

桃園市立中壢家事商業高級中等學校

資通安全維護計畫

中華民國 112 年 6 月 14 日

目 錄

壹、 依據及目的	4
貳、 適用範圍	4
參、 資通業務及重要性	4
一、 資通業務及重要性：	4
二、 非核心業務及說明：	6
肆、 資通安全政策及目標	7
一、 資通安全政策	7
二、 資通安全目標	7
三、 資通安全政策及目標之核定程序	7
四、 資通安全政策及目標之宣導	8
五、 資通安全政策及目標定期檢討程序	8
伍、 資通安全推動代表	8
一、 資通安全管理代表	8
二、 資通安全推動小組	8
陸、 人力及經費配置	9
一、 人力及資源之配置	9
二、 經費之配置	10
柒、 資訊及資通系統之盤點	10
一、 資訊及資通系統盤點	10
二、 機關資通安全責任等級分級	11
捌、 資通安全風險評估	11
一、 資通安全風險評估	11
二、 資通安全風險之因應	11
玖、 資通安全防護及控制措施	11
一、 資訊及資通系統之管理	12
二、 存取控制與加密機制管理	12
三、 作業與通訊安全管理	13
四、 資通安全防護設備	15
壹拾、 資通安全事件通報、應變及演練	15

壹拾壹、資通安全情資之評估及因應.....	15
一、資通安全情資之分類評估.....	15
二、資通安全情資之因應措施.....	16
壹拾貳、資通系統或服務委外辦理之管理.....	17
一、選任受託者應注意事項.....	17
二、監督受託者資通安全維護情形應注意事項.....	17
壹拾參、資通安全教育訓練.....	17
一、資通安全教育訓練要求.....	17
二、資通安全教育訓練辦理方式.....	17
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	18
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	18
一、資通安全維護計畫之實施.....	18
二、資通安全維護計畫之持續精進及績效管理.....	18
壹拾陸、資通安全維護計畫實施情形之提出.....	19
壹拾柒、相關附件.....	20

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機關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桃園市立中壢家事商業高級中等學校（以下簡稱本機關、本校）。

參、資通業務及重要性

一、資通業務及重要性：

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： 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	欣和排課系統（學校責任） 天方資訊系統（學校責任） 國教署學生學習歷程系統（學校責任+向上集中）	為本機關依組織法執掌，足認為重要者。	可能使本校部分業務中斷	由上級管理單位訂之

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。	天方資訊系統 (學校責任)	為本機關依組織法執掌，足認為重要者。	可能使本校部分業務中斷	由上級管理單位訂之
總務業務： 學校文書、事務及出納等事項	公文系統 (向上集中)	為本機關依組織法執掌，足認為重要者。	可能使本校部分業務中斷	由上級管理單位訂之
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	天方資訊系統 (學校責任)	為本機關依組織法執掌，足認為重要者。	可能使本校部分業務中斷	由上級管理單位訂之

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：該項核心業務所必須使用之資通系統名稱。
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：該項業務使用之系統失效後，機關業務運作有何影響。
5. 最大可容忍中斷時間單位以小時計(對外服務以小時，對內服務以工作小時計)。

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
學校首頁	資訊無法即時公告，影響行政效率	72 小時
調代課系統	影響調代課作業，但仍可改手動處理	72 小時
學校讀卡管理系統	影響學生到離校紀錄及家長簡訊發送， 但仍有書面記錄	72 小時
校園英聽廣播系統	影響學校影音廣播	96 小時
圖書館管理系統	影響學生借還書作業，但仍可改手動處理	96 小時
電子刊物平台	影響學生線上閱讀電子刊物，但仍可改 電子檔下載閱讀	96 小時

各欄位定義

1. 非核心業務系統：公務機關非核心業務相關之資通系統，如差勤服務、郵件服務、用戶端服務等。
2. 業務失效影響說明：該項業務使用之系統失效後，機關業務運作有何影響。
3. 最大可容忍中斷時間單位以小時計(對外服務以小時，對內服務以工作小時計)。

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. 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。
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. 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郵件開啟率及附件點閱率分別低於 5% 及 2%。
3. 資通安全教育訓練人員受訓且通過評量合格率達 90%。（含線上學習之人員）

（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

資通安全政策由本校簽陳資通安全管理代表核定。

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每年透過教育訓練、內部會議、張貼公告等方式，向所有人員進行宣導，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、資通安全推動代表

一、資通安全管理代表

依本法第 11 條之規定，本校訂定圖書館馬主任肇亨為資通安全管理代表，負責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，由資通安全管理代表召集各業務部門主管/副主管以上之人員代表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，並依資通安全管理代表指示負責下列事項，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. 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，最低應設置資通安全人員 1 人，其分工如下，本校現有資通安全人員名單及職掌應列冊，並適時更新。
 - (1) 資通安全認知與訓練業務，負責推動資通安全教育訓練等業務之推動。
 - (2) 資通安全防護業務，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。

(3) 資通安全管理法法遵事項業務時，負責本機關對所屬公務機關或所管特定非公務機關之法遵義務執行事宜。

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，並提升機關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. 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，並經資通安全管理代表核定後，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，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：相關基礎設施級其他機關內部之支援服務，如電力、消防等。
 - (5) 人員資產：內部設備維運管理人員、主管、使用人員，以及委外廠商駐點人員等。
 - (6) 資料資產：以紙本形式儲存之資訊，如程序、清單、計畫、報告、指引手冊、政策、公文、作業紀錄、作業規範、各種應用系統文件及管理手冊，契約、法律文件、軟體使用授權等等。
- 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」，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

本校配合桃園市高中資訊資源向上集中，核列資通安全等級分類為 D 級。

捌、資通安全風險評估

一、資通安全風險評估

本校應每年針對資訊及資通系統資產進行風險評估。

二、資通安全風險之因應

選擇防護及控制措施時，亦應考量採行該項措施可能對資通安全風險之影響。

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. 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。
2. 資訊及資通系統管理人應確保資訊及資通系統被妥善的保存或備份。
3. 資訊及資通系統管理人應確保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

依教育局規定辦理。

(二) 資通系統權限管理

1. 資通系統應設置通行碼管理，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. 資通系統之特權帳號不得共用。
3. 資通系統之管理者每季應清查系統特權帳號。

(四) 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) 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. 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. 使用者未經同意不得私自安裝應用軟體，管理者並應每半年定期針對管理之設備進行軟體清查。
3. 使用者不得私自使用已知或有嫌疑惡意之網站。

(二) 遠距工作之安全措施

- (1) 提供虛擬桌面存取，以防止於私有設備上處理及儲存資訊。
- (2) 遠距工作終止時之存取權限撤銷，並應返還相關設備。

(三) 確保實體與環境安全措施

1. 電腦機房之門禁管理

- (1) 電腦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電腦機房，管理者並應定期檢視授權人員之名單。
- (3) 人員及設備進出應留存記錄。

2. 電腦機房之環境控制

- (1) 電腦機房之空調、電力應建立備援措施。
- (2) 電腦機房應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，以減少環境不安全之危險。

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) 機密性及敏感性資訊，不使用或下班時應該上鎖。

(四) 資料備份

1. 重要資料及資通系統應進行資料備份，其備份之頻率應滿足復原時間點目標之要求。
2. 敏感或機密性資訊之備份應加密保護。

(五) 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、敏感性之資料應與一般資料分開儲存，不得混用並妥善保管。
2. 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或備份磁帶，應保存於上鎖之櫃子，且需由專人管理鑰匙。

(六) 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. 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。

3. 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。
4. 下班時應關閉電腦及螢幕電源。
5. 如發現資安問題，應主動循機關之通報程序通報。

(七) 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

(八) 即時通訊軟體之安全管理

使用即時通訊軟體傳遞機關內部公務訊息，其內容不得涉及機密資料。但有業務需求者，應使用經專責機關鑑定相符機密等級保密機制或指定之軟、硬體，並依相關規定辦理。

四、資通安全防護設備

1. 應建置防毒軟體、網路防火牆，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

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，依本校資通安全事件通報應變程序辦理。

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、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。
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. 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。

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，以建立人員資通安全認知，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. 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審酌辦理。

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、資通安全維護計畫之持續精進及績效管理

1. 本校之資通安全推動小組應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。
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. 資通安全防护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) 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 之規定，應依桃園市政府來文要求於規定時間內向上級或監督機關，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、相關附件

附件表單。

桃園市立中壢家事商業高級中等學校
資通安全推動小組成員及分工表

單位職級	姓名	業務分工	分機	備註
秘書	馬肇亨	資通安全政策及目標之研議 協助跨部門權責分工之協調	102	
教務主任	鍾瓊瑤	資通安全政策及目標之研議 督導所屬資通系統工作事項	201	
圖書館主任	呂美娥	資通安全政策及目標之研議 督導所屬資通系統工作事項	811	
學務主任	洪宏財	資通安全政策及目標之研議 督導所屬資通系統工作事項	301	
總務主任	曾盛甲	資通安全政策及目標之研議 督導所屬資通系統工作事項	501	
實習主任	林志信	資通安全政策及目標之研議 督導所屬資通系統工作事項	609	
進修部主任	周如芬	資通安全政策及目標之研議 督導所屬資通系統工作事項	701	
輔導室主任	翁崇修	資通安全政策及目標之研議 督導所屬資通系統工作事項	801	
人事室主任	吳瑞芬	資通安全政策及目標之研議 督導所屬資通系統工作事項	901	
會計室主任	邱遠輝	資通安全政策及目標之研議 督導所屬資通系統工作事項	911	
實習處資處科主任	高毓鎂	協助資通安全事項辦理與推動 資通安全技術之研究	606	
教務處設備組長	葉淑櫻	協助資通安全事項辦理與推動 資通安全技術之研究	206	
教務處資訊組長	鄭筱芸	統籌資通安全事項之辦理與推動 協助資通安全事件通報與處置	210	
教務處資訊技士	許靜芳	資通安全事項之辦理與推動 資通安全事件通報與處置	637	

桃園市中壢家事商業高級中等學校

資訊及資通系統資產清冊

製表日期： 112 年 8 月 1 日

項次	資產名稱	類別	擁有者/ 職稱	管理者 (部門)	使用者 (部門)	存放 位置	數量	說明	防護 需求 等級	核心 系統	備註
1	天方資訊系統	軟體	徐惠珊/ 組長	教務處	各處室	機房	1	校務系統	高	☒ 是 ☐ 否	
2	欣和排課系統	軟體	倪身怡/ 組長	教務處	教務處	機房	1	校務系統	高	☒ 是 ☐ 否	
3	學生學習歷程系統	軟體	徐惠珊/ 組長	教務處	教務處	國教署	1	已向上集中	普	☒ 是 ☐ 否	
4	學校官網	軟體	許靜芳/ 技士	教務處	各處室	桃園市政府	1	已向上集中	普	☐ 是 ☒ 否	
5	調代課系統	軟體	倪身怡/ 組長	教務處	教務處	機房	1	校務系統	中	☐ 是 ☒ 否	
6	學生讀卡管理系統	軟體	林雅月/ 教官	學務處	學務處	機房	1	學務系統	中	☐ 是 ☒ 否	
7	校園英聽廣播系統	軟體	葉淑櫻/ 組長	教務處	教務處	教務處 設備組	1	校務系統	普	☐ 是 ☒ 否	
8	圖書館管理系統	軟體	呂美娥/ 主任	圖書館	圖書館	機房	1	圖書系統	普	☐ 是 ☒ 否	
9	電子刊物平台	軟體	呂美娥/ 主任	圖書館	圖書館	桃園市政府	1	圖書系統	普	☐ 是 ☒ 否	

承辦人：

單位主管：

機關首長：

桃園市中壢家事商業高級中等學校

風險評估表

製表日期：112 年 8 月 1 日

項次	資產名稱	類別	擁有者/ 職稱	機密性 (C)	完整性 (I)	可用性 (A)	資訊資產 價值 (C, I, A 取最大 值)	發生可能 性/威脅 等級(T)	脆弱等級 (V)	風險值 資訊資產價 值*(T*V)
1	天方資訊系統	軟體	徐惠珊/ 組長	4	4	3	4	2	2	16
2	欣和排課系統	軟體	倪身怡/ 組長	2	3	2	3	2	2	12
3	學生學習歷程系統	軟體	徐惠珊/ 組長	3	3	3	4	1	1	4
4	學校官網	軟體	許靜芳/ 技士	2	3	3	3	1	1	3
5	調代課系統	軟體	倪身怡/ 組長	1	2	2	2	1	2	4
6	學生讀卡管理系統	軟體	林雅月/ 教官	2	2	1	3	1	2	6
7	校園英聽廣播系統	軟體	葉淑櫻/ 組長	1	1	1	1	1	1	1
8	圖書館管理系統	軟體	呂美娥/ 主任	1	2	2	2	1	1	2
9	電子刊物平台	軟體	呂美娥/ 主任	1	1	1	1	1	1	1

承辦人員：

單位主管：

機關首長：

桃園市中壢家事商業高級中等學校

資通安全保密同意書

立同意書人_____於民國____年____月____日起於_____任職，
因業務涉及單位重要之資訊及資通系統，故同意下列保密事項：

- 一、於業務上所知悉之機敏資料及運用之資通系統等，應善盡保管及保密之責。
- 二、相關業務之資訊、文件，不得私自洩漏與業務無關之人員。
- 三、遵守其他本單位資通安全相關之法令及規定。
- 四、如有危害本單位資通安全之行為，願負相關之責任。

立同意書人：_____（簽章）

身份證字號：_____

服務機關：_____

機關首長：_____

中 華 民 國 年 月 日

中壢家商委外廠商執行人員保密切結書

立切結書人_____（簽署人姓名）等，受_____（廠商名稱）委派至中壢家商（機關名稱，以下稱機關）處理業務，謹聲明恪遵機關下列工作規定，對工作中所持有、知悉之資訊系統作業機密或敏感性業務檔案資料，均保證善盡保密義務與責任，非經機關權責人員之書面核准，不得擷取、持有、傳遞或以任何方式提供給無業務關係之第三人，如有違反願賠償一切因此所生之損害，並擔負相關民、刑事責任，絕無異議。

- 一、未經申請核准，不得私自將機關之資訊設備、媒體檔案及公務文書攜出。
- 二、未經機關業務相關人員之確認並代為申請核准，不得任意將攜入之資訊設備連接機關網路。若經申請獲准連接機關網路，嚴禁使用數據機或無線傳輸等網路設備連接外部網路。
- 三、經核准攜入之資訊設備欲連接機關網路或其他資訊設備時，須經電腦主機房掃毒專責人員進行病毒、漏洞或後門程式檢測，通過後發給合格標籤，並將其粘貼在設備外觀醒目處以備稽查。
- 四、廠商駐點服務及專責維護人員原則應使用機關配發之個人電腦與週邊設備，並僅開放使用機關內部網路。若因業務需要使用機關電子郵件、目錄服務，應經機關業務相關人員之確認並代為申請核准，另欲連接網際網路亦應經機關業務相關人員之確認並代為申請核准。
- 五、機關得定期或不定期派員檢查或稽核立切結書人是否符合上列工作規定。
- 六、本保密切結書不因立切結書人離職而失效。
- 七、立切結書人因違反本保密切結書應盡之保密義務與責任致生之一切損害，立切結書人所屬公司或廠商應負連帶賠償責任。

立切結書人：

姓名及簽章 身分證字號 聯絡電話及戶籍地址

立切結書人所屬廠商：

廠商名稱及蓋章 廠商負責人姓名及簽章 廠商聯絡電話及地址

填表說明：

- 一、廠商駐點服務人員、專責維護人員，或逗留時間超過三天以上之突發性維護增援、臨時性系統測試或教育訓練人員（以授課時需連結機關網路者

為限)及經常到機關洽公之業務人員皆須簽署本切結書。

二、 廠商駐點服務人員、專責維護人員及經常到機關洽公之業務人員每年簽署本切結書乙次。

中 華 民 國 年 月 日

中壢家商委外廠商執行人員保密同意書

茲緣於簽署人_____（簽署人姓名，以下稱簽署人）參與_____（廠商名稱，以下稱廠商）得標 中壢家商（以下稱機關）資通業務委外案_____（案名）（以下稱「本案」），於本案執行期間有知悉或可得知悉或持有政府公務秘密及業務秘密，為保持其秘密性，簽署人同意恪遵本同意書下列各項規定：

第一條 簽署人承諾於本契約有效期間內及本契約期滿或終止後，對於所得知或持有一切機關未標示得對外公開之公務秘密，以及機關依契約或法令對第三人負有保密義務之業務秘密，均應以善良管理人之注意妥為保管及確保其秘密性，並限於本契約目的範圍內，於機關指定之處所內使用之。非經機關事前書面同意，不得為本人或任何第三人之需要而複製、保有、利用該等秘密或將之洩漏、告知、交付第三人或以其他任何方式使第三人知悉或利用該等秘密，或對外發表或出版，亦不得攜至機關或機關所指定處所以外之處所。

第二條 簽署人知悉或取得機關公務秘密與業務秘密應限於其執行本契約所必需且僅限於本契約有效期間內。簽署人同意公務秘密與業務秘密，應僅提供、告知有需要知悉該秘密之履約廠商團隊成員人員。

第三條 簽署人在下述情況下解除其所應負之保密義務：

原負保密義務之資訊，由機關提供以前，已合法持有或已知且無保密必要者。

原負保密義務之資訊，依法令業已解密、依契約機關業已不負保密責任、或已為公眾所知之資訊。

原負保密義務之資訊，係自第三人處得知或取得，該第三人就該等資訊並無保密義務。

第四條 簽署人若違反本同意書之規定，機關得請求簽署人及其任職之廠商賠償機關因此所受之損害及追究簽署人洩密之刑責，如因而致第三人受有損害者，簽署人及其任職之廠商亦應負賠償責任。

第五條 簽署人因本同意書所負之保密義務，不因離職或其他原因不參與本案而失其效力。

第六條 本同意書一式叁份，機關、簽署人及_____（廠商）各執存一份。

簽署人姓名及簽章：

身分證字號：

聯絡電話：

戶籍地址：

所屬廠商名稱及蓋章：

所屬廠商負責人姓名及簽章：

所屬廠商地址：

中 華 民 國 年 月 日

桃園市中壢家事商業高級中等學校

審查結果及改善報告

範圍	全機關			
日期	_____年_____月_____日			
審查日期	_____年_____月_____日			
項 目				
編號	建議或待改善項目	改善措施	改善期程規劃	相關佐證資料
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				
11				

桃園市中壢家事商業高級中等學校

改善績效追蹤報告

製表日期： 年 月 日

審查發現			
審查日期	____年____月____日____時		受審查單位
審查區域			
建議或待改善項目與內容	待改善項目： 建議項目：		
影響範圍評估			
發生原因分析			
改善措施成效追蹤			
改善措施		預計成效	執行情況
管理面			
技術面			
人力面			
資源面			
作業程序			
其他			

績效管考			
改善措施確認	☐ 合格／完成 ☐ 待追蹤(追蹤期限：_____年_____月_____日) ☐ 不合格(說明：_____)		
經費需求或編列執行金額	萬元。	經費執行情形	
預定完成日期		實際完成日期	
完成進度或情形說明	。		
改善成效考核			
後續成效追蹤			
資通安全推動小組承辦人員		機關首長(或資通安全管理代表)	