臺北市立松山高級商業家事職業學校

資訊安全維護計畫

第 1.1 版

生效日期：110 年 10 月 21 日

文件制／修訂紀錄表

文件版本	生效日期	制／修定摘要說明	承辦單位	承辦人
V1.0	108 年 2 月 25 日	初次建立	教務處	葉育如
V1.1	110 年 10 月 21 日	附件 1.推動小組成員新增設備組長及代理人	教務處	林世宗

【目錄】

壹、依據及目的

本計畫依據資通安全管理法第 10 條及其施行細則第 6 條訂定。

貳、適用範圍

本計畫適用範圍涵蓋本機關。

參、核心業務及重要性

一、核心業務及重要性：

本機關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
教務業務 1.課程編排、教學實施、學籍管理、成績評量，並與學務、輔導單位配合實施教育輔導等事項 2.提供資訊服務	學籍系統 (配合資訊向上集中，將移往教育局)	為本機關依組織法執掌，足認為重要者	影響教務、學務、輔導業進行及網路服務。	無
學生事務：衛生保健、學生團體活動，並與教務、輔導單位配合實施生活輔導等事項。	學籍系統 (配合資訊向上集中，將移往教育局)	為本機關依組織法執掌，足認為重要者	影響教務、學務、輔導業務進行。	無
總務業務：學校文書、事務、財物管理及出納等事項	無	為本機關依組織法執掌，足認為重要者	無	無
輔導業務:學生資料蒐集與分析、學生智力、性向、人格等測驗之實施，學生興趣、學習成就與志願之調查、輔導諮商之進行，並辦理特殊教育及親職教育等事項。	學籍系統 (配合資訊向上集中，將移往教育局)	為本機關依組織法執掌，足認為重要者	影響教務、學務、輔導業務進行。	無
圖書管理業務	無	為本機關依組織法執掌，足認為重要者	無	無

各欄位定義：
1.核心業務名稱：請參考資通安全管理法施行細則第 7 條之規定列示。
2.作業名稱：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.最大可容忍中斷時間單位以小時計。

二、非核心業務及說明：

本機關之非核心業務及說明如下表：

非核心業務	業務失效影響說明	最大可容忍中斷時間
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
WWW、DNS、人事差勤系統、集中支付系統、財產管理系統、電	影響機關行政效率	無

子相簿、電子書、題庫系統、Radius、DHCP、線上資料庫、線上維修系統、場地借用系統、會議預約系統		

各欄位定義：
1.業務名稱：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。(請依機關實際情形列出)
2.作業名稱：該項業務內各項作業程序的名稱。
3.說明：說明該業務之內容。
4.最大可容忍中斷時間單位以小時計。

肆、資通安全政策及目標

一、資通安全政策

為使本機關業務順利運作，防止資訊或資通業務受未經授權之存取、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：

(一)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。

(二)針對各資料的機密性與完整性應妥善保護，避免資料遭竄改。

(三)建立資通安全防護(如:防火牆、防毒軟體)。

(四)辦理資通安全教育訓練(一般使用者與主管，每人每年三小時以上之一般資通安全教育訓練)，提升同仁資通安全意識。

(五)針對辦理資通安全業務有功相關人員應依資通安全管理法子法之「公務機關所屬人員資通安全事項獎懲辦法」進行獎勵。

(六)禁止多人共用同一帳號。

(七)落實資通安全通報機制。

二、資通安全目標

(一)資安事件發生，於規定的時間完成通報、應變及復原作業。

(二)配合上級機關辦理之電子郵件社交工程演練郵件開啟率及附件點閱率分別低於10%及6%。

(三)全年度資安通報平臺之資安事件等級第1、2級發生件數少於3件(含)以下，等級第3、4級不得發生。

(四)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。

三、資通安全政策及目標核定程序

資通安全政策由教務處提至資訊教育推動小組會議討論，通過後實施。

四、資通安全政策及目標之宣導

(一)本機關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。

(二)本機關應每年向利害關係人(例如社團報名系統委由廠商提供服務(非本機關維運自行或委由廠商建置之資通系統))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訊教育推動小組會議中檢討其適切性。

伍、資通安全推動組織

一、資通安全長

本機關訂定校長為資通安全長，負責督導機關資通安全相關事項，其任務包括：

資通安全管理政策及目標之核定、核轉及督導。

(一)資通安全責任之分配及協調。

(二)資通安全資源分配。

(三)資通安全防護措施之監督。

(四)資通安全事件之檢討及監督。

(五)資通安全相關規章與程序、制度文件核定。

(六)資通安全管理年度工作計畫之核定。

(七)資通安全相關工作事項督導及績效管理。

(八)其他資通安全事項之核定。

二、資訊安全小組(資訊教育推動小組兼辦)

(一)組織

為推動本機關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以上之人員代表成立資訊教育推動小組，其任務包括：

1.跨處室資通安全事項權責分工之協調。

2.整體資通安全措施之協調研議。

3.資通安全計畫之協調研議。

4.其他重要資通安全事項之協調研議。

(二)分工及職掌

本機關之資訊教育推動小組依下列分工進行責任分組，並依資通安全長之指示負責下列事項，本機關資訊教育推動小組分組人員名單及職掌應列冊(附件 1)，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)訂定機關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機關年度工作計畫。

(4)傳達機關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)資通安全相關規章與程序、制度之執行。

(2)資料及資通系統之安全防護事項之執行。

(3)資通安全事件之通報及應變機制之執行。

(4)其他資通安全事項之辦理與推動。

3.績效管理組：

(1)辦理資通安全內部稽核。

(2)每年 10 月前召開資通安全管理審查會議，提報資通安全事項執行情形，以利教育部稽核審查使用。

(3)成員由資通安全長指派之。

陸、專職人力及經費配置

一、人力及資源配置

(一)本機關依資通安全責任等級分級辦法之規定，屬資通安全責任等級 D 級，最低應設置資通安全兼辦人員 1 人，人員名單及職掌應列冊(附件 1)，並適時更新。

(二)本機關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，並提升機關內資通安全專業人員之資通安全管理能力。本機關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。

(三)本機關負責重要資通設備之管理、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(附件 2)，並視需要實施人員輪調，建立人力備援制度。

(四)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。

(五)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。

二、經費配置

(一)資訊教育推動小組於規劃配置相關經費及資源時，應考量本機關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。

(二)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

(一)本機關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，分別為資訊資產、軟體資產、實體資產、支援服務資產等。

(二)資訊及資通系統資產項目如下：

資產類別	資產項目
軟體資產	附件 3。
硬體資產	附件 3。
服務資產	附件 3。
人員資產	附件 1。
個資資產	(1) 紙本個資：教職員通訊錄。

	(2) 資料庫個資，學籍系統學生個人資料檔案。

(三)本機關每年度應執行財物盤點，欄位應包含：資產名稱、資產類別、使用者、保管者、存放位置。

(四)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。

(五)各單位管理之資訊或資通系統如有異動，應即時填具財物移轉單，並確實移轉使用者及保管者。

二、機關資通安全責任等級分級

本機關配合資訊資源向上集中計畫，核心資通系統由上級或監督機關兼辦或代管，資通安全責任等級為 D 級。

捌、資通安全防護及控制措施

本機關之防護及控制措施詳如本機關資通安全維護計畫，採行相關之防護及控制措施如下:

一、資訊及資通設備之管理

(一) 資訊及資通設備之使用

1.本機關同仁使用資訊及資通設備須遵守設備管理相關規範。

2.本機關同仁使用資訊及資通設備時，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設備後，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.非本機關同仁使用本機關之資訊及資通設備，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.對於資訊及資通設備，宜識別並以文件記錄及實作可被接受使用之規則。

二、存取控制與加密機制管理

(一) 網路安全控管

1.本機關之防火牆區域劃分如下：

(1)外部網路：對外網路區域，連接外部廣網路(Wide Area Network, WAN)。

(2)內部區域網路(Local Area Network, LAN)：機關內部單位人員及內部伺服器使用之網路區段。

2.外部網路及內部區域網路間連線需經防火牆進行存取控制，非允許的服務與來源不能進入其他區域。

3.本機關應定期檢視防火牆政策是否適當。

4.本機關內部網路之區域應做合理之區隔，使用者應經授權後在授權之範圍內存取網路資源。

5.對網路系統管理人員或資通安全主管人員的操作，均應建立詳細的紀錄。並應定期檢視網路安全相關設備設定規則與其日誌紀錄，並檢討執行情形。

6.使用者應依機關規定之方式存取網路服務。

7.網域名稱系統(DNS)防護

(1)一般伺服器應關閉 DNS 服務，防火牆政策亦應針對 DNS 進行控管，關閉不需要的 DNS 服務存取。

(2)DNS 伺服器應經常性進行弱點漏洞管理與修補、落實存取管控機制。

(3)內部主機位置查詢應指向機關內部 DNS 伺服器。

8.無線網路防護

(1)機密資料原則不得透過無線網路及設備存取、處理或傳送。

(2)無線設備應具備安全防護機制以降低阻斷式攻擊風險，且無線網路之安全防護機制應包含外來威脅及預防內部潛在干擾。

(3)用以儲存或傳輸資料且具無線傳輸功能之個人電子設備與工作站，應安裝防毒軟體，並定期更新病毒碼。

(二) 資通業務權限管理

1.本機關之資通業務應設置通行碼管理，通行碼之要求需滿足：

(1)通行碼長度 8 碼以上。

(2)通行碼複雜度應包含英文大寫小寫、特殊符號或數字三種以上。

(3)使用者每 90 天應更換一次通行碼。

2.使用者辦理資通業務前應經授權，並使用唯一之使用者 ID，除有特殊營運或作業必要經核准並紀錄外，不得共用 ID。

3.使用者無繼續辦理資通業務時，應立即停用或移除使用者 ID，資通業務管理者應定期清查使用者之權限。

(三) 特權帳號之存取管理

1.資通設備之特權帳號請應經正式申請授權方能使用，特權帳號授權前應妥善審查其必要性，其授權及審查記錄應留存。

2.資通設備之特權帳號不得共用。

3.對於特權帳號，宜指派與該使用者日常公務使用之不同使用者 ID。

4.資通設備之特權帳號應妥善管理，並應留存特殊權限帳號之使用軌跡。

5.資通設備之管理者每季應清查系統特權帳號並劃定特權帳號逾期之處理方式。

(四) 加密管理

1.本機關之機密資訊於儲存或傳輸時應進行加密。

2.本機關之加密保護措施應遵守下列規定：

(1)應落實使用者更新加密裝置並備份金鑰。

(2)應避免留存解密資訊。

(3)一旦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.本機關之主機及個人電腦應安裝防毒軟體，並時進行軟、硬體之必要更新或升級。

(1)經任何形式之儲存媒體所取得之檔案，於使用前應先掃描有無惡意軟體。

(2)電子郵件附件及下載檔案於使用前，宜於他處先掃描有無惡意軟體。

(3)確實執行網頁惡意軟體掃描。

2.使用者不得私自安裝點對點檔案分享軟體及未經合法授權軟體。

3.使用者不得私自使用已知或有嫌疑惡意之網站。

4.使用者應定期進行作業系統及軟體更新，以避免惡意軟體利用系統或軟體漏洞進行攻擊。

(二) 遠距工作之安全措施

1.本機關資通業務之操作及維護以現場操作為原則，避免使用遠距工作，如有緊急需求時，應申請並經資訊教育推動小組同意後始可開通。(附件 7)

2.資訊教育推動小組應定期審查已授權之遠距工作需求是否適當。

3.針對遠距工作之連線應採適當之防護措施，並且記錄其登入情形。

(1)提供適當通訊設備，並指定遠端存取之方式。

(2)提供虛擬桌面存取，以防止於私有設備上處理及儲存資訊。

(3)遠距工作終止時之存取權限撤銷，並應返還相關設備。

(三) 電子郵件安全管理

1.使用者使用電子郵件時應提高警覺，並使用純文字模式瀏覽，避免讀取來歷不明之郵件或含有巨集檔案之郵件。

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.使用者應確保電子郵件傳送時之傳遞正確性。

5.本機關應配合上級機關辦理電子郵件社交工程演練，並檢討執行情形。

6.本機關另訂定電子郵件使用規範。

(四) 確保實體與環境安全措施

1.通訊機房之管理

(1)通訊機房應進行實體隔離。

(2)機關人員或來訪人員應申請及授權後方可進入通訊機房。(附件 4)

(3)人員進入管制區應配戴身分識別之標示，並隨時注意身分不明或可疑人員。

(4)僅於必要時，得准許外部支援人員進入通訊機房。

(5)人員及設備進出通訊機房應留存記錄。

2.通訊機房之環境控制

(1)通訊機房之空調、電力得建立備援措施。

(2)通訊機房得安裝之安全偵測及防護措施，包括熱度及煙霧偵測設備、火災警報設備、溫濕度監控設備、漏水偵測設備、入侵者偵測系統，以減少環境不安全引發之危險。

(3)各項安全設備應定期執行檢查、維修。

3.辦公室區域之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)文件及可移除式媒體在不使用或不上班時，應存放在櫃子內。

(3)機密性及敏感性資訊，不使用或下班時應該上鎖。

(4)機密資訊或處理機密資訊之資通業務應避免存放或設置於公眾可接觸之場域。

(5)顯示存放機密資訊或具處理機密資訊之資通業務地點之通訊錄及內部人員電話簿，不宜讓未經授權者輕易取得。

(6)資訊或資通業務相關設備，未經管理人授權，不得被帶離辦公室。

(五) 資料備份

1.重要資料應進行資料備份，其備份之頻率應滿足復原時間點目標之要求，並執行異地存放。

2.本機關應每季確認重要資料備份之有效性。且測試該等資料備份時，宜於專屬之測試系統上執行，而非直接於覆寫回原資通設備。

3.敏感或機密性資訊之備份應加密保護。

(六) 媒體防護措施

1.使用隨身碟或磁碟機等存放資料時，具機密性、敏感性之資料應與一般資料分開儲存，不得混用並妥善保管。

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，並應保留傳送及簽收之記錄。

3.為降低媒體劣化之風險，宜於所儲存資訊因相關原因而無法讀取前，將其傳送至其他媒體。

4.對機密與敏感性資料之儲存媒體實施防護措施，包含機密與敏感之紙本，應保存於上鎖之櫃子，且需由專人管理鑰匙。

(七) 電腦使用之安全管理

1.電腦、業務系統或自然人憑證，若超過十五分鐘不使用時，應立即登出或啟動螢幕保護功能並取出自然人憑證。

2.禁止私自安裝點對點檔案分享軟體及未經合法授權軟體。

3.連網電腦應隨時配合更新作業系統、應用程式漏洞修補程式及防毒病毒碼等。

4.筆記型電腦及實體隔離電腦應定期以人工方式更新作業系統、應用程式漏洞修補程式及防毒病毒碼等。

5.下班時應關閉電腦及螢幕電源。

6.如發現資安問題，應主動循通報程序通報。

7.支援資訊作業的相關設施如影印機、傳真機等，應安置在適當地點，以降低未經授權之人員進入管制區的風險，及減少敏感性資訊遭破解或洩漏之機會。

(八) 行動設備之安全管理

1.機密資料不得由未經許可之行動設備存取、處理或傳送。

2.機敏會議或場所不得攜帶未經許可之行動設備進入

四、資通安全防護設備

本機關應建置防毒軟體、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。

玖、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，本機關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**。

壹拾、資通安全情資之評估及因應

本機關接獲資通安全情資，應評估該情資之內容，並視其對本機關之影響、本機關可接受之風險及本機關之資源，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

本機關接受資通安全情資後，應指定資通安全兼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：

1. 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。

2. 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。

3. 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。

4. 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

本機關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。

1. 資通安全相關之訊息情資

由資訊教育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。

2. 入侵攻擊情資

由資通安全專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、敏感資訊之內容，應採取遮蔽或刪除之方式排除，例如個人資料及業務秘密，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

資訊教育推動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。

壹拾壹、資通系統或服務委外辦理之管理

本機關委外辦理資通系統之建置、維運或資通服務之提供，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。受託者應填具委外廠商執行人員保密切結書、保密同意書及委外廠商保密切結書。(附件 5、6)

壹拾貳、資通安全教育訓練

一、資通安全教育訓練要求

本機關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. 承辦單位應於每學年年初，考量管理、業務及資訊等不同工作類別之需求，擬定資通安全認知宣導及教育訓練計畫(附件 8)，以建立員工資通安全認知，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(附件 9)。
2. 本機關資通安全認知宣導及教育訓練之內容得包含：
   (1) 資通安全法令規定。
   (2) 資通安全作業內容。
3. 員工報到時，應使其充分瞭解本機關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，適用所屬員工。

壹拾參、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

本機關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、臺北市政府及所屬各機關學校公務人員平時獎懲標準表，及臺北市立高級中等學校組織規程準則規定辦理之。

壹拾肆、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，使本機關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，應與本機關之資通安全政策、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(附件 10)。

1.稽核機制之實施

(1) 資訊教育推動小組應定期(至少每年一次)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) 辦理稽核前資訊教育推動小組應擬定資通安全稽核計畫(附件 11)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(附件 13)、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，資訊教育推動小組應於執行稽核前 14 日，通知受稽核單位，並將稽核期程、稽核項目紀錄表(附件 12)及稽核流程等相關資訊提供受稽單位。

(4) 本機關之稽核人員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稽核結果及改善報告(附件 14)中，並提供給受稽單位填寫辦理情形。

(5) 稽核結果應對資訊安全長報告，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、是否定期更改密碼）。

2.改善績效追蹤報告(附件 15)

(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.本機關之資訊教育推動小組應於每年 10 月底前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.持續改善機制之管理審查應做成改善績效追蹤報告，相關紀錄並應予保存，以作為

管理審查執行之證據。

壹拾伍、資通安全維護計畫實施情形之提出

本機關依據資通安全管理法第 12 條之規定，應於**每年 11 月中向臺北市政府教育局資訊教育科**，提出資通安全維護計畫實施情形，使其得瞭解本機關之年度資通安全計畫實施情形。

壹拾陸、相關法規、程序及表單

一、相關法規及參考文件

(一)資通安全管理法

(二)資通安全管理法施行細則

(三)資通安全責任等級分級辦法

(四)資通安全事件通報及應變辦法

(五)資通安全情資分享辦法

(六)公務機關所屬人員資通安全事項獎懲辦法

(七)資訊系統風險評鑑參考指引

(八)政府資訊作業委外安全參考指引

(九)無線網路安全參考指引

(十)網路架構規劃參考指引

(十一)行政裝置資安防護參考指引

(十二)政府行動化安全防護規劃報告

(十三)安全軟體發展流程指引

(十四)安全軟體設計指引

(十五)安全軟體測試指引

(十六)資訊作業委外安全參考指引

(十七)本機關資通安全事件通報及應變程序

二、附件表單

附件 1. 資訊教育推動小組成員及分工表

附件 2. 資通安全保密同意書

附件 3. 資訊及資通資產清冊

附件 4. 管制區域人員進出登記表

附件 5. 委外廠商執行人員保密切結書、保密同意書

附件 6. 委外廠商保密切結書

附件 7. 人員申請遠距工作保密切結書

附件 8. 年度資通安全教育訓練計畫

附件 9. 資通安全認知宣導及教育訓練簽到表

附件 10. 資通安全維護計畫實施情形

附件 11. 資通安全稽核計畫

附件 12. 稽核項目紀錄表
附件 13. 稽核委員聘任同意暨保密切結書
附件 14. 稽核結果及改善報告
附件 15. 改善績效追蹤報告