國立高雄餐旅大學

NATIONAL KAOHSIUNG UNIVERSITY
OF HOSPITALITY AND TOURISM

資通安全維護計畫

版本編號：4.0

發行日期： 112 年 09 月21 日

目　　錄

壹、依據及目的

資通安全維護計畫(以下簡稱本計畫)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

一、本計畫適用範圍涵蓋國立高雄餐旅大學(以下簡稱本校)全機關。

二、ISMS 適用範圍包含全校範圍內之核心資通系統、保有個資或防護需求中等級以上之資通系統及相關網路與資訊機房活動。

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
校務行政	校務資訊管理系統(包含在校生及教職員資訊系統)	為本校依組織法執掌，足認為重要者。	重大影響校內行政、學務日常運作	8 小時
校務行政	校園入口網暨單一簽入系統	為本校依組織法執掌，足認為重要者。	重大影響校內行政日常運作	10 小時
校務行政	公文線上簽核系統	為本校依組織法執掌，足認為重要者。	重大影響校內行政日常運作	8 小時
校務行政	教務資訊系統	為本校依組織法執掌，足認為重要者。	重大影響校內行政日常運作	8 小時
校務行政	行政電子郵件系統	為本校依組織法執掌，足認為重要者。	重大影響校內行政日常運作	8 小時

二、 非核心業務及說明：

本校之非核心業務及說明如下表：

非核心資通系統	業務失效影響說明	最大可容忍中斷時間
響應式全球資訊網	影響校內行政日常運作	24 小時
財產管理系統	影響校內行政日常運作	24 小時
主計系統	影響校內行政日常運作	24 小時
教師評鑑暨提聘系統	影響校內行政日常運作	24 小時
人事差勤登錄管理系統	影響校內行政日常運作	24 小時

肆、資通安全政策及目標

一、 資通安全政策

為強化資訊安全管理，確保所屬之資訊資產的機密性、完整性及可用性，以提供本校之資訊業務持續運作之資訊環境，並符合相關法規之要求，使其免於遭受內、外部的蓄意或意外之威脅，特定此政策規範。資訊安全政策願景如下：強化人員認知、避免資料外洩；落實日常維運、確保服務可用。

二、 資通安全目標

(一)辦理資訊安全教育訓練，推廣員工資訊安全之意識與強化其對相關責任之認知。

(二)保護本校業務活動資訊，避免未經授權的存取、修改，確保其正確

完整。

(三)定期進行內部與外部稽核，確保相關作業皆能確實落實。

(四)確保本校關鍵核心系統維持一定水準的系統可用性。

三、 資通安全政策及目標之核定程序

資通安全政策由本校圖書資訊處簽陳資安長核定。

四、 資通安全政策及目標之宣導

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。

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。

六、 資通安全政策及目標之制、修訂、核定與宣導方式，應遵循本校ISMS 文件「IS-01-001 資訊安全政策」。

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，本校訂定副校長為資通安全長，負責督導機關資通安全相關事項，其任務包括：

(一)資通安全管理政策及目標之核定、核轉及督導。

(二)資通安全責任之分配及協調。

(三)資通安全資源分配。

(四)資通安全防護措施之監督。

(五)資通安全事件之檢討及監督。

(六)資通安全相關規章與程序、制度文件核定。

(七)資通安全管理年度工作計畫之核定

(八)資通安全相關工作事項督導及績效管理。

(九)其他資通安全事項之核定。

二、 資通安全暨個人資料保護推動委員會

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，本會以副校長擔任召集人，各行政單位一級主管及各學院院長及共同教育委員會主任委員為當然委員，每年至少召開會議一次。本會任務包括：

(一) 資通安全及個人資料保護政策之擬議。

(二) 資通安全及個人資料管理制度之審議及推展。

(三) 資通系統及個人資料盤點與風險評鑑管理作業督導。

(四) 資通安全及個人資料保護教育訓練督導。

(五) 資安事件之處置及審議。

(六) 其他資通安全及個資保護管理之規劃及執行事項。

三、資通安全工作小組

本校之資通安全工作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，本校資通安全工作小組分組人員名單及職掌應列冊，並適時更新之：

(一)資訊安全管理代表：由圖書資訊處處長擔任。

1. 協調資訊安全執行小組與緊急處理小組執行資訊安全相關作業。
2. 負責對資訊安全狀況進行預警、監控，並對資訊安全狀況與事件進行處置。
3. 對於資訊安全管理之改善提出建議，以及協助執行資訊安全之自我檢核。
4. 對於存取控制管理定期進行事件紀錄檢核，以及管理程序檢核。

(二)資訊安全執行小組：依本校「IS-04-001 資訊安全組織成員表」人員組成，負責規劃及執行各項資訊安全作業。

1. 制定資訊安全管理相關規範。
2. 推動資訊安全相關活動。
3. 辦理資訊安全相關教育訓練。
4. 建立風險管理制度，執行風險管理。
5. 建立安全事件緊急應變暨復原措施。
6. 執行稽核改善建議事項。
7. 執行預防措施之改善。

8. 研討新資訊安全產品或技術。

9. 執行資訊安全委員會決議事項。

10. 鑑別資訊安全相關之法規。

11. 資訊安全執行小組應每年於召開管理審查會議前，針對本校提供之資訊服務來識別資訊安全的相關法令、法規與契約之要求，並明確定義至「外來文件一覽表」中，且定期更新該列表。

(三)資訊安全稽核小組：依本校「IS-04-001 資訊安全組織成員表」人員組成，負責評估資訊安全管理制度之執行情形。

1. 擬定資訊安全內部稽核計畫。

2. 執行資訊安全內部稽核。

3. 撰寫資訊安全內部稽核報告。

4. 追蹤不符合事項之改善執行情形。

陸、專職(責)人力及經費配置

一、 專職(責)人力及資源之配置

(一)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 C 級，最低應設置資通安全專職(責)人員 1 人，本校現有資通安全專責人員名單及職掌應列冊，並適時更新。

(二)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，並提升本校資通安全專業人員之資通安全管理能力。

(三)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。

(四)資安專職(責)人員專業職能之培養(如證書、證照、培訓紀錄等)，應依據資通安全責任等級分級辦法之規定。

1. 資安專職(責)人員總計應持有 1 張以上資通安全專業證照。

2. 資安專職(責)人員總計應持有 1 張以上資通安全職能評量證書。

(五)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。

(六)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。

(七)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

(一)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。

(二)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。

(三)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。

(二)資通系統清冊包含或於本校 IP 網段內、或使用本校網域名稱之資通系統。

(三)物聯網設備管理清冊包含學校採購及公務使用之物聯網設備。

(四)資訊資產分類

資訊資產依其性質不同，分為 7 類：人員、文件、軟體、通訊、硬體、資料、環境。

1. 人員（People/PE）：包含全體同仁及委外廠商。
2. 文件（Document/DC）：以紙本形式存在之文書資料、報表等相關資訊，包含公文、列印之報表、表單、計畫等紙本文件。
3. 軟體（Software/SW）：作業系統、應用系統程式、套裝軟體等，包含原始程式碼、應用程式執行碼、資料庫等。
4. 通訊（Communication/CM）：提供資訊傳輸、交換之線路或服務。
5. 硬體（Hardware/HW）：網路設備、主機設備等相關硬體設施。
6. 資料（Data/DA）：儲存於硬碟、磁帶、光碟等儲存媒介之數位

資訊。

7. 環境（Environment/EV）：相關基礎設施及服務，包含辦公室實體、實體機房、電力、消防設施等。

(五)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。核心資通系統及相關資產，並應加註標示。

(六)本校每年辦理資訊及資通系統資產盤點，相關作業規範應遵循本校 ISMS 文件「IS-02-003 資訊資產管理程序書」。

二、 機關資通安全責任等級分級

依據資通安全責任等級分級辦法第 6 條辦理，本校為資通安全等級分類 C 級機關。

捌、資通安全風險評估

一、 本校應每年針對資訊及資通系統資產進行風險評估。

二、 本校風險評鑑流程分為高階風險評鑑及詳細風險評鑑兩個階段。

(一)高階風險評鑑

依據「資通安全責任等級分級辦法」附表九，識別本校所有資通訊系統，並進行防護需求等級評估，並由資訊安全執行小組彙整「資訊系統清冊」，以鑑別資訊系統安全等級。

(二)詳細風險評鑑

1. 符合下列規範之資訊系統、服務及流程，應進行威脅弱點評

估：

(1) 資訊系統防護需求等級評估為中或高。

(2) 本校關鍵業務流程之資通系統。

(3) 屬於本校 ISMS 施作範圍內之網路機房重要基礎設施、服務。

2. 依各資訊資產之分類，進行選擇所需評估的事件(威脅-弱點)類別。

3. 依可能性評估級距及衝擊性評估級距之標準評估各事件發生的可能性及衝擊性，並將各資產面臨之主要事件登載於「威脅弱點評估表」。

4. 資訊資產價值之數值若為 7（含 7）以上，必須進行威脅弱點評估。

5. 資訊資產之機密性、可用性及完整性之數值，若其中一項數值為 4 者，必須進行威脅弱點評估。

6. 風險值的計算

資訊資產風險值=資訊資產價值 x 可能性(等級)X 衝擊性(等級)。

三、 本校應每年針對資訊及資通系統資產進行風險評估。相關作業規範應遵循本校 ISMS 文件「IS-02-004 風險評鑑與管理程序書」。

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

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. 本校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。
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. 本校之網路區域劃分如下：

(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. 應定期檢視防火牆政策是否適當，並適時進行防火牆軟、硬體

之必要更新或升級。

4. 對於通過防火牆之來源端主機 IP 位址、目的端主機 IP 位址、來源通訊埠編號、目的地通訊埠編號、通訊協定、登入登出時間、存取時間以及採取的行動，均應予確實記錄。

5. 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。

6. 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。

7. 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。

8. 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。

(二)資通系統權限管理

1. 本校之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) 通行碼需要混合英文、數字以增強密碼複雜度。

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. 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. 資通系統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. 資通系統之管理者每年應清查系統特權帳號。

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) 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。

(3) 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。

(4) 確實執行網頁惡意軟體掃描。

(5) 使用者不得私自使用已知或有嫌疑惡意之網站。

(6) 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使用 IT 維運管理平台為原則，避免使用遠距工作。

2. 每年進行帳號清除作業並由需求單位重新提出申請。

3. 針對遠距工作之連線應採適當之防護措施(並包含伺服器端之集中過濾機制檢查使用者之授權)，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) 進行遠距工作時之安全監視。

(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. 本校人員到職後應經申請方可使用電子郵件帳號。

2. 電子郵件伺服器應設置防毒及過濾機制，並適時進行軟硬體之必要更新。

3. 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。

4. 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。

5. 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。

6. 使用者應確保電子郵件傳送時之傳遞正確性。

7. 本校應定期舉辦(或配合上級機關舉辦)電子郵件社交工程演練，並檢討執行情形。

(四)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) 若外部人員或本校未具機房進出權限人員，因執行業務需求進入機房時，必須由資訊單位或保管單位指派人員監控或隨行並填寫「人員進出機房登記表」後方可進出機房，並遵守相關設備管理之規定。

(3) 僅於必要時，得准許外部支援人員進入電腦機房。

(4) 人員及設備進出電腦機房應留存記錄並定期審閱。

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) 電腦機房之溫濕度管控範圍為：機房溫度應維持在 15℃至

35℃，相對溼度維持在 30%RH 至 70%RH。

(3) 電腦機房應安裝之安全偵測及防護措施，包括極早期偵煙設備、火災警報設備、溫濕度監控設備、漏水偵測設備，以減少環境不安全引發之危險。

(4) 各項安全設備應定期執行檢查、維修，並應定時針對設備之管理者進行適當之安全設備使用訓練。

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系統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系統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) 資訊或資通系統相關設備，未經管理人授權，不得被帶離辦公室。

(五)資料備份

1. 重要資料及核心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. 本校應每年確認核心資通系統資料備份之有效性。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系統。
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. 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。

(七)電腦使用之安全管理

1. 電腦設備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，應主動循機關之通報程序通報。

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)通訊軟體之安全管理

1. 為避免公務機敏資料被不當竊取，個人電腦應避免非公務用通訊軟體。

2. 如因業務需要使用通訊軟體時，應遵循以下注意事項：

(1)不得使用通訊軟體傳輸公務機密、涉及資訊安全及個人隱私之事項，或其他非機密，但若不當公開或外洩，可能造成決策困擾、個人或機關信譽非必要損害等負面效應之事項。

(2)未確認傳遞者身分及訊息內容真實性前，不隨意點選訊息內超連結，以免落入釣魚、惡意或高風險網站陷阱。

(九)個人行動裝置之安全管理

1. 個人行動裝置非經允許，不得存取公務機敏資料。

2. 個人行動裝置應避免作為公務用途，例如將個人手機、平板電腦等連接公務電腦做為外接儲存裝置。

四、 系統獲取、開發及維護

(一)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. 於資通系統開發期間，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。

2. 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。

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業務持續運作演練。

六、 執行弱點掃描與滲透測試

(一)本校每兩年應針對全部核心資通系統，辦理弱點掃描與滲透測試檢測，針對高風險漏洞進行修補作業。

(二)完成高風險漏洞修補作業後，應進行復測，以確保應修補之高風險漏洞皆已完成修補。

七、 執行資通安全健診

(一)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。

(二)針對執行健診所發現之漏洞應進行修補作業。

八、 資通安全防護設備

(一)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。

(二)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。

九、確保資通系統管理量能

1.資通系統集中化管理：引進虛擬化作業系統以集中管理資通系統，後續將持續推廣宣導虛擬化作業系統，整併外單位資通系統以提升資通系統管理量能。

2.適度降低資通系統數量：盤點校園資訊資產，若有實用性不高及未能滿足資安需求的資通系統，將適時檢討汰除以降低資通系統數量及強化校園資安環境。

十、落實管理危害國家資通資通安全產品

1.依行政院政策要求，公務用之資通訊產品(含軟體、硬體及服務)不得

使用大陸廠牌。

2.依行政院政策要求，針對學校出租場域，於學校委外契約或場地租借使用規定，明定不得使用危害國家資安之產品(如大陸廠排軟體、硬體及服務)

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「IS-02-011 安全事件管理程序書」。

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

由資訊安全執行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：受委託者應配置充足且經適當之資安資格訓練人員。

二、 監督受託者資通安全維護情形應注意事項

(一)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。

(二)委託關係終止或解除時，應確認受託者刪除或銷毀履行委託契約而持有之資料。

(三)受託者應採取之其他資通安全相關維護措施 。

(四)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

(一)本校依資通安全責任等級分級屬 C 級，資安人員每年至少 1 名人員接受 12 小時以上之資安專業課程訓練或資安職能訓練。

(二)本校資訊人員每兩年應接受 3 小時以上之資安專業課程訓練。

(三)本校之資訊人員、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

(一)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。

(二)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。

(三)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。

三、 資通安全教育及訓練之政策，除適用所屬員工外，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「職工助理獎懲案件處理原則」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. 辦理稽核前資訊安全稽核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目的、期間、稽核小組成員、稽核項目及稽核程序，並應將前次稽核之結果納入稽核範圍。
3. 依本校 ISMS 範圍及 ISMS 範圍以外之單位(行政、教學單位)分別規劃辦理資通安全內部稽核作業，並依每年規劃分別擬定資通安全內稽計畫。
4. 辦理稽核時，資安稽核組應於執行稽核前一周，通知受稽核單位，並將稽核期程、稽核項目紀錄表及稽核流程等相關資訊提供受稽單位。

5. 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，亦可委託外部專家或顧問協助執行，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中，並提供給受稽單位填寫辦理情形。
6. 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。
7. 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

(一)本校之資通安全委員會應(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。

(二)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：

(1)資通安全政策及目標之實施情形。

(2)資通安全人力及資源之配置之實施情形。

(3)資通安全防護及控制措施之實施情形。

(4)內外部稽核結果。

(5)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。

(三)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 條規定，應向教育部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

(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)資訊作業委外安全參考指引

(八)本校 ISMS 一至三階管理文件

二、附件表單

1. 本校ISMS四階表單
2. 資通安全維護計畫實施情形