國立臺灣師範大學附屬高級中學
資通安全維護計畫

目　　錄

壹、依據及目的

本計畫依據資通安全管理法第10條及施行細則第6條訂定。

貳、適用範圍

本計畫適用範圍涵蓋國立臺灣師範大學附屬高級中學全機關（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
學生資料管理	臺北市高中第二代校務行政系統（已向上集中至臺北市政府）	為本校依組織法執掌，足認為重要者	學生成績資料無法輸入及查詢。 學生出缺席狀況無法統計與查詢。	24小時	中
學生學習成果資料管理	學習歷程檔案（已向上集中至臺北市政府）	為本校依組織法執掌，足認為重要者	學生學習成果無法上傳及審核	24小時	中
網域名稱管理	DNS（已向上集中至國教署）	為本校依組織法執掌，足認為重要者	無法連線到指定主機	24小時	普
郵件服務	Mail server（使用教育雲端帳號）	為本校依組織法執掌，足認為重要者	無法處理郵件，影響對外網路聯繫，降低公	24小時	普

			務處理效率。		
公告各項校務相關訊息	高中部官網（已向上集中至成大）	為本校依組織法執掌，足認為重要者	發生資通安全事件致資通系統受影響時，可能造成未經授權之資訊揭露，對機關之營運、資產或信譽等方面將產生嚴重之影響。	24小時	中
公告各項校務相關訊息	國中部官網（已向上集中至成大）	為本校依組織法執掌，足認為重要者	發生資通安全事件致資通系統受影響時，可能造成未經授權之資訊揭露，對機關之營運、資產或信譽等方面將產生嚴重之影響。	24小時	中

附註：

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
差勤電子表單系統（國教署維運）	發生資通安全事件致資通系統受影響時，可能造成未經授權之資訊揭露，對機關之營運、資產或信譽等方面將產生嚴重之影響。	24小時	普
校務基金會計管理系統（國教署維運）	會計帳務無法處理時，對主管機關及學校、廠商等產生嚴重影響	24小時	普
公文簽核&檔案管理系統	無法收發公文，影響機關行政效率	48小時	普
財產管理系統	致本校財產管理產生窒礙難行之嚴重影響	72小時	普
圖書館自動化系統	借還書資料遺失，如讀者未依規定還書，無從催還，可能連帶造成財產的損失。	8工作小時	普

附註：

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

一、資通安全政策

為使本校業務順利運作，防止資訊或資通系統受未經授權之存取、使用、控制、洩漏、破壞、竄改、銷毀或其他侵害，並確保其機密性（Confidentiality）、完整性（Integrity）及可用性（Availability），特制訂本政策如下，以供全體同仁共同遵循：

1. 建立資通安全風險管理機制，定期因應內外在資通安全情勢變化，檢討資通安全風險管理之有效性。
2. 保護機敏資訊及資通系統之機密性與完整性，避免未經授權的存取與竄改。
3. 應強固核心資通系統之韌性，確保機關業務持續營運。
4. 因應資通安全威脅情勢變化，辦理資通安全教育訓練，以提高本校同仁之資通安全意識，本校同仁亦應確實參與訓練。
5. 針對辦理資通安全業務有功人員應進行獎勵。
6. 勿開啟來路不明或無法明確辨識寄件人之電子郵件。
7. 禁止多人共用單一資通系統帳號。

二、資通安全目標

(一) 量化型目標

1. 知悉資安事件發生，能於規定的時間完成通報、應變及復原作業。
2. 電子郵件社交工程演練之程郵件開啟率應低於10%（含），社交工程郵件點閱率應低於6%（含）及社交工程郵件附件開啟率應低於2%（含）。

(二) 質化型目標

1. 適時因應法令與技術之變動，調整資通安全維護之內容，以避免資通系統或資訊遭受未經授權之存取、使用、控制、洩漏、破壞、竄改、銷毀或其他侵害，以確保其機密性、完整性及可用性。

2. 達成資通安全責任等級分級之要求，並降低遭受資通安全風險之威脅。

3. 提升人員資安防護意識、防止發生中毒或入侵事件。

三、資通安全政策及目標之核定程序

本政策經資通安全委員會核定後實施，修訂時亦同。

四、資通安全政策及目標之宣導

1. 本校之資通安全政策及目標應每年透過教育訓練、內部會議、張貼公告等方式，向機關內所有人員進行宣導，並檢視執行成效。

2. 本校應每年進行資安政策及目標宣導，並檢視執行成效。

五、資通安全政策及目標定期檢討程序

資通安全政策及目標應定期於資通安全管理審查會議中檢討其適切性。

伍、資通安全推動組織

一、資通安全長

依資通安全管理法第11條之規定，本校訂定校長為資通安全長，負責推動及督導機關資通安全相關事項，其任務包括：

1. 資通安全管理政策及目標之核定及督導。

2. 資通安全責任之分配及協調。

3. 資通安全資源分配。

4. 資通安全防護措施之監督。

5. 資通安全事件之檢討及監督。

6. 資通安全相關規章與程序、制度文件核定。

7. 資通安全管理年度工作計畫之核定

8. 資通安全相關工作事項督導及績效管理。

9. 其他資通安全事項之核定。

二、資通安全推動小組

(一) 組織

為推動本校之資通安全相關政策、落實資通安全事件通報及

相關應變處理，由資通安全長召集各業務部門主管成立資通安全推動小組，其任務包括：

1. 跨部門資通安全事項權責分工之協調。
2. 應採用之資通安全技術、方法及程序之協調研議。
3. 整體資通安全措施之協調研議。
4. 資通安全計畫之協調研議。
5. 其他重要資通安全事項之協調研議。

(二) 分工及職掌

本校之資通安全推動小組依下列分工進行責任分組，並依資通安全長指示負責下列事項，本校資通安全推動小組分組人員名單及職掌應列冊，並適時更新之：

1. 策略規劃組：
   (1) 資通安全政策及目標之研議。
   (2) 訂定本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。
   (3) 依據資通安全目標擬定年度工作計畫。
   (4) 傳達資通安全政策與目標。
   (5) 其他資通安全事項之規劃。
2. 資安防護組：
   (1) 資通安全技術之研究、建置及評估相關事項。
   (2) 資通安全相關規章與程序、制度之執行。
   (3) 資訊及資通系統之盤點及風險評估。
   (4) 資料及資通系統之安全防護事項之執行。
   (5) 資通安全事件之通報及應變機制之執行。
   (6) 其他資通安全事項之辦理與推動。

陸、人力及經費配置

一、 人力及資源之配置

1. 依資通安全責任等級分級辦法之規定暨國教署112年11月1日臺教國署資字第1120146074號函示，本校資安責任等

級核定為 D 級。最低應設置資通安全人員1人。

2. 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業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。
3. 本校負責重要資通系統之管理、維護、設計及操作之人員，若負有機密維護責任者，應簽屬「保密切結書」如文件編號 HSNU-ISMS-D-016，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. 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。

二、經費之配置

1. 資通安全推動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. 各單位如有資通安全資源之需求，應配合機關預算規劃期程向資通安全推動小組提出，由資通安全推動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。
3. 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

1. 本校每年辦理資訊及資通系統資產盤點，依管理責任指定對應之資產管理人，並依資產屬性進行分類。
2. 資訊及資通系統資產項目如下：
   (1) 資訊資產：以數位等形式儲存之資訊，如資料庫、資料檔案、系統文件、操作手冊、訓練教材、研究

報告、作業程序、永續運作計畫、稽核紀錄及歸檔之資訊等。

(2) 軟體資產：應用軟體、系統軟體、開發工具、套裝軟體及電腦作業系統等。

(3) 實體資產：電腦及通訊設備、可攜式設備及資通系統相關之設備等。

(4) 支援服務資產：相關基礎設施及其他機關內部之支援服務，如電力、消防等。

(5) 人員：包含全體同仁以及委外廠商。

3. 本校應依資訊及資通系統盤點結果製作「資訊及資通系統資產清冊」，欄位應包含：資訊及資通系統名稱、資產名稱、資產類別、擁有者、管理者、使用者、存放位置、防護需求等級。

4. 資訊及資通系統資產應以標籤標示於設備明顯處，並載明財產編號、保管人、廠牌、型號等資訊。

5. 各單位管理之資訊或資通系統如有異動，應即時通知資通安全推動小組更新資產清冊。

二、機關資通安全責任等級分級

依資通安全責任等級分級辦法之規定暨國教署112年11月1日臺教國署資字第1120146074號函示，本校資安責任等級核定為D級。

捌、資通安全風險評估

一、 資通安全風險評估

1. 本校應每年針對資訊及資通系統資產進行風險評估。

2. 資通安全推動小組應每年召開會議檢討可接受風險值，並適當調整。

3. 風險值的計算

風險值=（資訊資產價值×威脅等級×弱點等級）

4. **資訊資產價值**之決定將依據資訊資產之機密性、完整性及可用性評估之後，取三者之最大值以為資訊資產之價值。

(1) 機密性評估標準

評估標準	數值
普：發生資通安全事件致資通系統受影響時，可能造成未經授權之資訊揭露，對機關之營運、資產或信譽等方面將產生有限之影響。	1
中：發生資通安全事件致資通系統受影響時，可能造成未經授權之資訊揭露，對機關之營運、資產或信譽等方面將產生嚴重之影響。	2
高：發生資通安全事件致資通系統受影響時，可能造成未經授權之資訊揭露，對機關之營運、資產或信譽等方面將產生非常嚴重或災難性之影響。	3

(2) 完整性評估標準

評估標準	數值
普：發生資通安全事件致資通系統受影響時，可能造成資訊錯誤或遭竄改等情事，對機關之營運、資產或信譽等方面將產生有限之影響。	1
中：發生資通安全事件致資通系統受影響時，可能造成資訊錯誤或遭竄改等情事，對機關之營運、資產或信譽等方面將產生嚴重之影響。	2
高：發生資通安全事件致資通系統受影響時，可能造成資訊錯誤或遭竄改等情事，對機關之營運、資產或信譽等方面將產生非常嚴重或災難性之影響。	3

(3) 可用性評估標準

評估標準	數值
普：發生資通安全事件致資通系統受影響時，可	1

能造成對資訊、資通系統之存取或使用之中斷，對機關之營運、資產或信譽等方面將產生有限之影響。	
中：發生資通安全事件致資通系統受影響時，可能造成對資訊、資通系統之存取或使用之中斷，對機關之營運、資產或信譽等方面將產生嚴重之影響。	2
高：發生資通安全事件致資通系統受影響時，可能造成對資訊、資通系統之存取或使用之中斷，對機關之營運、資產或信譽等方面將產生非常嚴重或災難性之影響。	3

5. 威脅等級對應表

評估標準	評估值
威脅發生之可能性為低	1
威脅發生之可能性為中	2
威脅發生之可能性為高	3

6. 弱點等級對應表

評估標準	評估值
弱點不容易被威脅利用	1
弱點容易被威脅利用	2
弱點非常容易被威脅利用	3

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
臺北市高中第二代校務行政系統	已向上集中至台北市政府	學生資料管理	24小時

學習歷程檔案	已向上集中至台北市政府	學生學習成果資料管理	24小時
Mail server	使用教育雲端帳號	郵件服務	24小時
DNS	已向上集中至國教署	網域名稱管理	24小時
高中部官網	已向上集中至國教署（成功大學）	公告各項校務相關訊息	24小時
國中部官網	已向上集中至國教署（成功大學）	公告各項校務相關訊息	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

(一) 資訊及資通系統之保管

1. 管理人應確保資通系統及資訊已盤點造冊並適切分級，並持續更新以確保其正確性。
2. 管理人應確保資通系統及資訊被妥善的保存或備份。
3. 管理人應確保重要之資通系統及資訊已採取適當之存取控制政策。

(二) 資訊及資通系統之使用

1. 本校同仁使用資訊及資通系統前應經其管理人授權。
2. 本校同仁使用資訊及資通系統時，應留意其資通安全要求事項，並負對應之責任。
3. 本機關同仁使用資訊及資通系統後，應依規定之程序歸還。資訊類資訊之歸還應確保相關資訊已正確移轉，並安全地自原設備上抹除。
4. 非本校同仁使用本機關之資訊及資通系統，應確實遵守本機關之相關資通安全要求，且未經授權不得任意複製

資訊。

5. 對於資訊及資通系統，宜識別並以文件記錄及實作可被接受使用之規則。

(三) 資訊及資通系統之刪除或汰除

1. 資訊及資通系統之刪除或汰除前應評估機關是否已無需使用該等資訊及資通系統，或該等資訊及資通系統是否已妥善移轉或備份。
2. 資訊及資通系統之刪除或汰除時宜加以清查，以確保所有機敏性資訊及具使用授權軟體已被移除或安全覆寫。
3. 具機敏性之資訊或具授權軟體之資通系統，宜採取實體銷毀，或以毀損、刪除或覆寫之技術，使原始資訊無法被讀取，並避免僅使用標準刪除或格式化功能。

二、存取控制與加密機制管理

(一) 網路安全控管

1. 使用者不得於辦公室內私裝電腦及網路通訊等相關設備。
2. 使用者應遵守網路安全規定，如有違反網路安全情事，應依資訊安全規定，限制或撤銷其網路資源存取權利。

(二) 權限管理

1. 密碼設置原則，應避免使用易猜測或個人資訊為設定，並應滿足：
   (1) 長度8碼以上。
   (2) 複雜度應包含英文大寫、小寫、特殊符號或數字三種以上。
   (3) 資訊系統之系統管理者應至少每3個月變更密碼，一般使用者應至少每6個月變更密碼。
2. 應依使用者業務需要開通帳號權限，且不得共用帳號。
3. 使用者無繼續使用資通系統時，應立即停用或移除使用者帳號。

(三) 加密管理

1. 機密資訊於儲存或傳輸時應進行加密。
2. 加密保護措施應避免留存解密資訊，若加密資訊具遭破

解跡象，應立即更改之。

三、作業與通訊安全管理

(一) 防範惡意軟體之控制措施

1. 本校之主機及個人電腦應安裝防毒軟體，並適時維護軟、硬體。
2. 任何形式之儲存媒體所取得之檔案，應確定有無惡意程式或病毒。
3. 使用者未經同意不得私自安裝來路不明、有違法疑慮或與業務無關的軟體。

(二) 電子郵件安全管理

1. 使用者使用電子郵件時應提高警覺，避免讀取來歷不明之郵件。
2. 原則不得電子郵件傳送機密性或敏感性之資料，如有業務需求者應依相關規定進行加密或其他之防護措施。
3. 使用者不得利用機關所提供電子郵件服務從事侵害他人權益或違法之行為。
4. 本校應配合上級機關舉辦電子郵件社交工程演練，並檢討執行情形。

(三) 確保實體與環境安全措施

1. 應考量採用辦公桌面的淨空政策，以減少機密資訊、文件及可移除式媒體等在辦公時間之外遭未被授權的人員取用、遺失或是被破壞的機會。
2. 資訊或資通系統相關設備應妥善存放，未經管理人授權，不得被帶離辦公室。

(四) 媒體防護措施

1. 使用隨身碟或磁片等存放資料時，具機密性、敏感性之資料應妥善保管。
2. 資訊如以實體儲存媒體方式傳送，應留意實體儲存媒體之包裝，選擇適當人員進行傳送。

(五) 電腦使用之安全管理

1. 個人電腦（含可攜式電腦）不使用時，應立即登出或啟

動螢幕保護程式及螢幕保護密碼，並將螢幕逾時設定為10分鐘以內。

2. 禁止安裝使用未經合法授權軟體。
3. 個人電腦應定期進行更新作業系統及防毒病毒碼等。
4. 如發現資安問題，應主動循機關之通報程序通報。
5. 重要資料應定期備份。

四、資通安全防護設備

1. 本機關應建置防毒軟體、網路防火牆應適時進行軟、硬體更新及維護作業。
2. 網路防火牆設定檔必要時應進行備份作業。

壹拾、 資通安全事件通報及應變相關機制

一、本校遵守教育部所訂定之資通安全事件通報、應變及演練相關機制。

二、本校資通安全事件通報窗口為資訊室。

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。

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

由資通安全推動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。

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。

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保密切結書，格式如：文件編號 HSNU-ISMS-D-024「委外廠商保密切結書」。
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「委外廠商自我檢核表」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

本校依資通安全責任等級分級屬D級，資通安全人員、一般使用者與主管，每人每年應接受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. 資通安全推動小組應考量管理、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，以建立教職員工資通安全認知，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。
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. 教職員工報到時，應使其充分瞭解本校資通安全相關作業規範及其重要性。

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內部檢查機制

資通安全內部檢查小組應定期(至少每二年一次)執行一次內部檢查作業，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。

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每年至少召開二次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) 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。

(2) 資通安全維護計畫內容之適切性。

(3) 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.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.不符合項目及矯正措施。

(4) 風險評鑑結果及風險處理計畫執行進度。

(5) 重大資通安全事件之處理及改善情形。

(6) 利害關係人之回饋。

(7) 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」如文件編號 HSNU-ISMS-D-047，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

本校依據資通安全管理法第12條之規定，應每年向上級或監督機關提出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

二、附件資料表單

HSNU-ISMS-D-001 資通安全組織成員表

HSNU-ISMS-D-016 保密切結書

HSNU-ISMS-D-024 委外廠商保密切結書

HSNU-ISMS-D-045 資訊安全管理制度內部檢查表

HSNU-ISMS-D-047 矯正與預防處理單

委外廠商自我檢核表