

附件十五：委外廠商查核項目表

附件十六：內部稽核計畫

附件十七：稽核項目紀錄表

附件十八：內部稽核報告

附件十九：矯正與預防處理單

資通安全維護計畫與附件關聯

壹、依據及目的

貳、適用範圍

參、核心業務及重要性

肆、資通安全政策及目標(資訊安全政策)

伍、資通安全推動組織(資訊安全組織)

陸、專職(責)人力及經費配置(資訊安全組織成員表、保密切結書)

柒、資訊及資通系統之盤點(資訊資產管理)

捌、資通安全風險評估(風險評鑑與管理)

玖、資通安全防護及控制措施(資訊資產異動作業、存取控制管理、實體安全管理、通信與作業管理)

資通安全維護計畫與附件關聯

壹拾、資通安全事件通報、應變及演練相關機制(資通安全事件通報及應變程序、委外廠商執行人員保密切結書、委外廠商執行人員保密同意書、委外廠商查核項目表)

壹拾貳、資通系統或服務委外辦理之管理(系統開發與維護)

壹拾參、資通安全教育訓練

壹拾肆、公務機關所屬人員辦理業務涉及資通安全事項之考核機制

壹拾伍、資通安全維護計畫及實施情形之持續精進及績效管理機制(內部稽核計畫、稽核項目紀錄表、內部稽核報告、矯正與預防處理單)

壹拾陸、資通安全維護計畫實施情形之提出

壹拾柒、相關法規、程序及表單

總　結

- 說、寫、做一致
- 管理階層的支持
- 資通安全工作推動不是一個人的事
- 委外廠商的合約及管理
- 一般人員的教育訓練
- 融入變成日常的習慣。


Q&A

感謝聆聽

聯絡方式：05-2787140#139　E-mail：liu0604@mail.edu.tw