教育部110年12月30日臺教資（四）字第1100179797號函，訂定「國立大專校院資通安全維護作業指引」，推動全校落實資通安全管理法相關規定。 教育部111年9月5日臺教資（四）字第1112703805號函，函送「111年全國大專校院資安長會議」紀錄，明示私立大專校院得參照「國立大專校院資通安全維護作業指引」辦理資安事件應變機制及相關防護措施。教育機構資安驗證中心依據作業指引，研擬全機關範圍導入ISMS建議優先落實之執行策略，提供各校參考。

教育機構資安驗證中心協助教育部執行109至112年度資通安全實地稽核計畫，對於教育部部屬機關構及國立大專校院進行稽核，確認在資安法相關要求的法遵符合情形，以及資通安全維護計畫實施情形。實地稽核工作以「資通安全實地稽核項目檢核表」及「資通系統防護基準實施情形調查」為查檢項目，與行政院資通安全稽核所使用的版本相同，檢核表涵蓋了策略面、管理面及技術面，共9大構面115項檢核項目，防護基準包含78項控制措施。實地稽核工作以這些項目與控制措施作為查檢架構，受稽機關同樣也可依據這些項目，檢視機關內的資安管理作為是否已符合要求。

實地稽核中常見的稽核發現包括，資安推動組織未涵蓋所有單位、組織成員非一級主管、組織架構未完善；核心系統盤點與分級之適切性，以及是否納入ISMS範圍；備份、備援與回復機制的完善、合理性；營運衝擊分析與業務持續運作計畫適切性；資訊或資安經費占比偏低、在專職人力配置、相關證照與教育訓練不足；委外合約中未將防護需求等級、安全系統發展生命週期、對委外廠商之資安要求、監督等項目納入規範；系統身分驗證資訊未遮蔽、使用者帳號清查與權限控管、未限制登入嘗試等。這些稽核發現，也與「國立大專校院資通安全維護作業指引」關注的面向有不少重疊。

因此，教育機構資安驗證中心以國立大專校院資通安全維護作業指引為框架，並參考檢核表項目、防護基準控制措施內容及實地稽核發現之經驗，依人員的職務與責任整理應辦事項，提供各校落實全機關範圍導入ISMS執行策略之建議。

(一) 資通安全長之配置

依據作業指引設置資通安全長之後，更重要的是必須讓資通安全長完全掌握「資通安全實地稽核項目檢核表」策略面的三大構面共26項目的實施情形，從全校整體考量進行資安工作的推動及監督。第一構面核心業務及其重要性，包括核心系統的分級與是否納入ISMS、核心系統的盤點、營運衝擊分析與業務持續運作計畫、系統備援與備份等重點項目。第二構面資通安全政策及推動組織應注意機關的資安政策、目標與評估方式，以

及資安組織、人員考核等內容。第三構面資安專責人力及經費則須留意組織的資安經費占比、人員配置與認知、人員訓練與證照有效性等。

教育部實地稽核時，將會安排與資通安全長的訪談，稽核委員從訪談過程了解資通安全長是否充分掌握核心業務及其重要性、資通安全政策及推動組織、資安專責人力及經費。這個訪談過程，建議校方應備妥簡報及佐證資料，讓資通安全長說明策略面的推動情況。教育機構資安驗證中心針對【資通安全長應掌握事項】策略面的三大構面共26項目設計簡報範本(https://tinyurl.com/y9s6283h)，歡迎各校下載再調整成自己的內容。

(二) 資通安全推動組織

各依據作業指引將各單位主管納入資通安全推動組織之後，依據「資通安全實地稽核項目」的「2.4成立資通安全推動組織，負責推動、協調監督及審查資通安全管理事項？推動組織層級之適切性，且業務單位是否積極參與？」，各單位主管不只應參與資通安全推動相關會議，更重要的是主管在單位內必須有積極的資安推動作為，督導單位人員落實資安文件、落實資安、教育訓練、採購規範、配合稽核等五大資安工作重點，詳見【單位主管應辦事項】。

教育機構資安驗證中心針對主管應督導單位人員落實五大資安工作重點設計宣導簡報(https://tinyurl.com/5f8w2fj4)，歡迎各校加以利用，讓單位主管能充分了解如何進行必要的資安作為。另外也拍攝了這部分的宣導影片(https://youtu.be/vRoqoPxtP2U)，各校也可以直接提供給單位主管線上觀看，配合宣導簡報觀看能更快讓單位主管對自己的責任有所了解。

(三) 資通系統及資訊之盤點

全校單位的資通系統盤點，建議可由計資中心人員協助各單位進行資訊資產盤點以及風險評估作業。依據作業指引對全校資通系統進行盤點及風險評估之後，更重要的是系統管理人員、系統委外承辦人員、系統開發人員等三類人員必須充分認知與自身職責相關的稽核重點，進而落實相關資安工作。

【系統管理人員】應注意檢核表「第7構面資通安全防護及控制措施」要求事項，例如系統的防護基準與安全健診、資訊資產與實體環境管理等。【系統委外承辦人員】應注意檢核表「第5構面資通系統或服務委外辦理之管理措施」要求事項，在擬定委外作業徵求說明書(RFP)時，應將防護基準需求納入，建議參考行政院國家資通安全會報技術服務中心「資通系統委外開發RFP」、公共工程委員會「投標須知範本」及「資訊服務採購契約範本」，並將分(轉)包、廠商資安管理評估等項目都納入RFP中。【系統開發人員】應注意檢核表「第8構面資通系統發展及維護

安全」要求事項，資通系統開發過程依安全系統發展生命週期(SSDLC)納入資安要求，若是委外開發則應納入委外契約。

對相關人員進行教育訓練時，詳見【系統管理人員應辦事項】、【系統委外承辦人員應辦事項】、【系統開發人員應辦事項】，歡迎用教育機構資安驗證中心設計的各構面宣導簡報，以及在【落實稽核工作】善用教育機構資安驗證中心提供的檢核自評工具。

（四）內部實施資通安全稽核

依據「資通安全實地稽核項目」的「6.3訂定內部資通安全稽核計畫，包含稽核目標、範圍、時間、程序、人員等，且落實執行？」，既然作業指引建議由行政單位或就資通系統(保有個人資料)風險高低、教學單位特性評估訂定推動先後順序分年分階段規劃辦理內部稽核並且規劃及執行稽核發現事項改善措施，那就應該在內部稽核計畫明確訂定逐年進行範圍直到全校完成稽核，詳見【落實稽核工作】。

依據作業指引分年分階段規劃辦理內部稽核，在此之前更是要讓全校人員都能開始重視資安管理，像是新進人員資安宣導、資安通識教育訓練、落實辦公室資安管理措施、社交工程演練、落實資安事件通報。近年來多數資安事件都發生於一般人員對於資訊安全知識認知不足、使用雲端服務收集個人資料卻未做好管控或是公務個人電腦安裝非公務用軟體等等問題，這些缺失都可以透過落實新進人員資安宣導，每年接受三小時以上資通安全通識教育訓練、社交工程演練來強化人員對資訊安全知識的認知，來避免資安事件發生，詳見【一般人員應辦事項】。

各校以全機關為範圍導入ISMS應優先落實的執行策略

各校以全機關為範圍實施資安管理，請參考本規劃所列應優先落實的執行策略(111年版)，以具體要求學校所有行政、教學、研究單位全面配合優先落實下列資安管理作為。

🔔【單位主管應辦事項】推動執行之建議

基於行政院版檢核表「2.4成立資通安全推動組織，負責推動、協調監督及審查資通安全管理事項？推動組織層級之適切性，且**業務單位是否積極參與**？」，學校必須對行政、教學、研究單位主管進行重點宣導(可引用教育機構資安驗證中心設計的簡報https://tinyurl.com/5f8w2fj4)，要求**單位主管應掌握下列資安管理措施**。

一、在學校資安管理專責單位的協助及教育訓練下，主管應要求**單位自建或委外開發系統(包含APP)之負責人員應落實建立資安管控文件**，以符合下列檢核項目。

項次	檢核內容
4.1	確實**盤點資產建立清冊**(如識別擁有者及使用者等)，且鑑別其資產價值？
4.1.1	依「國立大專校院資通安全維護作業指引」，學校辦理資通系統及資訊之盤點，盤點範圍應包含全校各單位。各校每年提交之「**資通系統資產清冊**」至少應包含落於各校**IP網段內**、或使用各校**網域名稱**之資通系統。
4.2	訂定資產異動管理程序，**定期更新**資產清冊，且落實執行？
4.3	建立風險準則且執行**風險評估**作業，並針對重要資訊資產鑑別其可能遭遇之風險，分析其喪失**機密性、完整性及可用性**之衝擊？

APP另須依據「行政院及所屬各機關行動化服務發展作業原則」第十一條「各機關開發之行動化服務應符合個人資料保護法及行政院訂定之政府資通安全管理等相關規定，並通過經濟部工業局訂定**行動化應用軟體之檢測項目**，始得提供民眾下載使用。」APP開發負責人員應將檢測合格證書提供學校資安管理專責單位，由資安專責人員至政府入口網站管理平臺，辦理服務績效填報及基本資安檢測合格證書上傳作業。教育部109年8月27日臺教資(五)字第1090125304A號函，要求

行動化服務開發需求應依106年7月28日修正「行政院及所屬各機關行動化服務發展作業原則」進行相關評估及開發作業。**此項工作應持續推動，並落實管理機制，隨時可呈報執行成效**。

二、在學校資安管理專責單位的協助及教育訓練下，主管應要求**單位自建或委外設置物聯網設備之負責人員應落實建立資安管控文件**，以符合下列檢核項目。

項次	檢核內容
4.1.2	清查**物聯網設備**，盤點範圍包含機關採購、公務使用之物聯網設備，並建立管理**清冊**？
4.4.1	針對物聯網設備採取適當管控機制，如**連線控管**、**變更廠商預設帳密**、**禁止使用弱密碼**、**修補安全漏洞**？

以上檢核項目的相關實施要求亦可參考教育部110年9月22日臺教資(四)字第1100128345號函，資通系統及資訊資產之盤點應包含物聯網設備(如網路印表機、網路攝影機、門禁設備、環控系統、無線網路基地台、無線路由器等)，盤點清單應檢核不得使用弱密碼、廠商預設密碼，並符合規範之密碼複雜度要求，以及設定適當網路存取限制。**此項工作應持續推動，並落實管理機制，隨時可呈報執行成效**。

三、在學校資安管理專責單位的協助及教育訓練下，主管應要求**單位內落實辦公室資安管理措施，並張貼海報強化宣導效果**(可引用教育機構資安驗證中心設計的海報https://tinyurl.com/4t6xt4ju)，以符合下列檢核項目。

項次	檢核內容
7.10	建立**電子資料**安全管理機制(含防疫個資)，包含**分級**規則(如機密性、敏感性及一般性等)、**存取權限、資料安全、人員管理及處理規範**等，且落實執行？
7.10.1	依「各級學校使用資通系統或服務蒐集及使用個人資料注意事項」，學校為行政目的使用資通系統或雲端資通服務（**如Google表單**、**Microsoft Forms** 等問卷調查服務）涉及蒐集個人資料者，注意**資料蒐集最小化、存取控制及詳閱設定內容**(雲端資通服務)等項目，並落實教育訓練宣導。
7.18	訂定**電子郵件**之使用規則且落實執行，依郵件內容之機密性、敏感性**規範傳送限制**？
7.24	針對**電子資料相關設備**進行安全管理(如相關儲存媒體、設備有**安全處理程序**及**分級**標示、**報廢**程序等)？

7.25	落實資訊設備回收再使用及汰除之安全控制作業程序，以確保任何**機密性或敏感性**資料確實**刪除**？
7.26	針對使用者電腦訂定**軟體安裝管控規則**？確認授權軟體及免費軟體使用情形？
7.19	針對**電腦機房及重要區域**之**安全控制、人員進出管控、環境維護**(如溫溼度控制)等項目建立適當管理措施，落實執行？
7.20	定期評估及檢查重要資通設備之設置地點可能之**危害因素**(如火、煙、水、震動、化學效應、電力供應、電磁輻射或人為入侵破壞等)？
7.21	針對電腦機房及重要區域之公用服務(如水電消防通訊)建立適當之**備援方案**？
7.27	**個人行動裝置及可攜式媒體**訂定管理程序且落實執行，並定期審查、監控及稽核？

檢核項目7.10、7.10.1包含使用雲端服務之管理作為，依據行政院資通安全處108年7月18日院臺護字第1080182934號，提醒機關使用雲端硬碟服務可能受害，應檢視**使用公有雲**之必要性，倘確有使用需求，備妥平時資安告警機制及事件緊急應變作為。而且依據教育部110年9月8日臺教資(四)字第1100122001號，**使用雲端服務蒐集個人資料**應注意個資外洩資安風險。以上兩項可參考教育機構資安驗證中心設計的Google雲端檔案權限管理教學https://tinyurl.com/8ujtwp57、Google表單蒐集個人資料使用原則之實務操作說明https://tinyurl.com/ydzy3j74。**此項工作應持續推動，並落實管理機制，隨時可呈報執行成效**。

檢核項目7.26的相關實施要求亦可參考行政院秘書長109年7月21日院臺護字第1090094901A號函，為避免公務及機敏資料遭不當竊取，應落實辦理公務機關**個人電腦非經核准，不可安裝非公務用軟體**。**此項工作應持續推動，並落實管理機制，隨時可呈報執行成效**。

四、在學校資安管理專責單位的協助及教育訓練下，主管應要求**單位內人員達成必要的資安通識、資安專業訓練**，以符合下列檢核項目。

項次	檢核內容
3.5	人員**瞭解**機關之資通安全政策，以及應負之資安責任？
3.7	**資訊人員**每2年接受3小時以上之資通安全專業課程訓練或資通安全職能訓練，且每年接受3小時以上之資通安全通識教育訓練？
3.8	**一般使用者**及**主管**每年3小時以上資通安全通識教育訓練？

9.5	每半年配合教育部或自行進行1次**社交工程演練**？針對開啟郵件、點閱郵件附件或連結之人員加強資安意識教育訓練？

依據行政院國家資通安全會報網站於111年6月22日公告之資通安全管理法常見問題，FAQ3.18定義了**資訊人員**應包含**負責資通系統委外開發的業務單位人員**，也包含**具有系統維運管理權限的業務單位人員**。這些人員都應依照FAQ3.15規範資安專業訓練課程之認定實施方式，接受資通安全專業課程訓練或資通安全職能訓練。

另外，依據行政院資通安全處108年7月18日院臺護字第1080182934號，提醒有多起利用**社交工程郵件**夾帶微軟Office文件並開啟巨集功能下載惡意程式之攻擊手法，請預設關閉微軟Office文件巨集功能，避免遭有心人士利用進行攻擊。**此項工作應持續推動，並落實管理機制，隨時可呈報執行成效**。

五、學校資安管理專責單位應訂定資訊作業委外安全管理程序，做為全校資訊委外作業依循之依據，主管應要求**單位內辦理採購資通系統與服務委外業務者善盡風險評估及受託者選任監督相關措施**，以符合下列檢核項目。

項次	檢核內容
4.7	針對公務用之資通訊產品，包含軟體、硬體及服務等，**禁止使用大陸廠牌資通訊產品**？
4.7.1	透過委外契約或場地租借使用規定，要求**對外出租場域不得使用大陸廠牌資通訊產品？**
4.8	列冊管理大陸廠牌資通訊產品，並已於**110年底前**將該產品自公務環境中移除？如該產品仍有與公務環境介接之情況，是否經行政院核定評估同意？
5.16	針對涉及資通訊軟體、硬體或服務相關之採購案，契約範圍內之委外廠商是否為**大陸廠商**或所涉及之**人員**？是否有陸籍身分？是否允許委外廠商使用大陸廠牌之**資通訊產品**，包含軟體、硬體及服務等？
5.1	訂定**資訊作業委外安全管理程序**，包含委外選商及監督相關規定，確保委外廠商執行委外作業時，具備完善之資通安全管理措施或通過第三方驗證？
5.1.1	依行政院111年5月26日函送之「**資通系統籌獲各階段資安強化措施**」，將所要求之相關措施納入委外安全管理程序？
5.4	針對委外業務項目進行**風險評估**，以強化委外安全管理？

5.6	依資通系統分級，於**徵求建議書文件(RFP)**相關採購文件中明確**規範防護基準需求**？

檢核項目4.7、4.8、5.16的相關實施要求亦可參考行政院秘書長109年12月18日院臺護長字第1090201804A號函，要求**110年底前完成汰換**所使用或採購大陸廠牌資通訊產品軟體、硬體及服務，其中服務契約範圍所涉及的人員國籍是否為陸籍、所使用的服務是否為大陸所有亦須注意，並配合擴大盤點範圍為全機關，包含委外廠商及其分包廠商。以及可參考行政院秘書長109年7月21日院臺護字第1090094901A號函，為避免公務及機敏資料遭不當竊取，可於招標文件明定限制大陸地區之財物或勞務參與。檢核項目4.7.1是依據教育部111年9月21日臺教資(四)字第1112703805號函有關111年9月5日「111年全國大專校院資安長會議」紀錄，應注意對外出租場域不得使用大陸廠牌資通訊產品(包含軟體、硬體及服務)。**此項工作應持續推動，並落實管理機制，隨時可呈報執行成效**。

檢核項目5.1.1的相關實施要求應參考行政院資通安全處111年5月26日院臺護字第1110174630號函，資通系統籌獲需求、建置、維運各階段資安強化措施：(一)以資訊經費之5%以上估算資安經費為原則，需求規劃過程宜參考「資通系統防護基準驗證實務指引」及「資訊服務採購案之資安檢核事項」相關要求。(二)訂定資安相關評選項目或適當方式檢視、專業人員協助選任。(三)建置階段由資安專業人員協助檢視重點里程碑資安作為及安全軟體開發生命週期(SSDLC)。(四)維運階段由雙方資安人員確認資安管理措施履行及相關稽核工作。另外，檢核項目5.6的相關實施要求亦可參考行政院秘書長110年7月13日院臺護長字第1100177483號函，要求各機關資通訊相關採購案，應參考公共工程委員會「投標須知範本」及「資訊服務採購契約範本」，落實「**資訊服務採購案之資安檢核事項**」相關要求。**此項工作應持續推動，並落實管理機制，隨時可呈報執行成效**。

六、學校資安管理專責單位應訂定內部資通安全稽核計畫，做為全校內部稽核之依據，主管應**要求單位內人員配合稽核並定期追蹤改善情形**，以符合下列檢核項目。

項次	檢核內容
6.3	訂定**內部**資通安全**稽核**計畫，包含稽核目標、範圍、時間、程序、人員等，且落實執行？

6.3.1	依「國立大專校院資通安全維護作業指引」，學校辦理內部資通安全稽核，**稽核範圍應包含全校各單位**。各校得就資通系統(保有個人資料)風險高低、教學單位特性評估訂定推動先後順序，**分年分階段**規劃辦理，並明訂於各校資通安全維護計畫。
6.4	規劃及執行稽核發現事項改善措施，且**定期追蹤改善**情形？

最後，**單位主管在資安管理的配合與執行成效**，應反映於下列資安治理成熟度題項，由學校資安管理專責單位記錄保存相關佐證資料可供查核。

資安治理成熟度題項	現階段應推動執行重點
第2題.具備資安推動組織與執行管理審查	達到成熟度2之條件是「資安推動組織由資通安全長或指派人員擔任管理階層，定期召開管理審查會議，檢視資通安全推動情形。」，為了能落實全校重視資安管理，就應該讓資安推動組織納入具全校代表性的相關成員，也就是邁向成熟度4的「資安推動組織與管理審查會議**包含各單位主管**」。
第7題.規劃資安資源	各單位主管也有責任重視**單位內的資安資源規劃**，達到成熟度2之條件是「針對資安目標與風險需求，規劃所需經費或資源(係指投入於資安之人力、物力及財力)，且定期檢討執行情形。」
第12題.盤點資訊資產與執行風險評鑑	各單位主管也有責任重視**單位內的資訊資產盤點**，達到成熟度2之條件是「已**盤點**資訊資產(至少包含軟體、硬體及人員等)，已執行資安**風險評鑑**，並定期檢討執行情形(如定期依據資安風險評鑑結果，執行相關資安防護措施等)。」
第13題.執行資通系統分級與落實資安防護基準	各單位主管也有責任掌握**單位內的資通系統分級與防護基準**，達到成熟度2之條件是「已**盤點**資通系統，並列出清冊，完成**資通系統分級**及**防護基準**，並檢討執行情形。」

🔔【一般人員應辦事項】推動執行之建議

基於行政院版檢核表「3.8一般使用者及主管**每年3小時**以上**資通安全通識**教育訓練」，學校必須對全體人員進行重點宣導，要求**一般人員應達成下列資安管理要求**。

一、依據行政院資通安全處109年9月14日院臺護字第1090188336號函，為協助各機關新進人員儘速了解基本資安認知，行政院資通安全處訂定「**新進人員資安宣導單**(範本)」1份，參考並視需要調修內容後納入新進同仁報到程序，並確認同仁確實接收相關訊息，必要時得辦理測驗。**此項工作應持續推動，並落實管理機制，隨時可呈報執行成效**。

二、由學校資安管理專責單位提供教育訓練課程或學習資源，要求全體人員應**每年接受3小時以上之資通安全通識教育訓練**，以符合下列檢核項目。

項次	檢核內容
3.4	訂定人員之資通安全作業程序及權責？明確告知保密事項，且**簽署保密協議**？
3.5	人員**瞭解**機關之資通安全政策，以及應負之資安責任？
3.8	**一般使用者**及**主管**每年3小時以上資通安全通識教育訓練？

依據行政院國家資通安全會報網站於111年6月22日公告之資通安全管理法常見問題，FAQ3.16說明資安通識教育訓練可由機關自行辦理，**實體課程或數位課程均可**。而所謂的一般使用者及主管，不僅機關編制內人員，亦須包含會操作機關資通系統的人員(註譬如協助行政作業程序使用資通系統的工讀生)。

下列學習資源提供參考：

- ｅ等公務園+學習平臺
  https://sites.google.com/email.nchu.edu.tw/isms-training/
- CS資安防衛戰
  https://sites.google.com/email.nchu.edu.tw/isms-game/
- 全民資安素養網
  https://sites.google.com/email.nchu.edu.tw/isafemoe/
- 教育機構資安驗證中心數位課程
  https://sites.google.com/email.nchu.edu.tw/iscbonlinecourse/
  此課程線上施測的「零成本雲端測驗發證」機制也開放自行運用
  https://sites.google.com/email.nchu.edu.tw/online-exam/

三、學校全體人員應**落實辦公室資安管理措施，並張貼海報強化宣導效果**(可引用教育機構資安驗證中心設計的海報https://tinyurl.com/4t6xt4ju)，以符合下列檢核項目。

項次	檢核內容
7.10	建立**電子資料**安全管理機制(含防疫個資)，包含**分級**規則(如機密性、敏感性及一般性等)、**存取權限、資料安全、人員管理及處理規範**等，且落實執行？
7.10.1	依「各級學校使用資通系統或服務蒐集及使用個人資料注意事項」，學校為行政目的使用資通系統或雲端資通服務（**如Google 表單**、**Microsoft Forms** 等問卷調查服務）涉及蒐集個人資料者，注意**資料蒐集最小化、存取控制及詳閱設定內容**(雲端資通服務)等項目，並落實教育訓練宣導。
7.18	訂定**電子郵件**之使用規則且落實執行，依郵件內容之機密性、敏感性**規範傳送限制**？
7.24	針對**電子資料相關設備**進行安全管理(如相關儲存媒體、設備有**安全處理程序**及**分級**標示、**報廢**程序等)？
7.25	落實資訊設備回收再使用及汰除之安全控制作業程序，以確保任何**機密性或敏感性**資料確實**刪除**？
7.26	針對使用者電腦訂定**軟體安裝管控規則**？確認授權軟體及免費軟體使用情形？
7.19	針對**電腦機房及重要區域**之**安全控制、人員進出管控、環境維護**(如溫溼度控制)等項目建立適當管理措施，落實執行？
7.20	定期評估及檢查重要資通設備之設置地點可能之**危害因素**(如火、煙、水、震動、化學效應、電力供應、電磁輻射或人為入侵破壞等)？
7.21	針對電腦機房及重要區域之公用服務(如水電消防通訊)建立適當之**備援方案**？
7.27	**個人行動裝置及可攜式媒體**訂定管理程序且落實執行，並定期審查、監控及稽核？

檢核項目7.10、7.10.1包含使用雲端服務之管理作為，依據行政院資通安全處108年7月18日院臺護字第1080182934號，提醒機關使用雲端硬碟服務可能受害，應檢視**使用公有雲**之必要性，倘確有使用需求，備妥平時資安告警機制及事件緊急應變作為。而且依據教育部110年9月8日臺教資(四)字第1100122001號，**使用雲端服務蒐集個人資料**應注意個資外洩資安風險。以上兩項可參考教育機構資安驗證中心設計的Google雲端檔案權限管理教學https://tinyurl.com/8ujtwp57、Google表

單蒐集個人資料使用原則之實務操作說明https://tinyurl.com/ydzy3j74。**此項工作應持續推動，並落實管理機制，隨時可呈報執行成效**。

檢核項目7.26的相關實施要求亦可參考行政院秘書長109年7月21日院臺護字第1090094901A號函，為避免公務及機敏資料遭不當竊取，應落實辦理公務機關**個人電腦非經核准，不可安裝非公務用軟體**。**此項工作應持續推動，並落實管理機制，隨時可呈報執行成效**。

四、教育部對大學每半年實施一次社交工程演練，演練前應加強學校全體人員教育訓練(可參考教育機構資安驗證中心設計的社交工程主題網站https://socialengineering.email.nchu.edu.tw)，強化資安意識，以符合下列檢核項目。社交工程演練成績未達標準的學校，必須擬定改善計畫並針對開啟信件或點選連結人員加強訓練宣導。

項次	檢核內容
9.5	每半年配合教育部或自行進行1次**社交工程演練**？針對開啟郵件、點閱郵件附件或連結之人員加強資安意識教育訓練？

檢核項目9.5的相關實施要求亦可參考行政院資通安全處108年7月18日院臺護字第1080182934號，提醒有多起利用**社交工程郵件**夾帶微軟Office文件並開啟巨集功能下載惡意程式之攻擊手法，請預設關閉微軟Office文件巨集功能，避免遭有心人士利用進行攻擊。**此項工作應持續推動，並落實管理機制，隨時可呈報執行成效**。

五、學校採購、公務使用之物聯網設備，**負責人員應落實建立資安管控文件**，以符合下列檢核項目。

項次	檢核內容
4.1.2	清查**物聯網設備**，盤點範圍包含機關採購、公務使用之物聯網設備，並建立管理**清冊**？
4.4.1	針對物聯網設備採取適當管控機制，如**連線控管**、**變更廠商預設帳密**、**禁止使用弱密碼**、**修補安全漏洞**？

以上檢核項目的相關實施要求亦可參考教育部110年9月22日臺教資(四)字第1100128345號函，資通系統及資訊資產之盤點也應包含物聯網設備(如網路印表機、網路攝影機、門禁設備、環控系統、無線網路基地台、無線路由器等)，盤點清單應檢核不得使用弱密碼、廠商預設密碼，並符合規範之密碼複雜度要求，以及設定適當網路存取限制。**此項工作應持續推動，並落實管理機制，隨時可呈報執行成效**。

六、學校資安管理專責單位應訂定**資安事件通報**處理程序，加強學校全體人員宣導具備資安危機意識，一般人員至少能在遭遇如(1)公務電子郵件遭遇到侵害權益、假冒來源、內容有惡意連結時；(2)公務上使用通訊軟體未重視資安問題，像是群組傳遞敏感資料時；(3)公務電腦遭遇無法解決的病毒、木馬，或有人使用可疑的免費共享軟體時；(4)各單位機房的門禁出問題或發生重大異常事件，辦公室的敏感資料外流時。必須能意識到公務資安危機，聯繫學校資安通報窗口協助判斷與處理，以符合下列檢核項目。

項次	檢核內容
3.3	指定**專人或專責單位**負責資訊服務請求/事件處理、維運及檢討，且有適切分工？
9.8	訂定資安事件處理過程之**內部及外部溝通程序**？
9.9	所有資安事件，保留**完整紀錄**，並與其他相關管理流程連結，且落實執行後續檢討及改善？
9.7	近2年重大資安事件之**通報時間、過程、因應處理及改善措施**，依程序落實執行？
9.16	**第三級或第四級**資通安全事件後，由**資通安全長召開會議**協商相關事宜，並得請相關機關提供協助？

最後，**一般人員的資安管理作為與執行成效**，應反映於下列資安治理成熟度題項，由學校資安管理專責單位記錄保存相關佐證資料可供查核。

資安治理成熟度題項	現階段應推動執行重點
第18題.資訊人員、一般使用者及主管應具備資安認知且資訊人員應具備資安技能	達到成熟度2之條件是「一般使用者及主管每人**每年接受3小時**以上之**資通安全通識**教育訓練」
第20題.宣導資安政策與相關資安要求	達到成熟度2之條件是「針對全體人員執行資安政策與相關資安要求宣導(如透過**教育訓練、內部會議、公文、張貼公告**等)，且定期檢討執行情形(如檢討資安政策與相關資安要求宣導活動之規劃與執行作業等)。」
第23題.落實機敏資訊之加密管理	達到成熟度2之條件是「針對**機敏資訊**於**儲存或傳輸**時之加密措施有管理做法或機制，並檢討執行情形。」

第24題.執行惡意軟體之偵測與預防	達到成熟度2之條件是「執行惡意軟體偵測與預防措施(至少包含**限制未授權軟體**與**安裝防毒軟體**等)有管理做法或機制，並檢討執行情形。」
第29題.執行儲存媒體之防護措施	達到成熟度2之條件是「針對**機密與敏感性資料之儲存媒體**實施防護措施(至少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等)有管理做法或機制，並檢討執行情形。」
第26題.落實電子郵件安全管理	達到成熟度2之條件是「執行電子郵件之安全防護措施(至少包含建置**電子郵件之垃圾件過濾**與**電子郵社交工程演練**等)有管理做法或機制，並檢討執行情形。」
第36題.執行資安事件通報應變	達到成熟度2之條件是「針對**資安事件之通報與處理**(如召開會議檢討事件執行情形等)有管理做法或機制，並檢討執行情形。」
第37題.保存資通系統與資安設備日誌紀錄	達到成熟度2之條件是「針對資通系統與資安設備之**日誌紀錄**有管理做法或機制(日誌紀錄存取，應限定僅由系統管理者或具讀取權限者存取，日誌紀錄宜包含帳號、IP、時間、操作項目及執行參數，並由主管複核執行成果)，並檢討執行情形。」

🔔【系統管理員應辦事項】推動執行之建議

基於行政院版檢核表「第7構面**資通安全防護及控制措施**」，學校必須對各單位建置的系統之管理人員進行重點宣導(可引用教育機構資安驗證中心設計的簡報https://tinyurl.com/ym6k5uem)，要求**系統管理員應落實下列資安管理措施**。

一、**系統與服務獲得**，應符合下列檢核項目。

項次	檢核內容
7.1	針對**全部核心資通系統**定期辦理網站安全**弱點掃瞄**？(A級機關每年2次，B級機關每年1次，C級機關每2年1次。)
7.2	針對**全部核心資通系統**定期辦理系統**滲透測試**？(A級機關每年1次，B、C級機關每2年1次。)
8.9	將開發、測試及正式作業環境**區隔**，不同作業環境建立適當之資安保護措施？
8.11	測試如使用正式作業環境之**測試資料**，建立保護措施且留存相關作業**記錄**？
8.7	資通系統上線或更版前，執行**安全性要求測試**，包含**邏輯及安全性驗測**、**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**等，且檢討執行情形？
8.12	針對資通系統使用之**外部元件或軟體**，注意其安全漏洞通告且**定期評估**更新？

檢核項目8.7的相關案例可參考教育部110年6月29日臺教資(四)字第1100085899號函，基於多起因管理不當導致**重大資通安全事件**進行相關**根因分析**，包含「弱密碼及身分驗證缺失」、「未落實安全軟體發展生命週期(SSDLC)相關要求」，其中相關案例A：某學術單位未落實SSDLC相關要求，忘記密碼功能具有未發現之安全邏輯漏洞，致帳號遭未授權登入，洩漏多筆個人資料。案例B：某大學X系統因應疫情變化緊急上線，未經適當安全性測試程序，存在安全弱點致個資可被他人不當存取。有鑑於重大資通安全事件造成影響甚鉅，如因管理不當導致資通安全事件，教育部將以不遮蔽方式做成宣導案例，也將列入專案實地稽核，並循相關機制提報懲處。

二、**事件日誌與可歸責性**，應符合下列檢核項目。

項次	檢核內容
9.12	訂定應記錄之**特定資通系統事件**(如身分驗證失敗、存取資源失敗、重要行為、重要資料異動、功能錯誤及管理者行為等)、**日誌內容**、**記錄時間週期**及**留存政策**，且保留日誌**至少6個月**？
9.13	依日誌儲存需求，配置所需之**儲存容量**，並於日誌處理**失效時**採取**適當行動及提出告警**？
9.14	針對日誌之**存取控管**，並有適當之**保護控制措施**？

以上檢核項目的相關實施要求亦可參考行政院資通安全處108年7月18日院臺護字第1080182934號，要求對於重要資通訊設備及系統皆應**啟動存取稽核紀錄**，並妥善留存以利事後查核。**此項工作應持續推動，並落實管理機制，隨時可呈報執行成效**。

三、**系統與通訊保護**，應符合下列檢核項目。

項次	檢核內容
1.4	設置資通系統之**備援**設備，當系統服務中斷時，於可容忍時間內由備援設備取代提供服務？(**中/高**等級資通系統適用)
1.5	定期執行**重要**資料之**備份**作業，且備份資料**異地存放**？存放處所環境符合實體安全防護？
1.6	訂定備份資料之復原程序，且定期執行**回復測試**，以確保備份資料之有效性？復原程序定期檢討及修正？
1.7	針對核心資通系統制定**業務持續運作計畫**，並定期辦理全部**核心**資通系統之業務持續運作演練，包含人員職責應變、作業程序、資源調配及檢討改善等
1.7.1	轄管資通系統**網站**(包含學校系所、行政單位網站)**內容遭竄改時**，備妥**應變機制**，以利於發現網頁遭竄改後10分鐘內切換為維護公告頁面，並納入業務持續運作計畫**演練**情境？
7.11	建立**網路服務安全控制措施**且定期檢討？定期檢測網路運作環境之安全漏洞？
7.12	設定防火牆並**定期檢視防火牆規則**，有效掌握與管理防火牆連線部署？
7.13	針對機關內部同仁及委外廠商進行**遠端維護**資通系統，採「**原則禁止、例外允許**」方式辦理，並有適當之防護措施？

7.17	使用**預設密碼**登入資通系統時，於**登入後**要求立即**變更**密碼，並**限制使用弱密碼**？
7.16	資通系統**重要組態設定檔案**及其他**具保護需求**之資訊是否加密或其他適當方式儲存(如實體隔離、專用電腦作業環境、資料加密等)？針對系統與資料傳輸之**機密性與完整性**建立適當之防護措施？
7.22	針對**資訊之交換**，建立適當之交換程序及安全保護措施，以確保資訊之完整性及機密性？針對重要資料的交換過程，保存適當之監控紀錄？

檢核項目1.7.1依據教育部111年9月21日臺教資(四)字第1112703805號函有關111年9月5日「111年全國大專校院資安長會議」紀錄之要求，系統網站內容遭竄改時10分鐘內切換為維護公告頁面，並納入業務持續運作計畫演練情境。**此項工作應持續推動，並落實管理機制，隨時可呈報執行成效**。

檢核項目7.13的相關實施要求亦可參考行政院資通安全處110年3月2日院臺護字第1100165761號函，各機關開放機關內部同仁及委外廠商進行**遠端維護**資通系統，應採「**原則禁止、例外允許**」方式辦理，若機關因地理限制、處理時效及專案特性等因素，須開放前揭人員自遠端存取資通系統時，應至少辦理下列防護措施：(一)依資通安全管理法施行細則第4條及資通安全責任等級分級辦法附表十中有關遠端存取相關規定辦理，並建立及落實管理機制。(二)開放遠端存取期間原則以短天期為限，並建立異常行為管理機制。(三)於結束遠端存取期間後，應確實關閉網路連線，並更換遠端存取通道(如VPN)登入密碼。**此項工作應持續推動，並落實管理機制，隨時可呈報執行成效**。

檢核項目7.16的相關實施要求亦可參考行政院資通安全處110年1月14日院臺護字第1100160761號函，資通訊系統經機關評定為「**高**」等級之系統防護需求者，應依「資通安全責任等級分級辦法」規定，其**靜置資訊**及相關具保護需求之**機密資訊**應**加密儲存**。如發現機敏資訊有遭洩漏外洩情形，應依「資通安全事件通報及應變辦法」進行通報，並依限完成事件損害控制、復原、調查及改善。個人資料如有被竊取、洩漏、竄改或其他侵害者，應依「個人資料保護法」規定，於查明後以適當方式通知當事人。**此項工作應持續推動，並落實管理機制，隨時可呈報執行成效**。

四、**資通安全防護**，配合學校資安管理專責單位的要求，應符合下列檢核項目。

項次	檢核內容
7.5	完成**政府組態基準**導入作業？(**A、B**級機關應於核定後**1年內導入**)
7.6	完成**資通安全弱點通報機制(VANS)**導入作業，並持續維運及依主管機關指定方式提交資訊資產盤點資料？ (**A、B**級機關應於核定後**1年內導入**；**C**級機關應於核定後**2年內導入**。支持**核心業務**持續運作相關之資通系統主機與電腦應於規定時限內完成導入。)
7.7	完成**端點偵測及應變機制(EDR)**導入作業，並持續維運及依主管機關指定方式提交偵測資料？ (**A、B**級機關應於核定後**2年內導入**。支持**核心業務**持續運作相關之資通系統主機與電腦應於規定時限內完成導入。如囿於經費，可考量與核心業務之關聯性、資安風險程度及資訊資產重要性等，優先擇定並**分年**完成導入。)
7.8	依機關所屬等級建置應具備的**資通安全防護**措施：**A、B、C**級機關均應建置防毒軟體、網路防火牆、具有郵件伺服器者應備電子郵件過濾機制；**A、B**級機關應建置入侵偵測及防禦機制、具有對外服務之核心資通系統應備應用程式防火牆；A級機關應建置進階持續性威脅攻擊防禦措施。
7.9	負責電子郵件過濾系統管理者，定期檢討及更新**郵件過濾規則**？電子郵件進行**分析**，主動發現異常行為且進行改善(如針對大量異常電子郵件來源之IP位址，於防火牆進行阻擋等)？

五、**資通安全健診**，應符合下列檢核項目。

項次	檢核內容
7.3	**A**級機關**每年1次**，**B、C**級機關**每2年1次**辦理**資通安全健診**，包含網路架構檢視、網路惡意活動檢視、使用者電腦惡意活動檢視、伺服器主機惡意活動檢視、目錄伺服器設定及防火牆設定檢視等？
7.4	針對安全性檢測及資通安全健診結果**執行修補**作業，且於修補完成後驗證完成改善？

六、**資訊資產管理**，應符合下列檢核項目。

項次	檢核內容
4.1	確實**盤點資產建立清冊**(如識別擁有者及使用者等)，且鑑別其資產價值？
4.1.1	依「國立大專校院資通安全維護作業指引」，學校辦理資通系統及資訊之盤點，盤點範圍應包含全校各單位。各校每年提交之「**資通系統資產清冊**」至少應包含落於各校**IP網段內**、或使用各校**網域名稱**之資通系統。
4.2	訂定資產異動管理程序，**定期更新**資產清冊，且落實執行？
4.3	建立風險準則且執行**風險評估**作業，並針對重要資訊資產鑑別其可能遭遇之風險，分析其喪失**機密性、完整性及可用性**之衝擊？
7.10	建立**電子資料**安全管理機制(含防疫個資)，包含**分級**規則(如機密性、敏感性及一般性等)、**存取權限、資料安全、人員管理及處理規範**等，且落實執行？
7.24	針對**電子資料相關設備**進行安全管理(如相關儲存媒體、設備有**安全處理程序**及**分級**標示、**報廢**程序等)？
7.25	落實資訊設備回收再使用及汰除之安全控制作業程序，以確保任何**機密性或敏感性**資料確實**刪除**？
7.26	針對使用者電腦(在此是指系統管理者登入系統進行管理所使用的電腦)訂定**軟體安裝管控**規則？確認**授權軟體**及**免費軟體**之使用情形，且定期檢查？
7.27	針對個人**行動裝置及可攜式媒體**(在此是指系統管理者登入系統進行管理時有使用到的裝置)訂定管理程序，且落實執行，並定期審查、監控及稽核？

七、**電腦機房門禁管理**，應符合下列檢核項目。

項次	檢核內容
7.19	針對**電腦機房及重要區域**之**安全控制、人員進出管控、環境維護**(如溫溼度控制)等項目建立適當管理措施，落實執行？

八、**電腦機房環境控制**，應符合下列檢核項目。

項次	檢核內容
7.20	定期評估及檢查重要資通設備之設置地點可能之**危害因素**(如火、煙、水、震動、化學效應、電力供應、電磁輻射或人為入侵破壞等)？
7.21	針對電腦機房及重要區域之公用服務(如水電消防通訊)建立適當之**備援方案**？

最後，**系統管理員的資安管理作為與執行成效**，應反映於下列資安治理成熟度題項，由學校資安管理專責單位記錄保存相關佐證資料可供查核。

資安治理成熟度題項	現階段應推動執行重點
第12題.盤點資訊資產與執行風險評鑑	達到成熟度2之條件是「已**盤點**資訊資產(至少包含軟體、硬體及人員等)，已執行資安**風險評鑑**，並定期檢討執行情形(如定期依據資安風險評鑑結果，執行相關資安防護措施等)。」
第13題.執行資通系統分級與落實資安防護基準	達到成熟度2之條件是「已**盤點資通系統**，並列出清冊，完成資通系統**分級**及**防護基準**，並檢討執行情形。」
第22題.管理資通系統權限	達到成熟度2之條件是「針對資通系統設置**一般權限**與**特殊權限**要求(至少包含存取控制政策、角色權責區分及權限申請與變更作業等)有管理做法或機制，並檢討執行情形。」
第23題.落實機敏資訊之加密管理	達到成熟度2之條件是「針對**機敏資訊**於**儲存或傳輸**時之加密措施有管理做法或機制，並檢討執行情形。」
第25題.執行遠距工作安全控制措施	達到成熟度2之條件是「執行遠距工作之安全措施(至少包含對於**每一種允許之遠端存取類型**，均應先取得**授權**，建立**使用限制**、**組態**需求、連線需求及文件化，並採用**伺服端之集中過濾機制檢查**使用者授權等)有管理做法或機制(應**監控**資通系統遠端連線，資通系統應採用**加密**機制，資通系統遠端存取之來源應為機關已**預先定義及管理控制點**)，並檢討執行情形。」

第28題.執行資料備份	達到成熟度2之條件是「對資料進行備份(至少包含**重要資料備份**與**異地存放**等)，針對資料之備份作業有管理做法或機制(依資料等級、重要性，規劃備份方式與頻率，重要資料備份保存**至少3代**，執行安全距離之異地備份，針對具機敏性的資料進行**加密**保護，定期透過**復原測試**以確認備份之有效性)，並檢討執行情形。」
第31題.落實資通安全防護	達到成熟度2之條件是「執行資通安全防護(至少包含**防毒軟體**、**網路防火牆**)，且依機關所屬等級建置應具備的防護措施如入侵偵測及防禦機制、具有對外服務之核心資通系統應備應用程式防火牆、進階持續性威脅攻擊防禦措施。」
第32題.執行政府組態基準	達到成熟度2之條件是「**導入**與**持續維運**政府組態基準，並檢討執行情形。」
第33題.執行資通安全健診	達到成熟度2之條件是「依規定週期執行**資通安全健診**，並檢討執行情形。」
第37題.保存資通系統與資安設備日誌紀錄	達到成熟度2之條件是「針對資通系統與資安設備之**日誌紀錄**有管理做法或機制(日誌紀錄存取，應限定僅由系統管理者或具讀取權限者存取，日誌紀錄宜包含帳號、IP、時間、操作項目及執行參數，並由主管複核執行成果)，並檢討執行情形。」
第27題.落實機房管理	達到成熟度2之條件是「針對電腦機房之安全防護措施(如檢視機房**門禁授權名單**與設備、管理機房**溫濕度**等)有管理做法或機制，並檢討執行情形。」

🔔【系統委外承辦人員應辦事項】推動執行之建議

基於行政院版檢核表「第5構面**資通系統或服務委外辦理之管理措施**」，要求**系統委外承辦人員應落實下列資安管理措施**。學校必須對系統委外承辦人員進行重點宣導(可引用教育機構資安驗證中心設計的簡報 https://tinyurl.com/5b85ehnn)，負責資通系統或服務委外的承辦人必須知道如何具體要求委外廠商落實資安管理，承辦人員對於相關資安規範有充分了解與掌握，才可以監督及驗收廠商所交付的資通系統或服務。

另外，依據行政院資通安全處109年6月30日院臺護字第10900179556號函，調查資安責任等級A、B、C級公務機關之**委外情形**。**此項工作應持續推動，並落實管理機制，隨時可呈報調查狀況**。

一、依據行政院國家資通安全會報網站於111年6月22日公告之資通安全管理法常見問題，FAQ3.18定義了**資訊人員**應包含負**責資通系統委外開發的業務單位人員**，也包含**具有系統維運管理權限的業務單位人員**。這些人員都應依照FAQ3.15規範資安專業訓練課程之認定實施方式，接受資通安全專業課程訓練或資通安全職能訓練，以符合下列檢核項目。

項次	檢核內容
3.7	**資訊人員**每2年接受3小時以上之資通安全專業課程訓練或資通安全職能訓練，且每年接受3小時以上之資通安全通識教育訓練？

學校資安管理專責單位應全面為各單位負責系統委外承辦人員實施訓練課程，課程內容宜納入資通安全法規遵循、委外辦理之管理措施、資通系統防護基準、安全系統發展生命週期等主題，建議可參考教育機構資安驗證中心規劃的「**資通系統委外業務人員專業課程**」大綱。(https://sites.google.com/email.nchu.edu.tw/iscb-corporate-training-1/)

二、學校資安管理專責單位應訂定**資訊作業委外安全管理程序**，包含委外選商及監督相關規定。系統委外承辦人員應遵守程序執行委外業務，自行擔任或另行指定專案管理人員，負責委外專案之執行成效監督方式，如時程管控、安全管控等，以符合下列檢核項目。

項次	檢核內容
5.1	訂定**資訊作業委外安全管理程序**，包含委外**選商**及**監督**相關規定。
5.1.1	依行政院111年5月26日函送之「**資通系統籌獲各階段資安強化措施**」，將所要求之相關措施納入委外安全管理程序?

5.2	機關及委外廠商皆已指定**專案管理人員**，負責委外作業之資通安全管理事項？
5.3	委外廠商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**？
5.10	委外關係**終止或解除**時，確認委外廠商返還、移交、刪除或銷毀持有資料？

檢核項目5.1.1的相關實施要求應參考行政院資通安全處111年5月26日院臺護字第1110174630號函，資通系統籌獲需求、建置、維運各階段資安強化措施：(一)以資訊經費之5%以上估算資安經費為原則，需求規劃過程宜參考「資通系統防護基準驗證實務指引」及「資訊服務採購案之資安檢核事項」相關要求。(二)訂定資安相關評選項目或適當方式檢視、專業人員協助選任。(三)建置階段由資安專業人員協助檢視重點里程碑資安作為及安全軟體開發生命週期(SSDLC)。(四)維運階段由雙方資安人員確認資安管理措施履行及相關稽核工作。**此項工作應持續推動，並落實管理機制，隨時可呈報執行成效**。

三、**委外業務風險評估**，以「風險評估記錄(或相關會議記錄)」來做佐證，確認委外業務對於現有資產、流程、作業環境或特殊威脅之影響，以符合下列檢核項目。

項次	檢核內容
5.4	針對**委外業務項目進行風險評估**，包含可能影響資產、流程、作業環境或特殊對機關之威脅，以強化委外安全管理？

四、**禁止使用大陸廠牌資通訊產品及人員**，建議校內各單位在執行購案時，資通訊產品應該要求廠商在簽約時提供無大陸製品(品牌)之切結書(若是部分元件有陸製品難以逐一檢核判定)，並落實宣導(可參考教育機構資安驗證中心設計的限制使用危害國家資通安全產品主題網站 https://tinyurl.com/mpsrvn79)。

項次	檢核內容
4.7	針對公務用之資通訊產品，包含軟體、硬體及服務等，**禁止使用大陸廠牌資通訊產品**？
4.7.1	透過委外契約或場地租借使用規定，要求**對外出租場域不得使用大陸廠牌資通訊產品**？

4.8	列冊管理大陸廠牌資通訊產品，並已於**110年底前**將該產品自公務環境中移除？如該產品仍有與公務環境介接之情況，是否經行政院核定評估同意？
5.16	針對涉及資通訊軟體、硬體或服務相關之採購案，契約範圍內之委外廠商是否為**大陸廠商**或所涉及之**人員**？是否有陸籍身分？是否允許委外廠商使用大陸廠牌之**資通訊產品**，包含軟體、硬體及服務等？

檢核項目4.7、4.8、5.16的相關實施要求亦可參考行政院秘書長109年12月18日院臺護長字第1090201804A號函，要求**110年底前完成汰換**所使用或採購大陸廠牌資通訊產品軟體、硬體及服務，其中服務契約範圍所涉及的人員國籍是否為陸籍、所使用的服務是否為大陸所有亦須注意，並配合擴大盤點範圍為全機關，包含委外廠商及其分包廠商。以及可參考行政院秘書長109年7月21日院臺護字第1090094901A號函，為避免公務及機敏資料遭不當竊取，可於招標文件明定限制大陸地區之財物或勞務參與。檢核項目4.7.1是依據教育部111年9月21日臺教資(四)字第1112703805號函有關111年9月5日「111年全國大專校院資安長會議」紀錄，應注意對外出租場域不得使用大陸廠牌資通訊產品(包含軟體、硬體及服務)。**此項工作應持續推動，並落實管理機制，隨時可呈報執行成效**。

五、**RFP規範防護基準**，建議可參考行政院國家資通安全會報技術服務中心的「資通系統委外開發RFP」，或者在RFP增加一節「資安需求」有這樣的文字：「本專案之系統開發或維運，必須依據本機關對該系統訂定等級(普/中/高)，完成資通安全責任等級分級辦法附表十資通系統防護基準之該等級全部適用項目要求」，以符合下列檢核項目。

項次	檢核內容
5.6	依資通系統分級，於**徵求建議書文件(RFP)**相關採購文件中明確規範**防護基準**需求？
8.8	資通系統開發委外辦理，將**系統發展生命週期**各階段**安全**需求納入委外契約？

檢核項目5.6的相關實施要求亦可參考依據行政院秘書長110年7月13日院臺護長字第1100177483號函，要求各機關資通訊相關採購案，應參考公共工程委員會「投標須知範本」及「資訊服務採購契約範本」，落實「**資訊服務採購案之資安檢核事項**」相關要求。另外應參考行政院資通安全處111年5月26日院臺護字第1110174630號函，資通系統籌獲需求、建置、維運各階段資安強化措施，要求作業方式應訂定資

安相關評選項目或適當方式檢視、專業人員協助選任。**此項工作應持續推動，並落實管理機制，隨時可呈報執行成效**。

六、**分(轉)包資安措施**，建議在RFP的「資安需求」有這樣的文字：「本專案允許複委託範圍，複委託之廠商亦須具備本專案受託廠商相同的資通安全維護措施」，以符合下列檢核項目。

項次	檢核內容
5.5	依委外業務項目性質允許委外廠商就委外業務項目分(轉)包？如允許分(轉)包，注意分(轉)包之範圍，以及分(轉)包之廠商具備資通安全維護措施？

七、**廠商資安管理評估**，建議可採用資通安全維護計畫範本參考附件9「委外廠商查核項目表」，在RFP的「資安需求」有這樣的文字：「本專案之受託廠商必須於服務建議書提出時附上委外廠商資訊安全自評表」，以符合下列檢核項目。

項次	檢核內容
5.7	對於資通系統之委外廠商，針對其人員(如能力、背景等)及開發維運環境之資通安全管理進行評估？

以上檢核項目外應參考行政院資通安全處111年5月26日院臺護字第1110174630號函，資通系統籌獲需求、建置、維運各階段資安強化措施，要求作業方式應訂定資安相關評選項目或適當方式檢視、專業人員協助選任。

八、**定期檢視人員媒體**，委外人員之監督管理的落實度與適切性，要能降低委外廠商對機關資通安全造成影響，要求廠商對於委外人員異動管控、儲存媒體管控記錄、帳號異動及人員進出記錄、伺服器主機系統組態更新異動記錄等定期提出相關報告備查，以符合下列檢核項目。

項次	檢核內容
5.15	定期檢視並分析資訊作業委外之人員安全、媒體保護管控、使用者識別及鑑別、組態管控等相關紀錄？

九、**要求委外廠商應配合落實的資安管理作為**，包含：資安責任保密規定、資安事件通報處理、定期或異常時稽核、廠商進出範圍限制、系統存取程序授權、系統安全檢測證明，以符合下列檢核項目。

項次	檢核內容
5.11	訂定委外廠商之資通安全責任及保密規定，且落實執行？

5.9	訂定委外廠商對於機關委外業務之資安事件通報相關處理規範？委外廠商違反資通安全相關法令或知悉資通安全事件時，立即通知機關並採行補救措施？
5.12	定期或於知悉委外廠商發生可能影響委外作業之資通安全事件時，對委外廠商所提供之服務、報告及紀錄等進行管理及安全檢視，以利後續追蹤及管理？
5.13	委外廠商專案成員進出機關範圍被限制？委外廠商駐點人員使用之資訊設備(如個人、筆記型、平板電腦、行動電話及智慧卡等)建立相關安全管控措施？
5.14	訂定委外廠商系統存取程序及授權規定(如限制可接觸系統、檔案及資料範圍)？委外廠商專案人員調整及異動，依系統存取授權規定，調整其權限？
7.13	針對機關內部同仁及委外廠商進行**遠端維護**資通系統，採「**原則禁止、例外允許**」方式辦理，並有適當之防護措施？
5.8	客製化資通系統開發要求委外廠商提供資通系統之安全性檢測證明，並針對非委外廠商自行開發之系統或資源標示其來源及提供授權證明？

以上檢核項目應參考行政院資通安全處111年5月26日院臺護字第1110174630號函，資通系統籌獲需求、建置、維運各階段資安強化措施，要求作業方式應於維運階段由雙方資安人員確認資安管理措施履行及相關稽核工作。

檢核項目7.13的相關實施要求亦可參考行政院資通安全處110年3月2日院臺護字第1100165761號函，各機關開放機關內部同仁及委外廠商進行**遠端維護**資通系統，應採「**原則禁止、例外允許**」方式辦理，若機關因地理限制、處理時效及專案特性等因素，須開放前揭人員自遠端存取資通系統時，應至少辦理下列防護措施：(一)依資通安全管理法施行細則第4條及資通安全責任等級分級辦法附表十中有關遠端存取相關規定辦理，並建立及落實管理機制。(二)開放遠端存取期間原則以短天期為限，並建立異常行為管理機制。(三)於結束遠端存取期間後，應確實關閉網路連線，並更換遠端存取通道(如VPN)登入密碼。**此項工作應持續推動，並落實管理機制，隨時可呈報執行成效**。

最後，**系統委外承辦人員的資安管理作為與執行成效**，應反映於下列資安治理成熟度題項，由學校資安管理專責單位記錄保存相關佐證資料可供查核。

資安治理成熟度題項	現階段應推動執行重點
第14題.評估委外廠商資安專業能力	達到成熟度2之條件是「針對**委外廠商**之資安專業資格或能力、資安專業技術能力、專案管理能力、廠商本身能力有管理做法或機制，並檢討執行情形。」
第15題.確保委外廠商資安管理	達到成熟度2之條件是「於**委外文件納入資安防護要求**(如保密協議、設備攜出/入規定、契約履約或終止後要求廠商刪除返還資料、於發生資安事件時必須通報機關並執行相關配合辦理、軟體交付前完成資安檢測作業、實施供應商資訊安全教育訓練、個人料處理保護要求等)，針對**委外資安防護要求**(如於委外專案會議，檢視資安管理要求達成情形)有管理做法或機制，並檢討執行情形。」
第16題.確保委外廠商資安稽核	達到成熟度2之條件是「進行委外廠商之資安稽核(至少包含**書面或實地稽核**等)，針對委外資安稽核作業(如已規劃委外資安稽核時程、項目並執行後續改善追蹤事宜等)有管理做法或機制，並檢討執行情形。」

🔔【系統開發人員應辦事項】推動執行之建議

基於行政院版檢核表「8.2資通系統開發過程依安全系統發展生命週期納入資安要求？」，必須要求**系統開發人員**落實**安全系統發展生命週期(Secure Software Development Life Cycle, SSDLC)**。原則上，以資安法實施後的新建或改版完成之資訊系統(不論是自行建置或委外開發)，發展過程應導入SSDLC，學校應盡快對系統開發人員進行重點宣導(可引用教育機構資安驗證中心設計的簡報https://tinyurl.com/fyn7naud)。

一、**需求階段**，應符合下列檢核項目。

項次	檢核內容
8.3	資通系統**開發前**，設計安全性要求，包含**機敏資料存取、用戶登入資訊檢核、用戶輸入輸出之檢查過濾**等，且檢討執行情形？
7.22	針對**資訊之交換**，建立適當之交換程序及安全保護措施，以確保資訊之完整性及機密性？針對重要資料的交換過程，保存適當之監控紀錄？
7.16	資通系統**重要組態設定檔案**及其他**具保護需求**之資訊是否加密或其他適當方式儲存(如實體隔離、專用電腦作業環境、資料加密等)？針對系統與資料傳輸之**機密性與完整性**建立適當之防護措施？
7.17	使用**預設密碼**登入資通系統時，於**登入後**要求立即**變更**密碼，並**限制使用弱密碼**？
7.10	建立**電子資料**安全管理機制(含防疫個資)，包含**分級**規則(如機密性、敏感性及一般性等)、**存取權限、資料安全、人員管理及處理規範**等，且落實執行？
9.12	訂定應記錄之**特定資通系統事件**(如身分驗證失敗、存取資源失敗、重要行為、重要資料異動、功能錯誤及管理者行為等)、**日誌內容**、**記錄時間週期**及**留存政策**，且保留日誌**至少6個月**？
9.13	依日誌儲存需求，配置所需之**儲存容量**，並於日誌處理**失效時**採取**適當行動及提出告警**？
9.14	針對日誌進行**存取控管**，並有適當之**保護控制措施**？

依據教育部110年6月29日臺教資(四)字第1100085899號函，基於多起因管理不當導致**重大資通安全事件**進行相關**根因分析**，包含「弱密碼及身分驗證缺失」、「未落實安全軟體發展生命週期(SSDLC)相關要

求」、「重要資料庫未最小授權」、「人員未經適當資安教育訓練」、「學校資安規範適用範圍未包含重要資通系統」，應加強相關措施。如因管理不當導致資通安全事件，教育部將以不遮蔽方式做成宣導案例，也將列入專案實地稽核，並循相關機制提報懲處。

另外，依據教育部110年6月18日臺教資(四)字第1100068264C號函，執行教育部委外辦理或補助建置維運伺服器主機及應用系統網站者，遵守「**教育部委外辦理或補助建置維運伺服器主機及應用系統網站資通安全及個人資料保護管理要點**」規定。譬如用戶登入資訊檢核之通行密碼要求：最小密碼長度8碼、密碼最長使用期限180天、密碼最短使用期限1天、避免重複使用前三次變更之密碼、禁止共用帳號密碼。譬如存取權限相關要求：主機、系統遠端維護時，應於加密通道進行及限制來源IP，並建立監控機制。譬如資料安全相關要求：移除任何測試性服務、資料、功能、模組、埠口、帳號等影響正式上線安全性之項目，並關閉有關作業系統、應用程式、開發套件及軟硬體版本資訊等相關錯誤訊息頁面，並確保已更新至最新版本。譬如人員管理相關要求：應用系統伺服器上之應用程式不得賦予資料庫及作業系統最高權限帳號，應給予最小需用權限，以免惡意人員透過資料庫管理系統破壞內部資訊作業。譬如處理規範相關要求：伺服主機應安裝主機型防火牆、防毒軟體、以及定期或不定期進行主機弱點掃描。

二、**設計階段**，應符合下列檢核項目。

項次	檢核內容
8.4	資通系統**設計階段**，依系統功能及要求，識別可能影響系統之**威脅**，進行**風險**分析及評估？

三、**開發階段**，應符合下列檢核項目。

項次	檢核內容
8.5	資通系統開發階段，避免**常見漏洞**(如OWASP Top 10等)？且針對防護需求等級**高**者，執行**源碼掃描**安全檢測？

四、**測試階段**，應符合下列檢核項目。

項次	檢核內容
8.6	資通系統測試階段，執行**弱點掃描**安全檢測？且針對防護需求等級**高**者，執行**滲透測試**安全檢測？

五、**部署階段**，應符合下列檢核項目。

項次	檢核內容
8.7	資通系統上線或更版前，執行**安全性要求測試**，包含**邏輯及安全性驗測、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**等，且檢討執行情形？
8.12	針對資通系統使用之**外部元件或軟體**，注意其安全漏洞通告且**定期評估**更新？
7.11	建立**網路服務安全控制措施**且定期檢討？定期檢測網路運作環境之安全漏洞？
7.12	設定防火牆並**定期檢視防火牆規則**，有效掌握與管理防火牆連線部署？

六、**跨階段措施**，應符合下列檢核項目。

項次	檢核內容
8.9	將開發、測試及正式作業環境**區隔**，不同作業環境建立適當之資安保護措施？
8.11	測試如使用正式作業環境之**測試資料**，建立保護措施且留存相關作業**記錄**？
8.10	儲存及管理資通系統發展**相關文件**？儲存方式及管理方式為何？

以上是「資通安全責任等級分級辦法」附表十「資通系統防護基準」要求落實「安全系統發展生命週期(SSDLC)」的檢核項目，系統發展過程的需求、設計、開發、測試、部署維運等每個階段都應該納入必要的安全項目考量。但是，這些只能算是SSDLC原則，如何才能更具體執行呢？基於行政院版檢核表「8.1自行或委外開發資通系統完成系統分級，且依資通系統防護基準執行控制措施？」之要求，既然「資通系統防護基準」是各機關自行或委外開發之資通系統應執行的控制措施，所有項目都必然應納入SSDLC的檢核項目，只要將防護基準所有項目一一釐清應該哪些階段進行探討，其實就是一種SSDLC的做法。教育機構資安驗證中心依據上述精神設計出「**SSDLC檢核表**」(https://sites.google.com/email.nchu.edu.tw/ssdlc)，提供各界可依循的SSDLC執行方案，其中也納入技服中心發布的「資通系統委外開發RFP」裡面有關於防護基準每個項目的實作指引，有助於系統開發人員知道具體的處理邏輯。

最後，**系統開發人員的資安管理作為與執行成效**，應反映於下列資安治理成熟度題項，由學校資安管理專責單位記錄保存相關佐證資料可供查核。

資安治理成熟度題項	現階段應推動執行重點
第38題.執行資通系統開發之安全需求設計	達到成熟度2之條件是「資通系統**開發前(進行)**，設計安全性要求(至少包含機敏資料存取、用戶登入資訊檢核及用戶輸入輸出之檢查過濾等)，針對資通系統開發前之安全性要求(如檢視系統開發安全性要求之妥適性等)有管理做法或機制，並檢討執行情形。」
第39題.執行資通系統開發之安全性測試	達到成熟度2之條件是「**上線前**執行安全性測試(至少包含弱點掃描，若為高等級之資通系統則需執行源碼掃描與滲透測試等)，針對上線前之安全性測試(如檢視系統測試方式，經主管複核試結果等)有管理做法或機制，並檢討執行情形。」
第40題.執行源碼安全管理	達到成熟度2之條件是「執行資通系統源碼安全措施(至少包含**源碼存取控制與版本控管**等)，針對資通系統源碼安全措施(如定期檢視版本控管情形與管理資通系統源碼存取權限等)有管理做法或機制，並檢討執行情形。」
第41題.區隔系統開發、測試及實作的環境與設備	達到成熟度2之條件是「**正式**作業環境已與其他(如辦公室、開發測試環境等)進行邏輯或實體區隔。除正式作業環境已區隔外，**開發**、**測試**亦進行部分邏輯或實體區隔。」
第34題.執行網站安全弱點檢測	達到成熟度2之條件是「**全部核心資通系統**依規定週期辦理網站安全弱點檢測，並檢討執行情形。」
第35題.執行系統滲透測試	達到成熟度2之條件是「**全部核心資通系統**依規定週期辦理系統滲透測試，並檢討執行情形。」

🔔【落實稽核工作】之建議

一、**內部稽核**，應符合下列檢核項目。

項次	檢核內容
6.3	訂定**內部資通安全稽核計畫**，包含稽核目標、範圍、時間、程序、人員等，且落實執行？ (A級機關：每年2次；B級機關：每年1次；C級機關：每2年1次)
6.3.1	依「國立大專校院資通安全維護作業指引」，學校辦理內部資通安全稽核，**稽核範圍應包含全校各單位**。各校得就資通系統(保有個人資料)風險高低、教學單位特性評估訂定推動先後順序，**分年分階段**規劃辦理，並明訂於各校資通安全維護計畫。
6.4	規劃及執行稽核發現事項**改善措施**，且定期追蹤改善情形？

二、**完成ISMS導入及通過第三方驗證**，應符合下列檢核項目。

項次	檢核內容
1.2	將**全部核心資通系統**納入資訊安全管理系統(ISMS)適用範圍？(A、B級機關：全部核心資通系統2年內完成ISMS導入，3年內通過公正第三方驗證，第三方核發之驗證證書應有TAF認證標誌；C級機關：全部核心資通系統2年內完成ISMS導入)
6.1	訂定、修正及實施機關**資通安全維護計畫**，且**每年**向上級或監督/主管機關提出資通安全維護計畫實施情形？
6.2	落實管理階層(如機關首長、資通安全長等)**定期(每年至少1次)**審查ISMS，以確保其運作之適切性及有效性？

三、依資通安全管理法第13條第1項規定，公務機關應**稽核**其所屬或監督機關之資通安全維護計畫實施情形。**教育部為落實前述法令規定**，每年自所屬公務機關及所管特定非公務機關擇定受稽核對象，查核其資通安全管理法及其子法相關法遵事項符合情形與資通安全維護計畫實施情形。**受稽機關配合事項**，在接獲通知後2週內填復「資通安全實地稽核項目檢核表」、「受稽機關現況調查表」、「技術檢測基本資料調查表」、「核心資通系統調查表」，並提供機關最新版之資通安全維護計畫。

教育機構資安驗證中心依據原先的紙本表單，另外設計出電子表單，提供各界更容易落實的**自評工具**，便於填報人員溝通協作、編輯修正

(https://sites.google.com/email.nchu.edu.tw/toolsisms/)。建議先從核心資通系統開始進行，再陸續擴展要求非核心資通系統，這樣可以讓學校資安專責單位時時掌握各資通系統的防護基準狀況，也能預評是否都能達成稽核項目要求，以及隨時掌握資安健診涵蓋面的相關安全狀況，這些自評工具可以成為各校的資安管理日常，而非被教育部擇定為稽核對象才來著手準備，強化資安管控機制就可以降低安全風險。

- 「實地稽核[資通系統防護基準]自評」電子表單
  https://sites.google.com/email.nchu.edu.tw/isms-saq-1
  應由**每個核心資通系統的管理員**負責填答，這個表單納入「教育部資通安全稽核計畫」附件4「核心資通系統調查表」，以及「資通安全責任等級分級辦法」附表十「資通系統防護基準」所列7大構面控制措施，做為資通系統防護基準自評及檢核用途。

- 「實地稽核[資通安全稽核項目]自評」電子表單
  https://sites.google.com/email.nchu.edu.tw/isms-saq-1
  應由**資安專責人員**負責填答，這個表單納入「教育部資通安全稽核計畫」附件1「資通安全實地稽核項目檢核表」所列9大構面稽核項目，做為資安管理自評及檢核用途。

- 「技術檢核[比照資安健診涵蓋面]所需資料調查」電子表單
  https://sites.google.com/email.nchu.edu.tw/isms-saq-2
  這部分有四個表單，應該是分別由單位內**負責使用者電腦安全、GCB組態設定、目錄伺服器安全、網路惡意活動檢視等工作的同仁**進行填答，這些表單納入「教育部資通安全稽核計畫」附件3「技術檢測基本資料調查表」所涵蓋資安健診的四類項目資料，做為技術檢核前被要求提供資料之調查與自評用途。

- 「技術檢核["網路架構"及"物聯網"檢測]所需資料調查」電子表格
  https://sites.google.com/email.nchu.edu.tw/isms-saq-2
  由於"網路架構"及"物聯網"檢測所需資料調查不容易以表單方式進行，這部份的資料直接編輯試算表內容較為方便。這部分要填報的資料包含**各類服務主機資訊、防護主機資訊、核心網路設備資訊、線路資訊、網段資訊、使用者電腦網段配置、物聯網設備資訊**，應該是邀請**各業務負責人**來共同編輯，做為技術檢核前被要求提供資料之調查與自評用途。

最後，**落實稽核工作的執行成效**，應反映於下列資安治理成熟度題項，由學校資安管理專責單位記錄保存相關佐證資料可供查核。

資安治理成熟度題項	現階段應推動執行重點
第9題.執行資安內部稽核	達到成熟度2之條件是「A級機關**每年2次**資安內稽，B級機關**每年1次**資安內稽，C級機關**每2年1次**資安內稽，並檢討執行情形。」
第10題.落實資安管理制度(ISMS)驗證	達到成熟度3之條件是「**全部核心資通系統**完成ISMS導入，並**通過ISMS第三方驗證**。」(A、B級機關全部核心資通系統2年內完成ISMS導入，3年內通過公正第三方驗證；C級機關全部核心資通系統2年內完成ISMS導入。) 教育部資科司已於108年9月3日函文核定國立大專校院等級，所以也就是110年9月2日前必須完成ISMS導入，而A、B級機關必須在**111年9月2日**前通過公正第三方驗證。尚未通過驗證者，至少要完成單位的ISMS四階文件制定，做為佐證。而通過驗證者，提出佐證的證書上面所列的驗證範圍應包含**全部核心資通系統**(核心資通系統應包含：支持核心業務持續運作必要之系統、防護需求等級為高者之資通系統)。 注意:「教育體系資通安全暨個人資料管理規範」雖為教育部自行發展之標準，具ISO 27001架構與精神，但未獲主管機關認可(未能取得TAF認證)，僅可做為**C級以下導入參考架構**，無法做為B級以上的第三方驗證。

🔔【落實資安法令與規範】之建議

最後提醒，應隨時關注我國資通安全相關政策、法令及規範(可參考教育機構資安驗證中心整理的心智圖https://tinyurl.com/6u7fvdc7)，做好相關因應措施，並定期檢討執行情形(如定期檢討資安法令與規範之盤點、執行及後續規範修正作業等)。資通安全長應隨時掌握瞭解近期教育體系重大資通安全政策(如國立大專校院資通安全維護作業指引、全國大專校院資安長會議相關指示等)，並督導協助相關事宜。