國立頭城高級家事商業職業學校
資通安全維護計畫

目　　錄

壹、依據及目的

依據資通安全管理法第10條及施行細則第6條訂定資通安全維護計畫，作為資訊安全推動之依循及應符合其所屬資通安全責任等級之要求，訂定、修正及實施資通安全維護計畫(以下簡稱本計畫)。為因應資通安全管理法及資通安全責任等級應辦事項要求，以符合法令規定並落實本計畫之資通作業安全。

貳、適用範圍

本計畫適用範圍涵蓋國立頭城高級家事商業職業學校全機關（以下簡稱本校）

參、核心業務及重要性

一、 核心業務及重要性：

本校之核心業務及重要性如下表：

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	24小時	中

各欄位定義：

1. 核心業務：請參考資通安全管理法施行細則第7條之規定列示。
2. 核心資通系統：該項業務內各項作業程序的名稱。

3. 重要性說明：說明該業務對機關之重要性，例如對機關財務及信譽上影響，對民眾影響，對社會經濟影響，對其他機關業務運作影響，法律遵循性影響或其他重要性之說明。

4. 業務失效影響說明：當系統失效時對學校所造成的衝擊及影響。

5. 最大可容忍中斷時間單位以小時計。

6. 資通系統分級：依據資通安全責任等級分級辦法附件九資通系統防護需求分級原則進行分級。

二、 非核心業務及說明：

本校之非核心業務及說明如下表：

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	48小時	普
主計出納系統	影響機關行政效率	48小時	普
財管系統 圖書館系統	影響機關行政效率 影響機關行政效率	48小時 48小時	普 普

各欄位定義：

1. 非核心業務：公務機關之非核心業務至少應包含輔助單位之業務名稱，如差勤服務、郵件服務、用戶端服務等。

2. 業務失效影響：說明該業務失效對機關之影響。

3. 最大可容忍中斷時間單位以小時計。

4. 資通系統分級：依據資通安全責任等級分級辦法附件九資通系統防護需求分級原則進行分級。

肆、資通安全政策及目標

依本校「資通安全政策」如附件一施行。

伍、資通安全推動組織

依本校「資通安全組織」辦法如附件二成立資通安全委員會並

成立資訊安全小組，「資通安全組織成員表」如附件三。

陸、專職(責)人力及經費配置

1、依據行政院110年6月9日院臺護字第1100176725I號函，本校資通安全責任等級為C級。在未完成向上集中前本校應設置資通安全專職人員。其業務內容如下，本校現有資通安全專責人員名單及職掌應表列於「資通安全組織成員表」如附件三，並適時更新。

(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及驗證、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，負責資通安全監控管理機制、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。

1. 本校之承辦單位於辦理資通安全人力資源業務時，應加強資通安全人員之培訓，並提升校內資通安全專責人員之資通安全管理能力。本校之相關單位於辦理資通安全業務時，如資通安全人力或經驗不足，得洽請相關學者專家或專業機關（構）提供顧問諮詢服務。

2. 資安專責人員專業職能之培養(如證書、證照、培訓紀錄等)，應參加主管機關辦理之相關專業研習，並鼓勵取得資通安全專業證照及資通安全職能評量證書。

3. 本校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「保密切結書」如附件四，並視需要實施人員輪調，建立人力備援制度。

4. 校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。

5. 專責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。

一、經費之配置

1. 資訊安全小組於規劃配置相關經費及資源時，應考量本校之資

通安全政策及目標，並提供建立、實行、維持及持續改善資通安全維護計畫所需之資源。

2. 各單位於規劃建置資通系統建置時，應一併規劃資通系統之資安防護需求，並於整體預算中合理分配資通安全預算所佔之比例。

3. 各單位如有資通安全資源之需求，應配合機關預算規劃期程向資訊安全小組提出需求，由資訊安全小組視整體資通安全資源進行分配，並經資通安全長核定後，進行相關之建置。

4. 資通安全經費、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

一、資訊及資通系統盤點

依本校「資訊資產管理」規定如附件五施行。

二、機關資通安全責任等級分級

依據行政院108年7月24日院臺護字第1080180748號函，依據資通安全責任等級分級辦法第6條辦理，並考量本校已有核心系統向上集中規劃，依同法第10條第4款調降等級為D級機關。

捌、資通安全風險評估

一、資通安全風險評估

依本校「風險評鑑與管理」規定如附件六施行。

二、核心資通系統及最大可容忍中斷時間

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	伺服器1台 前端操作電腦4台 邊際交換氣 骨幹交換器 防火牆	學籍管理、學生修課、出缺席、輔導狀況資料。	24小時

最大可容忍中斷時間以小時計。

玖、資通安全防護及控制措施

本校依據前章資通安全風險評估結果、自身資通安全責任等級之應辦事項及核心資通系統之防護基準，採行相關之防護及控制措施如下:

一、資訊及資通系統之管理

依本校「資訊資產異動作業」規定如附件七施行。

二、存取控制與加密機制管理

依本校「存取控制管理」規定如附件八施行。

三、作業與通訊安全管理

依本校資通安全管理制度文件「實體安全管理」規定如附件九、「通信與作業管理」規定如附件十施行。

四、系統獲取、開發及維護

1. 本校之資通系統應依「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，並注意下列事項：

(1) 開發過程請依安全系統發展生命週期(Secure Software Development Life Cycle, SSDLC)納入資安要求，並參考行政院國家資通安全會報頒布之最新「安全軟體發展流程指引」、「安全軟體設計指引」及「安全軟體測試指引」。

(2) 於資通系統開發前，設計安全性要求，包含機敏資料存取、用戶登入資訊檢核及用戶輸入輸出之檢查過濾，並檢討執行情形。

(3) 於上線前執行安全性要求測試，包含機敏資料存取、用戶登入資訊檢核及用戶輸入輸出之檢查過濾測試，並檢討執行情形。

(4) 執行資通系統源碼安全措施，包含源碼存取控制與版本控管，並檢討執行情形。

2. 餘依本校「系統開發與維護」規定如附件十一施行。

五、業務持續運作演練

本校應針對核心資通系統制定業務持續運作計畫，並每二年辦理一次核心資通系統持續運作演練。

六、執行資通安全健診

1. 本校每二年應辦理資通安全健診，其至少應包含下列項目，並檢討執行情形：

(1) 網路架構檢視。

(2) 網路惡意活動檢視。

(3) 使用者端電腦惡意活動檢視。

(4) 伺服器主機惡意活動檢視。

(5) 安全設定檢視。

七、資通安全防護設備

1. 本校應建置防毒軟體、網路防火牆、電子郵件過濾裝置，持續使用並適時進行軟、硬體之必要更新或升級。

2. 資安設備應定期備份日誌紀錄，定期檢視並由主管複核執行成果，並檢討執行情形。

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，本校應訂定資通安全事件通報、應變及演練相關機制，詳如附件十二「資通安全事件通報應變程序」。

壹拾壹、資通安全情資之評估及因應

本校接獲資通安全情資，應評估該情資之內容，並視其對本校之影響、本校可接受之風險及本校之資源，決定最適當之因應方式，必要時得調整資通安全維護計畫之控制措施，並做成紀錄。

一、資通安全情資之分類評估

本校接受資通安全情資後，應指定資通安全專職人員進行情

資分析，並依據情資之性質進行分類及評估，情資分類評估如下：

(一) 資通安全相關之訊息情資

資通安全情資之內容如包括重大威脅指標情資、資安威脅漏洞與攻擊手法情資、重大資安事件分析報告、資安相關技術或議題之經驗分享、疑似存在系統弱點或可疑程式等內容，屬資通安全相關之訊息情資。

(二) 入侵攻擊情資

資通安全情資之內容如包含特定網頁遭受攻擊且證據明確、特定網頁內容不當且證據明確、特定網頁發生個資外洩且證據明確、特定系統遭受入侵且證據明確、特定系統進行網路攻擊活動且證據明確等內容，屬入侵攻擊情資。

(三) 機敏性之情資

資通安全情資之內容如包含姓名、出生年月日、國民身份證統一編號、護照號碼、特徵、指紋、婚姻、家庭、教育、職業、病例、醫療、基因、性生活、健康檢查、犯罪前科、聯絡方式、財務情況、社會活動及其他得以直接或間接識別之個人資料，或涉及個人、法人或團體營業上秘密或經營事業有關之資訊，或情資之公開或提供有侵害公務機關、個人、法人或團體之權利或其他正當利益，或涉及一般公務機密、敏感資訊或國家機密等內容，屬機敏性之情資。

(四) 涉及核心業務、核心資通系統之情資

資通安全情資之內容如包含機關內部之核心業務資訊、核心資通系統、涉及關鍵基礎設施維運之核心業務或核心資通系統之運作等內容，屬涉及核心業務、核心資通系統之情資。

二、資通安全情資之因應措施

本校於進行資通安全情資分類評估後，應針對情資之性質進行相應之措施，必要時得調整資通安全維護計畫之控制措施。

(一) 資通安全相關之訊息情資

由資訊安全小組彙整情資後進行風險評估，並依據資通安全維護計畫之控制措施採行相應之風險預防機制。

(二) 入侵攻擊情資

由資通安全專職(責)人員判斷有無立即之危險，必要時採取立即之通報應變措施，並依據資通安全維護計畫採行相應之風險防護措施，另通知各單位進行相關之預防。

(三) 機敏性之情資

就涉及個人資料、營業秘密、一般公務機密、敏感資訊或國家機密之內容，應採取遮蔽或刪除之方式排除，例如個人資料及營業秘密，應以遮蔽或刪除該特定區段或文字，或採取去識別化之方式排除之。

(四) 涉及核心業務、核心資通系統之情資

資訊安全小組應就涉及核心業務、核心資通系統之情資評估其是否對於機關之運作產生影響，並依據資通安全維護計畫採行相應之風險管理機制。

壹拾貳、資通系統或服務委外辦理之管理

本校委外辦理資通系統之建置、維運或資通服務之提供時，應考量受託者之專業能力與經驗、委外項目之性質及資通安全需求，選任適當之受託者，並監督其資通安全維護情形。

一、選任受託者應注意事項

1. 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。
2. 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。
3. 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。

二、監督受託者資通安全維護情形應注意事項

1. 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第三方安全性檢測證明；涉及利用非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。
2. 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。

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

4. 與委外廠商簽訂契約時，應審查契約中保密條款，並要求委外廠商之業務執行人員簽署委外廠商執行人員保密切結書、保密同意書，格式如：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」。

5. 本校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，以本校「委外廠商查核項目表」如附件十五進行稽核以確認受託業務之執行情形。

壹拾參、資通安全教育訓練

一、資通安全教育訓練要求

1. 本校資安及資訊人員每年至少接受12小時以上之資安專業課程訓練或資安職能訓練。

2. 本校之一般使用者與主管，每人每年接受3小時以上之一般資通安全教育訓練。

二、資通安全教育訓練辦理方式

1. 資通安全小組應於每年年初，考量管理、業務及資訊等不同工作類別之需求，擬定資通安全教育訓練計畫，以建立教職員生資通安全認知，提升機關資通安全水準，並應保存相關之資通安全認知宣導及教育訓練紀錄（如：「教育訓練簽到表」）。

2. 本校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。

3. 教職員報到時，應使其充分瞭解本校資通安全相關作業規範及其重要性。

4. 資通安全教育及訓練之政策，除適用所屬教職員生外，對機關外部的使用者，亦應一體適用。

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

本校所屬人員之平時考核或聘用，依據公務機關所屬人員資通安全事項獎懲辦法、本校教職員獎懲實施要點及各相關規定辦理之。

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

一、資通安全維護計畫之實施

為落實本安全維護計畫，使本校之資通安全管理有效運作，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，。

二、資通安全維護計畫實施情形之稽核機制

(一) 稽核機制之實施

1. 資訊安全稽核小組應定期(至少每二年一次)或於系統重大變更或組織改造後執行一次內部稽核作業，以確認人員是否遵循本規範與機關之管理程序要求，並有效實作及維持管理制度。

2. 辦理稽核前資通安全小組應擬定「內部稽核計畫」如附件十六並安排稽核成員，稽核計畫應包括稽核之依據與目的、期間、重點領域、稽核小組組成方式、保密義務（稽核委員簽署「保密切結書」如附件四）、稽核方式、基準與項目及受稽單位協助事項，並應將前次稽核之結果納入稽核範圍。

3. 辦理稽核時，資訊安全稽核小組應於執行稽核前30日，通知受稽核單位，並將稽核期程、「稽核項目紀錄表」如附件十七及稽核流程等相關資訊提供受稽單位。

4. 本校之稽核人員應受適當培訓並具備稽核能力，且不得稽核自身經辦業務，以確保稽核過程之客觀性及公平性；另，於執行稽核時，應填具稽核項目紀錄表，待稽核結束後，應將稽核項目紀錄表內容彙整至「內部稽核報告」如附件十八中，並提供給受稽單位填寫辦理情形。

5. 稽核結果應對相關管理階層(含資安長)報告，並留存稽核過程之相關紀錄以作為資通安全稽核計畫及稽核事件之證據。

6. 稽核人員於執行稽核時，應至少執行一項特定之稽核項目（如是否瞭解資通安全政策及應負之資安責任、是否訂定人員之資

通安全作業程序與權責、是否定期更改密碼)。

(二) 稽核改善報告

1. 受稽單位於稽核實施後發現有缺失或待改善項目者，應對缺失或待改善之項目研議改善措施、改善進度規劃，並落實執行。
2. 受稽單位於稽核實施後發現有缺失或待改善者，應判定其發生之原因，並評估是否有其類似之缺失或待改善之項目存在。
3. 受稽單位於判定缺失或待改善之原因後，應據此提出並執行相關之改善措施及改善進度規劃，必要時得考量對現行資通安全管理制度或相關文件進行變更。
4. 機關應定期審查受稽單位缺失或待改善項目所採取之改善措施、改善進度規劃及佐證資料之有效性。
5. 受稽單位於執行改善措施時，應留存相關之執行紀錄，並填寫稽核結果及改善報告。

三、 資通安全維護計畫之持續精進及績效管理

1. 本校之資通安全委員會應於上下學期 (每年至少二次)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。
2. 管理審查議題應包含下列討論事項：
   (1) 過往管理審查議案之處理狀態。
   (2) 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。
   (3) 資通安全維護計畫內容之適切性。
   (4) 資通安全績效之回饋，包括：
      A. 資通安全政策及目標之實施情形。
      B. 資通安全人力及資源之配置之實施情形。
      C. 資通安全防護及控制措施之實施情形。
      D. 稽核結果。
      E. 不符合項目及矯正措施。
   (5) 風險評鑑結果及風險處理計畫執行進度。

(6) 重大資通安全事件之處理及改善情形。

(7) 利害關係人之回饋。

(8) 持續改善之機會。

3. 持續改善機制之管理審查應做成「矯正與預防處理單」如附件十八，相關紀錄並應予保存，以作為管理審查執行之證據。

壹拾陸、資通安全維護計畫實施情形之提出

本校依據資通安全法第12條之規定，應於十月前向上級或監督機關，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。

壹拾柒、相關法規、程序及表單

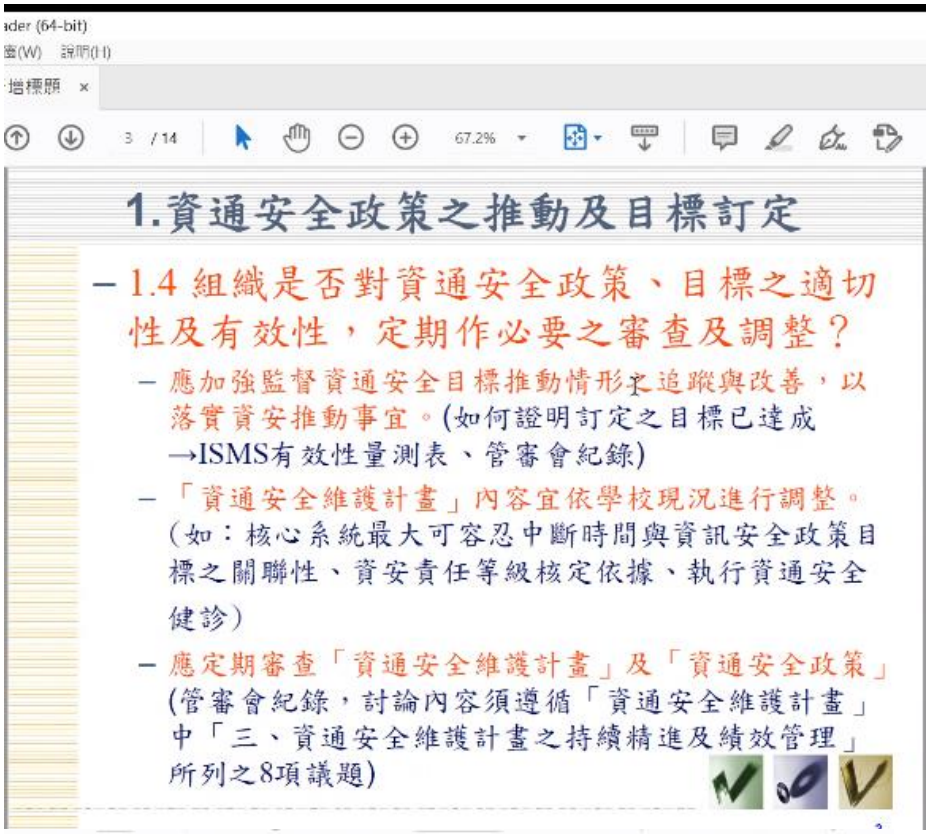
一、相關法規及參考文件

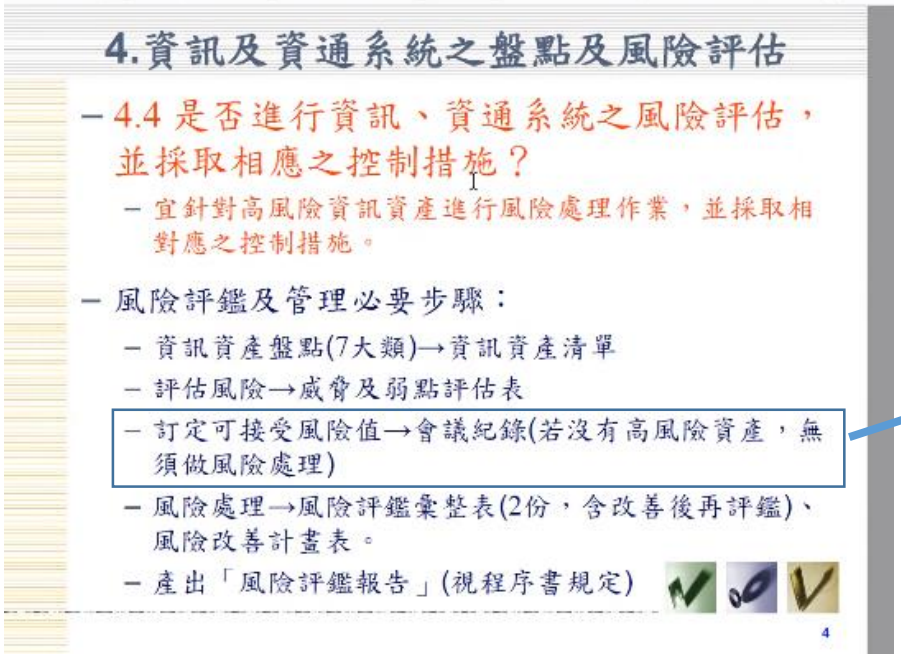
1. 資通安全管理法
2. 資通安全管理法施行細則
3. 資通安全責任等級分級辦法
4. 資通安全事件通報及應變辦法
5. 資通安全情資分享辦法
6. 公務機關所屬人員資通安全事項獎懲辦法
7. 資訊系統風險評鑑參考指引
8. 政府資訊作業委外安全參考指引
9. 無線網路安全參考指引
10. 網路架構規劃參考指引
11. 行政裝置資安防護參考指引
12. 政府行動化安全防護規劃報告
13. 安全軟體發展流程指引
14. 安全軟體設計指引
15. 安全軟體測試指引

16. 資訊作業委外安全參考指引

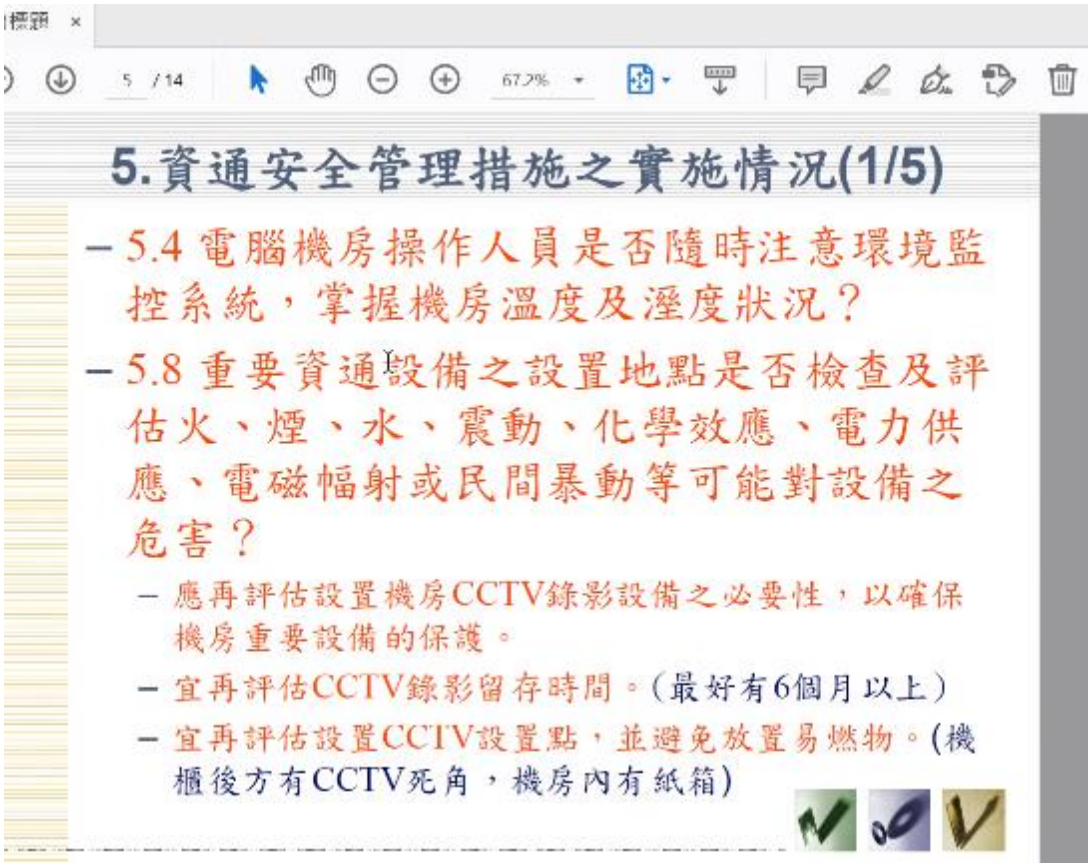
二、附件資料表單

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


ader (64-bit)
書(W) 說明(H)
增標題
3 / 14
67.2%
1.資通安全政策之推動及目標訂定
– 1.4 組織是否對資通安全政策、目標之適切性及有效性，定期作必要之審查及調整？
– 應加強監督資通安全目標推動情形之追蹤與改善，以落實資安推動事宜。(如何證明訂定之目標已達成→ISMS有效性量測表、管審會紀錄)
– 「資通安全維護計畫」內容宜依學校現況進行調整。(如：核心系統最大可容忍中斷時間與資訊安全政策目標之關聯性、資安責任等級核定依據、執行資通安全健診)
– 應定期審查「資通安全維護計畫」及「資通安全政策」(管審會紀錄，討論內容須遵循「資通安全維護計畫」中「三、資通安全維護計畫之持續精進及績效管理」所列之8項議題)


4.資訊及資通系統之盤點及風險評估
– 4.4 是否進行資訊、資通系統之風險評估，並採取相應之控制措施？
– 宜針對高風險資訊資產進行風險處理作業，並採取相對應之控制措施。
– 風險評鑑及管理必要步驟：
– 資訊資產盤點(7大類)→資訊資產清單
– 評估風險→威脅及弱點評估表
– 訂定可接受風險值→會議紀錄(若沒有高風險資產，無須做風險處理)
– 風險處理→風險評鑑彙整表(2份，含改善後再評鑑)、風險改善計畫表。
– 產出「風險評鑑報告」(視程序書規定)
4

需有會議


標題
5 / 14
67.2%
5.資通安全管理措施之實施情況(1/5)
– 5.4 電腦機房操作人員是否隨時注意環境監控系統，掌握機房溫度及溼度狀況？
– 5.8 重要資通設備之設置地點是否檢查及評估火、煙、水、震動、化學效應、電力供應、電磁幅射或民間暴動等可能對設備之危害？
– 應再評估設置機房CCTV錄影設備之必要性，以確保機房重要設備的保護。
– 宜再評估CCTV錄影留存時間。(最好有6個月以上)
– 宜再評估設置CCTV設置點，並避免放置易燃物。(機櫃後方有CCTV死角，機房內有紙箱)

5.資通安全管理措施之實施情況(2/5)

- 5.15 公文及儲存媒體在不使用或不在班時是否妥為存放？機密性、敏感性資訊是否妥為收存？
  - 辦公場所應加強文件保存管制措施。(辦公場所文件保存狀況、個人電腦資源回收筒等)
- 5.19 是否定期執行各項系統漏洞修補程式？
  - 宜再加強個人電腦的資訊安全防護與控管。(螢幕保護設定、7-zip版本過舊、安裝WinRAR非授權軟體、密碼超過時間未變更等、Windows系統更新等)

6

5.資通安全管理措施之實施情況(3/5)

- 5.22 備份資料是否定期回復測試，以確保備份資料之有效性？
  - 宜定期進行資料備份回復測試與演練作業，以確保備份資料之可用性。(演練紀錄)
- 5.23 對於敏感性、機密性資訊之傳送是否採取資料加密等保護措施？
  - 傳送機敏性資料檔案應進行加密保護。(如：新生資料)

5.資通安全管理措施之實施情況(4/5)

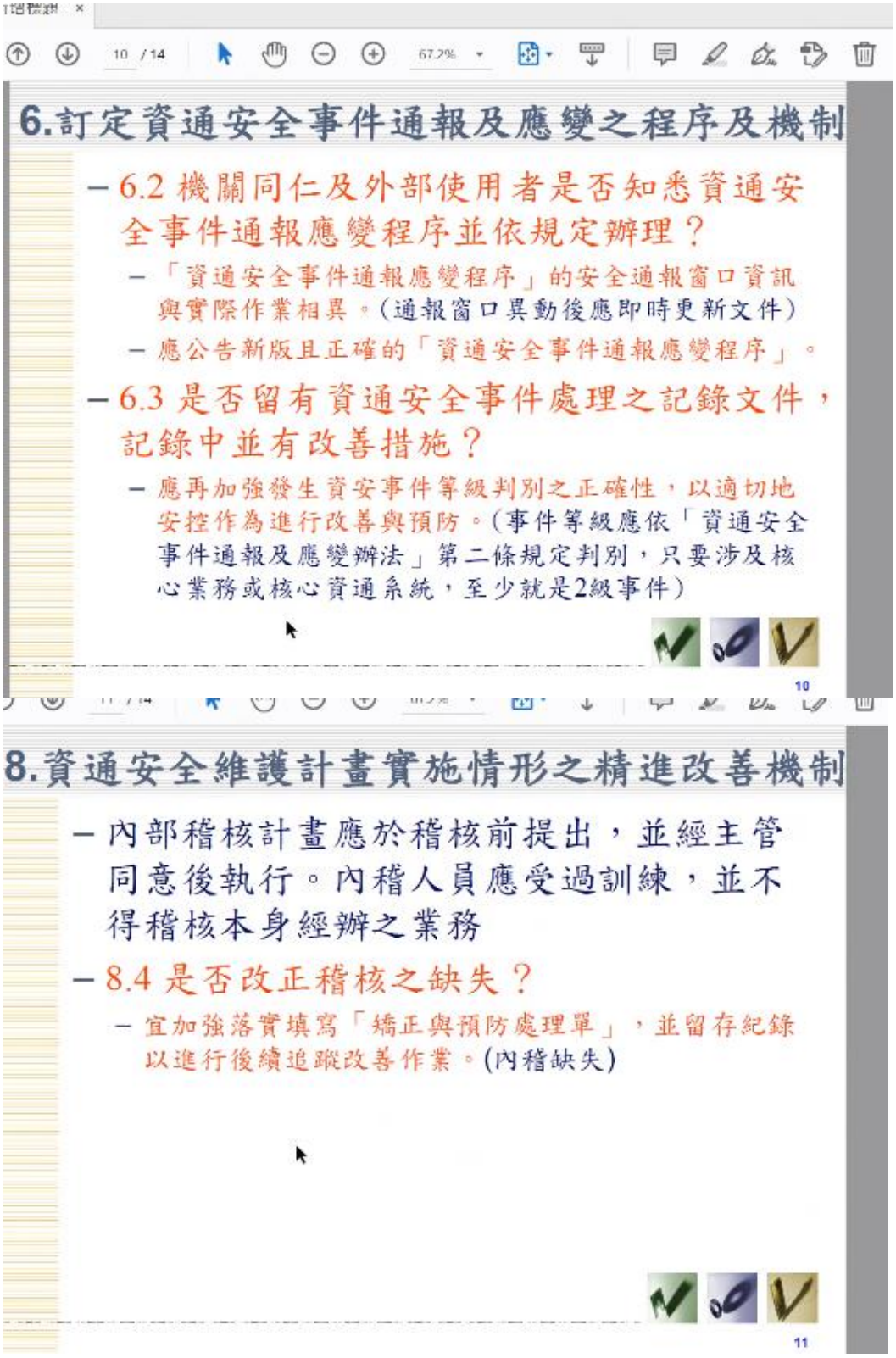
- 5.26 使用者存取權限是否定期檢查(建議每六個月一次)或在權限變更後立即複檢？
  - 系統帳號應加強帳號管理並禁止共用帳號。
  - 機房重要設備與電腦系統應定期審查系統的特權帳號權限。(帳號清查範圍應包含所有主機、應用系統及網路設備→帳號清查紀錄表、帳號清查結果報告)
- 5.27 通行碼長度是否超過8個字元？
- 5.28 通行碼是否規定需有大小寫字母、數字及符號組成？
  - 通行碼宜依規定長度超過8個字元，並由大小寫字母、數字及符號組成。

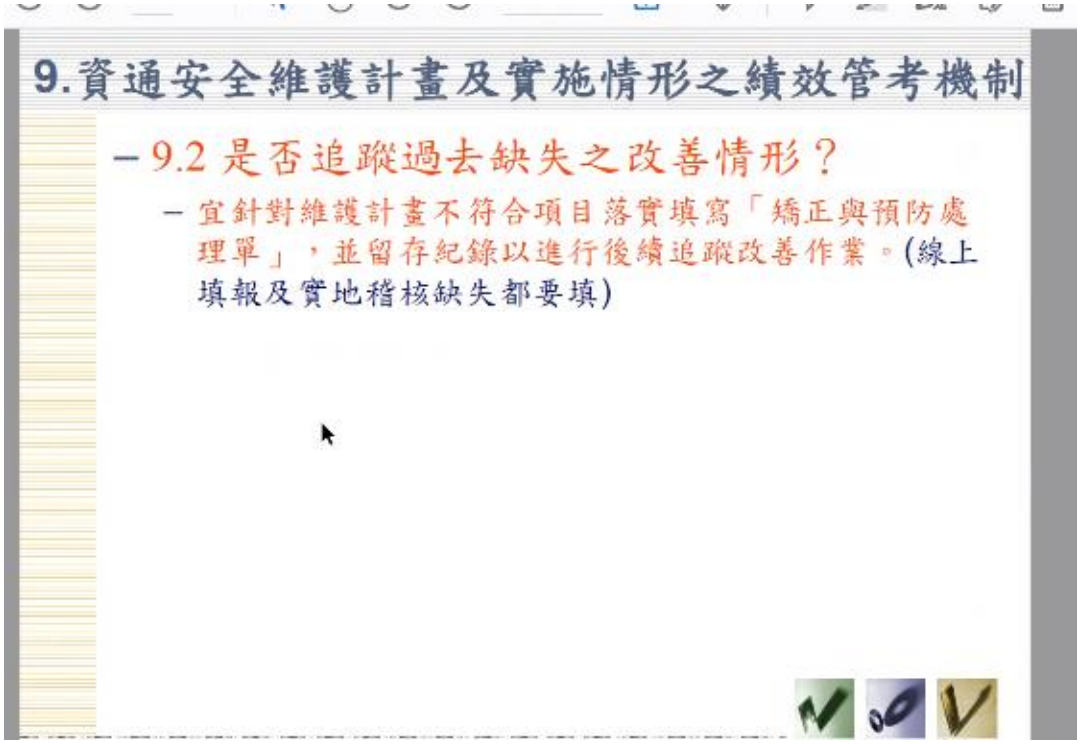
8

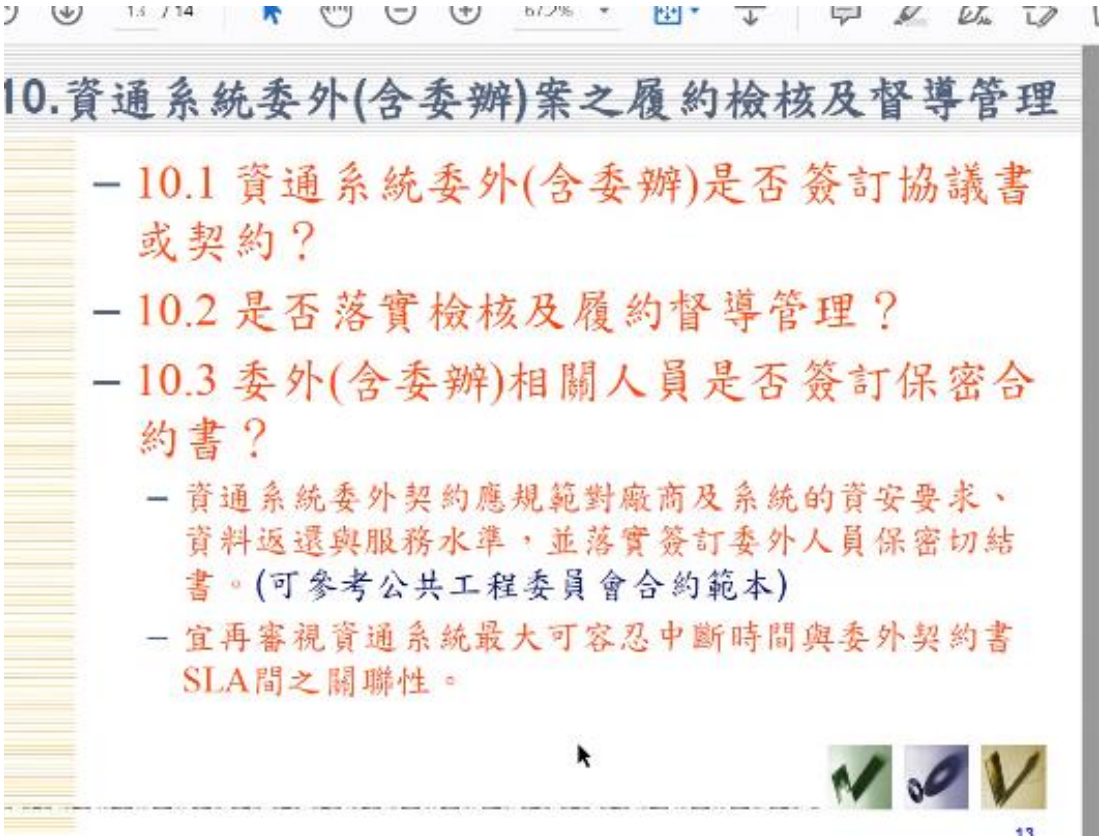
5.資通安全管理措施之實施情況(5/5)

- 5.29 是否依網路型態(Internet、Intranet、Extranet)訂定適當的存取權限管理方式？
  - 機房區域網路宜與行政區域網路區隔。
  - 宜再審慎評估防火牆規則。(注意外對內全開之規則)
- 5.30 對於重要特定網路服務，是否作必要之控制措施，如身份鑑別、資料加密或網路連線控制？
  - 對外網頁服務應採用https加密機制。
  - 應針對重要特定網路服務，作必要之控制措施。(限制防火牆管理者網路連線來源)

9


10 / 14
67.2%
6.訂定資通安全事件通報及應變之程序及機制
– 6.2 機關同仁及外部使用者是否知悉資通安全事件通報應變程序並依規定辦理？
– 「資通安全事件通報應變程序」的安全通報窗口資訊與實際作業相異。(通報窗口異動後應即時更新文件)
– 應公告新版且正確的「資通安全事件通報應變程序」。
– 6.3 是否留有資通安全事件處理之記錄文件，記錄中並有改善措施？
– 應再加強發生資安事件等級判別之正確性，以適切地安控作為進行改善與預防。(事件等級應依「資通安全事件通報及應變辦法」第二條規定判別，只要涉及核心業務或核心資通系統，至少就是2級事件)
10
8.資通安全維護計畫實施情形之精進改善機制
– 內部稽核計畫應於稽核前提出，並經主管同意後執行。內稽人員應受過訓練，並不得稽核本身經辦之業務
– 8.4 是否改正稽核之缺失？
– 宜加強落實填寫「矯正與預防處理單」，並留存紀錄以進行後續追蹤改善作業。(內稽缺失)
11


9.資通安全維護計畫及實施情形之績效管考機制
－9.2 是否追蹤過去缺失之改善情形？
－宜針對維護計畫不符合項目落實填寫「矯正與預防處理單」，並留存紀錄以進行後續追蹤改善作業。(線上填報及實地稽核缺失都要填)


10.資通系統委外(含委辦)案之履約檢核及督導管理
– 10.1 資通系統委外(含委辦)是否簽訂協議書或契約？
– 10.2 是否落實檢核及履約督導管理？
– 10.3 委外(含委辦)相關人員是否簽訂保密合約書？
– 資通系統委外契約應規範對廠商及系統的資安要求、資料返還與服務水準，並落實簽訂委外人員保密切結書。(可參考公共工程委員會合約範本)
– 宜再審視資通系統最大可容忍中斷時間與委外契約書SLA間之關聯性。