

新竹市立三民國民中學 108 年度資通安全維護計劃

目錄

壹、依據及目的.....	3
貳、適用範圍.....	3
參、核心業務及重要性.....	3
一、核心業務及重要性：-----	3
二、非核心業務及說明：-----	3
肆、資通安全政策及目標.....	4
一、資通安全政策-----	4
二、資通安全目標-----	4
三、資通安全政策及目標之核定程序-----	4
四、資通安全政策及目標之宣導-----	4
五、資通安全政策及目標定期檢討程序-----	5
伍、資通安全推動組織.....	5
一、資通安全長-----	5
二、資通安全推動小組-----	5
陸、專責人力及經費配置.....	6
一、專責人力及資源之配置-----	6
二、經費之配置-----	6
柒、資訊及資通系統之盤點.....	6
一、資訊及資通系統盤點-----	6
二、本校資通安全責任等級分級-----	7
捌、資通安全風險評估.....	7
一、資通安全風險評估-----	7
玖、資通安全防護及控制措施.....	7
一、資訊及資通系統之管理-----	7
二、存取控制與加密機制管理-----	8
三、作業與通訊安全管理-----	8
七、資通安全防護設備-----	9
壹拾、資通安全事件通報、應變及演練相關機制.....	9
壹拾壹、資通安全情資之評估及因應.....	9
一、資通安全情資之分類評估-----	9
二、資通安全情資之因應措施-----	10
壹拾貳、資通系統或服務委外辦理之管理.....	10
一、選任受託者應注意事項-----	10
二、監督受託者資通安全維護情形應注意事項-----	10
壹拾參、資通安全教育訓練.....	10

一、資通安全教育訓練要求 -----	10
二、資通安全教育訓練辦理方式 -----	11
壹拾肆、本校所屬人員辦理業務涉及資通安全事項之考核機制	11
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.....	11
一、資通安全維護計畫之實施 -----	11
二、資通安全維護計畫實施情形之稽核機制-----	11
三、資通安全維護計畫之持續精進及績效管理-----	12
壹拾陸、資通安全維護計畫實施情形之提出.....	12
壹拾柒、相關法規、程序及表單	12
一、相關法規及參考文件-----	12
二、附件表單-----	13

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新竹市三民國中全機關(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	管理單位
教務業務：課程發展、課程編排、教學實施、學籍管理、成績評量、教學設備、教具圖書資料供應、教學研究及教學評鑑，並與輔導單位配合實施教育輔導等事項	學籍成績系統	為本機關依組織法執掌，足認為重要者	無法更新查詢學生學籍成績資料	24 小時	新竹市網路中心
學生事務：公民教育、道德教育、生活教育、體育衛生保健、學生團體活動及生活管理，並與輔導單位配合實施生活輔導等事項。	學籍成績系統	為本機關依組織法執掌，足認為重要者。	無法更新查詢學生在校表現資料	24 小時	新竹市網路中心
總務業務：學校文書、事務及出納等事項	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。	無	為本機關依組織法執掌，足認為重要者。	無	無	

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	業務失效影響說明	最大可容忍中斷時間	管理單位
公文交換	電子公文無法即時送達本校，影響本校行政效率	48 小時	新竹市政府
人事業務系統	影響人員請假出勤登錄	24 小時	新竹市政府

非核心業務	業務失效影響說明	最大可容忍中斷時間	管理單位
會計資訊系統	影響經費申請核銷	48 小時	行政院主計處
校園資訊網	校園訊息無法對外公告	48 小時	主機位於學校，預計 109 年 向上集中新竹網路中心。
學校健康系統	學生傷病無法登記	48 小時	教育部

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. 應建立資通安全風險管理機制，定期因應內外資通安全情勢變化，檢討資通安全風險管理之有效性。
2. 應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. 應因應資通安全威脅情勢變化，鼓勵同仁積極參與上級所辦理的資通安全教育訓練，以提高本校同仁之資通安全意識。
4. 針對辦理資通安全業務有功人員應進行獎勵。
5. 勿開啟來路不明或無法明確辨識寄件人之電子郵件。
6. 勿開啟無法明辨識網域之網站。
7. 落實資通安全通報機制。

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. 提報教育機構資安通報平台之各級事件發生應為 10 件以下。

(二) 質化型目標：

1. 因應法令與技術之變動，定期調整資通安全維護計劃內容，避免資通系統或資訊遭受未經授權侵害，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、有效偵測與預防外部攻擊。

三、資通安全政策及目標之核定程序

資通安全政策由本校教務處簽陳資通安全長核定。

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透過適當的通知方式，向本校內所有人員進行宣導，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檢討其適切性。

伍、資通安全推動組織

一、資通安全長

依本法第 11 條之規定，本校訂定教務主任為資通安全長，負責督導本校資通安全相關事項，其任務包括：

- 1.資通安全管理政策及目標之核定、核轉及督導。
- 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，由資通安全長召集本校首長及各處室主任成立資通安全推動小組²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資通安全長之指示負責下列事項，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³：

1.策略規劃：

- (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本校年度工作計畫。
- (4)傳達本校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：

- (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。

3.績效管理：

- (1)辦理資通安全內部稽核。
- (2)每年定期確認資通安全事項執行情形。

陸、專責人力及經費配置

一、專責人力及資源之配置

1. 本校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，已設置資通安全人員 1 人，協助處理資通安全相關業務。
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，並提升本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。
4. 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，應配合本校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。
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

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，分別為資訊資產、軟體資產、實體資產、支援服務資產等。
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本校內部之支援服務，如電力、消防等。

3.本校每年度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」。

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、本校資通安全責任等級分級

本校自行辦理資通業務，未維運自行或委外開發之資通系統者，其資通安全責任等級為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.執行風險評估時應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」，並依其中之「詳細風險評鑑方法」進行風險評估之工作。

3.本校應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。

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

(一)資訊及資通系統之保管

資訊及資通系統管理人應確保資訊及資通系統已盤點造冊並適切分級，並持續更新以確保其正確性、重要之資訊及資通系統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取得管理人授權，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。

2. 非本校同仁使用本校之資訊及資通系統，應確實遵守本校之相關資通安全要求，且未經授權不得任意複製資訊。

3. 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

資訊及資通系統之刪除或汰除前應評估本校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。

二、存取控制與加密機制管理

(一)網路安全控管

1. 本校之網路防火牆統一由新竹市教育網路中心管理，區域劃分如下：
 - (1) 外部網路對外網路區域連接外部廣網路(WideAreaNetwork,WAN)。
 - (2) 內部區域網路(LocalAreaNetwork,LAN)：本校內部單位人員及內部伺服器使用之網路區段。
2. 本校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。
3. 使用者應依規定之方式存取網路服務，不得於辦公室內私裝電腦及網路通訊等相關設備。

(二)資通系統權限管理

1. 本校之資通系統應設置密碼，密碼之需滿足：
 - (1) 密碼長度 6 碼以上。
 - (2) 密碼複雜度應包含英文或數字兩種以上。
 - (3) 使用者應定期更換一次密碼。
2. 使用者使用資通系統前應經授權，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. 使用者無繼續使用資通系統時，應立即停用或移除使用者 ID，資通系統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. 資通系統之特權帳號請應經申請授權方能使用，特權帳號授權前應妥善審查其必要性。
5. 資通系統之管理者應定期清查系統特權帳號。

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，並時進行軟、硬體之必要更新或升級。
2. 設備管理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. 本校資通系統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，應申請並經管理員同意後始可開通。
2. 資通安全推動小組應定期審查已授權之遠距工作需求是否適當。

(三)電子郵件安全管理

1. 本校人員到職後應經申請方可使用電子郵件帳號，並應於人員離職後刪除電子郵件帳號之使用。
2. 使用者不得利用本校所提供電子郵件服務從事侵害他人權益或違法之行為。
3. 使用者應確保電子郵件傳送時之傳遞正確性。

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) 機密資訊或處理機密資訊之資通系統應避免存放或設置於公眾可接觸之場域。

(3) 資訊或資通系統相關設備，未經管理人授權，不得被帶離辦公室。

(七)電腦使用之安全管理

1. 禁止安裝點對點檔案分享軟體及未經合法授權軟體。
2. 如發現資安問題，應主動依循本校之通報程序通報。

七、資通安全防護設備

1. 本校應建置防毒軟體，持續使用並適時進行軟、硬體之必要更新或升級。

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，應指定資通安全專責人員進行情資分析，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本校、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本校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

資通安全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本校之運作產生影響，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。

二、監督受託者資通安全維護情形應注意事項

1. 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，應立即通知委託本校及採行之補救措施。
2. 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。
3. 受託者應採取之其他資通安全相關維護措施。
4. 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

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，一般使用者與主管，每人每年接受 3 小時以上之

一般或線上資通安全教育訓練。

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，以建立員工資通安全認知，提升本校資通安全水準，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。
4. 資通安全教育及訓練之政策，除適用所屬員工外，對本校外部的使用者，亦應一體適用。

壹拾肆、本校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，及本校各相關規定辦理之。

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. 資通安全推動小組應定期(每年一次)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本校之管理程序要求，並有效實作及維持管理制度。
2. 辦理稽核前資通安全推動小組應擬定資通安全稽核計畫並安排稽核成員，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. 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。
4. 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.本校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.本校之資通安全推動小組應於每年 12 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.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、上級本校要求、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.內外部稽核結果。
 - 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改善績效追蹤報告²⁴，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

本校依據本法第 11(16,17)條之規定，應於每年 12 月底前向新竹市網路中心，提出資通安全維護計畫實施情形²⁵，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.公務本校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
- 17.本校資通安全事件通報及應變程序

二、附件表單

- 1.資通安全推動小組成員及分工表
- 2.資通安全保密同意書
- 3.資通安全需求申請單
- 4.資訊及資通系統資產清冊
- 5.風險評估表
- 6.風險類型暨風險對策參考表
- 7.管制區域人員進出登記表
- 8.委外廠商執行人員保密切結書、保密同意書
- 9.委外廠商查核項目表
- 10.年度資通安全教育訓練計畫
- 11.資通安全認知宣導及教育訓練簽到表
- 12.資通安全維護計畫實施情形
- 13.資通安全稽核計畫
- 14.稽核項目紀錄表
- 15.稽核結果紀錄表
- 16.稽核委員聘任同意保密切結書
- 17.稽核結果及改善報告
- 18.改善績效追蹤報告