［回目錄］

國立屏東大學第二期高等教育深耕計畫-資安專章附件

本文件以未來 5 年各項績效指標為主要項目，提供各指標本校相關佐證文件資料。為方便委員閱覽，本文件設有超連結，目錄頁可點擊各績效項目，即跳轉至該項目，而每頁右上角均有**[回目錄]**之超連結按鈕。因篇幅關係，佐證資料將擷取部分內容，如委員須進一步參考細部資料，歡迎來電或來信。

國立屏東大學計算機與網路中心 敬啟

yuen@mail.nptu.edu.tw
08-7663800 #21302~21300

目錄

［回目錄］

A1 全校導入資訊安全管理系統（ISMS）

A1.K1 資通安全長之配置

資安長之配置：本校資訊安全管理要點(如下圖)明定由副校長擔任資安長。

國立屏東大學資訊安全管理要點

103 年 10 月 23 日本校第 2 次行政會議通過

一、為強化本校資訊安全管理，建立安全及可信賴之電子化系統，確保資料、系統、設備及網路之安全，特依行政院及所屬各機關資訊安全管理要點，訂定本要點。

二、本校有關資訊安全管理事務依下列分工原則：

(一)資訊安全政策、計畫及技術規範之研議、建置及評估等事項，由計算機與網路中心負責辦理。

(二)資料及資訊系統之安全需求研議、使用管理及維護等事項，由業務單位負責辦理。

(三)資訊機密維護及稽核使用管理事項，由秘書室會同相關單位負責辦理。

三、本校由副校長擔任資訊安全長，負責資訊安全管理事項之協調及推動，並由計算機與網路中心主任擔任執行秘書，以協助有關業務之推動。

四、資訊安全應定期或不定期進行稽核。

五、各單位對資訊相關職務及工作，應進行安全評估，並於人員進用、工作及任務指派時，審慎評估人員之適任性，並進行必要之考核；各單位對可存取機密性或敏感性資訊或系統之人員，及因工作需要須配賦系統存取特別權限之人員，應加強評估及考核。

六、各單位應加強資訊安全人力之培訓，提升資訊安全管理能力，若資訊安全人力或經驗如有不足，得洽請計算機與網路中心提供服務，必要時洽請學者專家或專業機關（構）提供顧問諮詢服務。

七、各單位負責重要資訊系統之管理、維護、設計及操作之人員，應妥適分工，分散權責，實施人員輪調，建立人力備援制度。

八、資訊作業相關人員離職時，應取消其進出識別證件，並確實做好電腦軟硬體及相關文件之移交工作。

九、各單位業務主管應負責督導所屬員工之資訊作業安全，防範不法及不當行為。

十、各單位辦理資訊業務委外作業時，應於事前研提資訊安全需求，明訂廠商之資訊安全責任及保密規定，並列入契約中，要求廠商遵守及定期考核，並派員監督。

十一、各單位對系統變更作業，應建立控管制度並建立紀錄備查。

十二、各單位使用軟體之權利及義務應依著作權法及有關議定之合約辦理。

十三、各單位應採行必要之事前預防及保護措施，偵測及防制電腦病毒及其他惡意軟體，確保系統正常運作。

十四、各單位利用公眾網路傳送資訊或進行交易處理，應遵守「臺灣學術網路管理規範」；並應評估可能之安全風險，確定資料傳輸具完整性、機密性、身分鑑別及不可否認性等安全需求。

十五、各單位應針對資料傳輸、撥接線路、網路線路與設備、對外連接介面及路由器等事項，研擬妥適安全控管措施。

［回目錄］

A1.K2 組織成員含跨全校各一級行政、學術單位，且每年至少開會 1 次

目前本校組織有**個人資料保護推動委員會**及**資安管理委員會**，現正規畫整合為**資通安全暨個人資料保護推動委員會**。

1.**個人資料保護推動委員會**：依本校個人資料保護管理要點(如下圖)，個人資料保護管理推動委員會成員，由各一級行政學術單位主管組成，每學年開會一次。

國立屏東大學個人資料保護管理要點

104 年 1 月 8 日本校第 5 次行政會議審議通過
104 年 11 月 12 日本校第 13 次行政會議修正通過

一、本校為落實個人資料之保護及管理，促進個人資料之合理利用，依據個人資料保護法及相關法令規定，特設個人資料保護推動委員會(以下簡稱本委員會)，並訂定本要點。

二、本要點名詞定義如下：

（一）個人資料：指自然人之姓名、出生年月日、國民身分證統一編號、護照號碼、特徵、指紋、婚姻、家庭、教育、職業、病歷、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方式識別該個人之資料。

（二）個人資料檔案：指依系統建立而得以自動化機器或其他非自動化方式檢索、整理之個人資料之集合。

三、本委員會任務如下：

（一）本校個人資料保護政策之擬議。

（二）本校個人資料管理制度之推展。

（三）本校個人資料隱私風險之評估及管理。

（四）本校個人資料保護意識提升及教育訓練計畫之擬議。

（五）本校個人資料管理制度基礎設施之評估。

（六）本校個人資料管理制度適法性與合宜性之檢視、審議及評估。

（七）其他本校個人資料保護、管理之規劃及執行事項。

四、本委員會以副校長、主任秘書、教務長、學生事務長、總務長、研發長、國際事務長、實習就業輔導處長、圖書館館長、人事室主任、主計室主任、計算機與網路中心主任及各學院院長共同組成，並以副校長為召集人，計算機與網路中心主任為執行秘書。

五、本委員會每學年開會一次，必要時得召開臨時會議，開會時得邀請相關人員列席。

六、本委員會設置個資保護稽核小組，負責個人資料保護稽核事宜，由召集人指派一名委員擔任稽核小組召集人，小組成員應接受個人資料保護稽核之相關教育訓練。

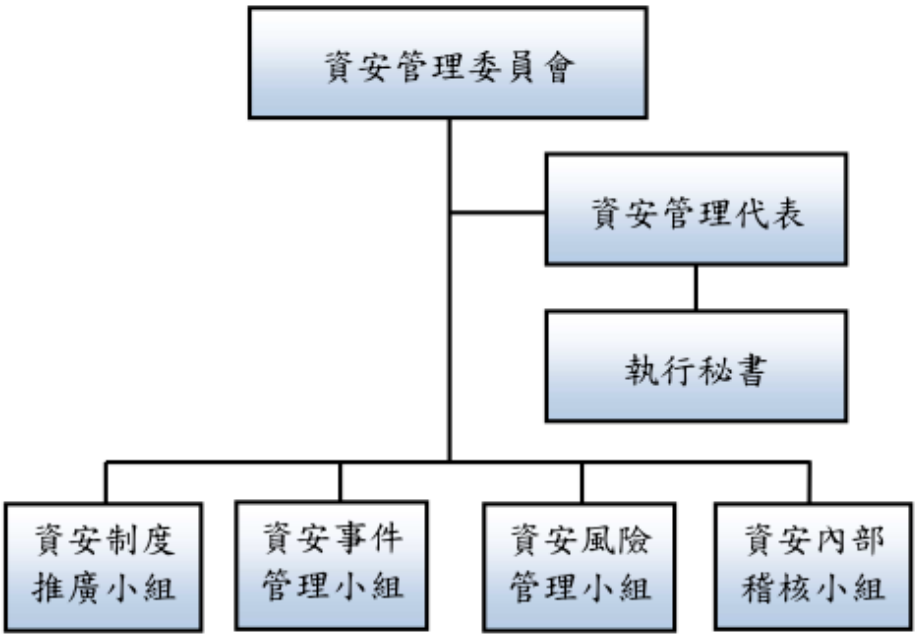
［回目錄］

2.**資安管理委員會**：依本校 ISMS-3-001 資訊安全組織章程(如下圖)，資安管理委員會設置資安制度推廣、資安事件管理、資安風險管理及資安內部稽核等 4 小組。委員會成員以副校長、教務長、學生事務長、總務長、研發長、圖書館館長及計算機與網路中心主任為當然委員。每年應召開一次管理審查會議。

國立屏東大學

名稱	資訊安全組織章程	安全等級	限閱
編號	ISMS-3-001	版次	1.2

5.1 ISMS 維運組織架構



5.1.1 資安管理委員會

本委員會以副校長、教務長、學生事務長、總務長、研發長、圖書館館長及計算機與網路中心主任為當然委員，並以副校長為召集人(資通安全長)。

…

5.4 管理審查會議

5.4.1 資安管理委員會每年應召開一次「管理審查會議」，必要時得召開臨時會議。

[回目錄]

111 年度資安管理委員會於 111 年 8 月 31 日召開，會議簽到表如下圖。

國立屏東大學 111 年度第 1 次資安管理委員會會議簽到表

時間：中華民國 111 年 8 月 31 日(星期三)下午 2 時 0 分

地點：本校民生校區五育樓 4 樓第四會議室

主席 ：劉副校長英偉　　紀錄 ：魏佑恩

出(列)席人員如下：

序號	單　位	職 稱	姓 名	簽　到
1	副校長室	副校長	劉英偉	
2	教務處	教務長	歐陽彥晶	
3	學生事務處	學務長	黃鐘慶	
4	總務處	總務長	李東泰	
5	研究發展處	研發長	許華書	
6	圖書館	館長	王慧蘭	
7	計算機與網路中心	主任	許良政	
列席人員：				
[redacted]顧問有限公司				
1	[redacted]	ISMS 輔導顧問	[redacted]	

[回目錄]

3. **資通安全暨個人資料保護推動委員會**(以下簡稱本委員會)，本委員會組織成員含跨全校各一級行政、學術單位主管，由副校長擔任資通安全長，負責資安管理事項之協調及推動，由計算機與網路中心主任擔任執行秘書；本委員會每年至少召開會議1次。下圖為本校**資通安全暨個人資料保護管理要點草案**。

國立屏東大學資通安全暨個人資料保護管理要點草案

年　月　日本校第　次行政會議審議通過

一、本校為推動資通安全管理並落實個人資料保護及管理，促進個人資料之合理利用，依據資通安全管理法、個人資料保護法等相關規定，訂定本要點（以下簡稱本要點）。

二、為落實資通安全暨個人資料保護管理，應成立資通安全暨個人資料保護推動委員會(以下簡稱本委員會)。本委員會以行政副校長、主任秘書、教務長、學生事務長、總務長、研發長、國際事務長、實習就業輔導處長、圖書館館長、人事室主任、主計室主任、計算機與網路中心主任、體育室主任、師資培育中心主任及各學院院長共同組成，並以行政副校長(資通安全長)為召集人，計算機與網路中心主任為執行秘書。

三、本委員會任務如下：

（一）本校資通安全及個人資料保護政策與制度之審議。

（二）本校資通安全及個人資料保護風險管理作業督導。

（三）本校資通安全及個人資料保護管理資源協調與流程改善。

（四）處理本校資通安全及個人資料保護重大緊急事件。

（五）本校資通安全及個人資料管理制度適法性與合宜性之檢視、審議及評估。

（六）其他本校資通安全及個人資料保護管理之規劃及執行事項。

四、本委員會每學年開會一次，必要時得召開臨時會議，開會時得邀請相關人員列席。

[回目錄]

A1.K3 每年辦理全校資通系統盤點

本校每年依規定調查盤點全校資通系統與服務資產，各資通系統業管單位依防護需求分級原則，填寫**系統等級分級評估表**、**資通系統防護基準檢查表**，相關資料彙整全校**資通系統與服務資產清冊**，並至行政院資通安全管考系統提報。

1.**資通系統與服務資產清冊：**以下為 111 年度提報內容(部分內容遮蔽)

國立屏東大學資通系統與服務資產清冊					機關等級：C級										
系統名稱(必填)	建置方式(必填)	系統管理者(部門/單位)(必填)	系統使用者(部門/單位)(必填)	主機設置於機關內(是/否)(必填)	核心系統(是/否)(必填)	含機敏資訊(是/否/其他機關維運)(必填) 註：系統建置方式為「主管/上級/其他機關」者請填「其他機關維運」	機敏資訊以非明文方式儲存(是/否/無機敏資訊/其他機關維運)	機敏資訊類別註：「無機敏資訊」及「其他機關維運」者免填)	防護需求等級(普/中/高/套裝軟體/其他機關維運)(必填)	是否包含於ISMS導入範圍(是/否/其他機關維運)(必填) 註：系統建置方式為「主管/上級/其他機關」者請填「其他機關維運」	最大可容忍中斷時間(單位：工作小時	是否符合防護基準(必填) 註：「不適用」僅適用於「由上級、主管或其他機關提供之系統」或「套裝軟體」	不符合防護基準項目代碼 註：「是否符合防護基準」為「部分符合」及「不符合」者為必填，項目代碼參附件7-3，多項請以「/」隔開	系統日誌保存時間是否超過6個月(是/否/其他機關維運)(必填) 註：系統建置方式為「主管/上級/其他機關」者請填「其他機關維運」
選課系統	本機關自行開發	教務處課務組	教務處課務組	是											
學籍資訊系統	本機關自行開發	教務處註冊組	教務處註冊組	是											
成績資訊系統	本機關自行開發	教務處註冊組	教務處註冊組	是											
卡務系統	本機關委外開發	教務處註冊組	教務處註冊組	是											
畢業離校資訊系統	本機關自行開發	教務處註冊組	教務處註冊組	是											
招生資訊系統	本機關自行開發	教務處綜合業務組	教務處綜合業務組、專案業務組、幼兒教育學系	是											
數位學習平台系統	本機關委外開發	教務處教學發展組	教務處教學發展組	是											
授課預警系統	本機關自行開發	教務處教學發展組	教務處教學發展組	是											
教學評量系統	本機關自行開發	教務處教學發展組	教務處教學發展組	是											
導師系統	本機關自行開發	學生事務處	學生事務處及各院所系	是											
就學貸款資訊系統	本機關自行開發	學務處生輔組	學務處生輔組	是											
學生宿舍門禁系統(4組)	本機關購置套裝軟體	學務處生輔組	學務處生輔組	是											

[回目錄]

國立屏東大學資通系統與服務資產清冊　機關等級：C級　彙整日期：111 年 4 月 14 日

系統名稱(必填)	建置方式(必填)	系統管理者(部門/單位)(必填)	系統使用者(部門/單位)(必填)	主機設置於機關內(是/否)(必填)	核心系統(是/否)(必填)	含機敏資訊(是/否/其他機關維運)(必填) 註：系統建置方式為「主管/上級/其他機關」者請填「其他機關維運」	機敏資訊以非明文方式儲存(是/否/無機敏資訊/其他機關維運)	機敏資訊類別註：「無機敏資訊」及「其他機關維運」者免填)	防護需求等級(普/中/高/套裝軟體/其他機關維運)(必填)	是否包含於ISMS導入範圍(是/否/其他機關維運)(必填) 註：系統建置方式為「主管/上級/其他機關」者請填「其他機關維運」	最大可容忍中斷時間(單位：工作小時	是否符合防護基準(必填) 註：「不適用」僅適用於「由上級、主管或其他機關提供之系統」或「套裝軟體」	不符合防護基準項目代碼 註：「是否符合防護基準」為「部分符合」及「不符合」者為必填，項目代碼參附件7-3，多項請以「/」隔開	系統日誌保存時間是否超過6個月(是/否/其他機關維運)(必填) 註：系統建置方式為「主管/上級/其他機關」者請填「其他機關維運」
學生宿舍監視系統(29組)	本機關購置套裝軟體	學務處生輔組	學務處生輔組	是										
校務行政系統B37學生健康管理系統	本機關自行開發	學務處衛生保健組	學務處衛生保健組	是										
校園傷病服務系統	本機關購置套裝軟體	學務處衛生保健組	學務處衛生保健組	是										
健康促進服務系統	本機關購置套裝軟體	學務處衛生保健組	學務處衛生保健組	否										
諮商輔導服務e化系統	本機關委外開發	學生諮商中心	學生諮商中心	是										
電子公文線上簽核系統	本機關委外開發	總務處文書組	總務處文書組	是										
校園監視系統	本機關購置套裝軟體	總務處事務組	總務處事務組	是										
薪資暨所得稅管理查詢資訊系統	本機關委外開發	總務處出納組	總務處出納組	是										
出納及零用金管理系統	本機關租用服務	總務處出納組	總務處出納組	是										
財產管理系統	本機關委外開發	總務處保管組	總務處保管組	是										
空間管理系統	本機關自行開發	總務處保管組	總務處保管組	是										
意見溝通平臺系統	本機關自行開發	秘書室	秘書室	是										
教師評鑑管理系統	本機關自行開發	秘書室校務研究與發展中心	秘書室校務研究與發展中心	是										

國立屏東大學資通系統與服務資產清冊　機關等級：C級　彙整日期：111 年 4 月 14 日

系統名稱(必填)	建置方式(必填)	系統管理者(部門/單位)(必填)	系統使用者(部門/單位)(必填)	主機設置於機關內(是/否)(必填)	核心系統(是/否)(必填)	含機敏資訊(是/否/其他機關維運)(必填) 註：系統建置方式為「主管/上級/其他機關」者請填「其他機關維運」	機敏資訊以非明文方式儲存(是/否/無機敏資訊/其他機關維運)	機敏資訊類別註：「無機敏資訊」及「其他機關維運」者免填)	防護需求等級(普/中/高/套裝軟體/其他機關維運)(必填)	是否包含於ISMS導入範圍(是/否/其他機關維運)(必填) 註：系統建置方式為「主管/上級/其他機關」者請填「其他機關維運」	最大可容忍中斷時間(單位：工作小時	是否符合防護基準(必填) 註：「不適用」僅適用於「由上級、主管或其他機關提供之系統」或「套裝軟體」	不符合防護基準項目代碼 註：「是否符合防護基準」為「部分符合」及「不符合」者為必填，項目代碼參附件7-3，多項請以「/」隔開	系統日誌保存時間是否超過6個月(是/否/其他機關維運)(必填) 註：系統建置方式為「主管/上級/其他機關」者請填「其他機關維運」
教師履歷管理系統	本機關自行開發	秘書室校務研究與發展中心	秘書室校務研究與發展中心	是										
產學合作管理系統	本機關自行開發	研發處技合組	全校教職員	是										
僑生及港澳生招生系統	本機關自行開發	國際處國際學生組	國際處國際學生組	是										
選送赴海外教育見實習平台	本機關自行開發	國際事務處/計算機中心	全國師培大學	是										
圖書館網頁系統	本機關自行開發	期刊資訊組	圖書館	是										
圖書館自動化系統	本機關委外開發	期刊資訊組	圖書館	否										
圖書館門禁安全系統	本機關購置套裝軟體	典閱組	典閱組	是										
應屆畢業生流向調查系統	本機關自行開發	職涯發展與輔導組	職涯發展與輔導組	是										
畢業後流向調查系統	本機關自行開發	職涯發展與輔導組	職涯發展與輔導組	是										
學生校外實習系統	本機關自行開發	職涯發展與輔導組	職涯發展與輔導組	是										
學生證照管理系統	本機關自行開發	職涯發展與輔導組	職涯發展與輔導組	是										
證照獎勵管理系統	本機關自行開發	職涯發展與輔導組	職涯發展與輔導組	是										
校友資訊系統	本機關自行開發	校友服務組	校友服務組	是										

[回目錄]

國立屏東大學資通系統與服務資產清冊				機關等級：C級		彙整日期：111 年 4 月 14 日								
系統名稱(必填)	建置方式(必填)	系統管理者(部門/單位)(必填)	系統使用者(部門/單位)(必填)	主機設置於機關內(是/否)(必填)	核心系統(是/否)(必填)	含機敏資訊(是/否/其他機關維運)(必填) 註：系統建置方式為「主管/上級/其他機關」者請填「其他機關維運」	機敏資訊以非明文方式儲存(是/否/無機敏資訊/其他機關維運)	機敏資訊類別註：「無機敏資訊」及「其他機關維運」者免填	防護需求等級(普/中/高/套裝軟體/其他機關維運)(必填)	是否包含於ISMS導入範圍(是/否/其他機關維運)(必填) 註：系統建置方式為「主管/上級/其他機關」者請填「其他機關維運」	最大可容忍中斷時間(單位：工作小時	是否符合防護基準(必填) 註：「不適用」僅適用於「由上級、主管或其他機關提供之系統」或「套裝軟體」	不符合防護基準項目代碼 註：「是否符合防護基準」為「部分符合」及「不符合」者為必填，項目代碼參附件7-3，多項請以「/」隔開	系統日誌保存時間是否超過6個月(是/否/其他機關維運)(必填) 註：系統建置方式為「主管/上級/其他機關」者請填「其他機關維運」
活動報名系統	本機關自行開發	計網中心系統組	全校各學術行政單位	是										
行動屏大App	本機關委外開發	計網中心系統組	計算機與網路中心系統組	是										
教職員工電子郵件主機系統	本機關購置套裝軟體	計網中心網路組	全校教職員工	是										
教職員個人網站空間系統	本機關自行開發	計網中心網路組	計網中心網路組	是										
電子郵件公告系統	本機關自行開發	計網中心網路組	全校職員	是										
學生網路郵局系統	本機關購置套裝軟體	計網中心網路組	全校學生	是										
主機房門禁系統	本機關購置套裝軟體	計算機與網路中心	計算機與網路中心	是										
主機房監視系統	本機關購置套裝軟體	計算機與網路中心	計算機與網路中心	是										
會計帳務資訊管理系統	本機關租用服務	主計室	主計室	是										
網路請購查詢系統	本機關租用服務	主計室	主計室	是										
人力資源系統	本機關自行開發	人事室	人事室	是										
人事差勤系統	主管/上級/其他機關提供	人事室	人事室	是										
保費整合管理系統	本機關租用服務	人事室	人事室	是										
財金專業教室監視系統	本機關購置套裝軟體	財務金融學系	財務金融學系	是										

[回目錄]

2. **系統分級評估表：**因篇幅有限，以下擷取教務處「選課系統」、學務處「學生宿舍門禁系統」、總務處「電子公文線上簽核系統」為例。

「選課系統」資通系統分級評估表

表單編號：　　日期：_111_年__03__月_30_日

系統網址：	IP：
軟體財產編號：	
系統建置方式：✓自行開發 □自行委外 □其他	系統屬性：✓業務 □行政
系統建置廠商：	系統維運廠商：
系統管理者(部門)：教務處課務組	系統使用者(部門)：教務處課務組
核心系統/非核心系統：✓ Y □ N(註1)	是否含機敏資料：□ Y ✓N
最大可容忍中斷時間：_ 備註：8小時為1工作天	
本資產是否含有大陸元件：□ Y ✓ N 註：「系統建置方式」為「主管/上級機關提供」得免填	
業務內容(功能)說明： 課程規劃管理、開排課作業、學生選課作業、課程地圖雷達圖(含核心能力及指標)、扣考作業、課務基本資料設定	

註1：核心系統-資通安全管理法施行細則第七條（參閱附件3核心系統定義）

影響構面				資通系統分級（影響構面最高者）
機密性	完整性	可用性	法律遵循性	
普	中	中	普	中

影響構面	防護需求等級		影響說明
機密性	初估	普	本系統主要為學生選課資訊，發生資通安全事件可能造成資料外洩，對學校及學生將產生有限之影響。
完整性	初估	中	發生資通安全事件，可能造成選課資訊錯誤或遭竄改等情事，對學校及學生將產生嚴重之影響。
可用性	初估	中	選課期間若發生系統中斷，將嚴重影響學生選課權益。
法律遵循性	初估	普	本系統主為提供學生選課相關管理服務，遵循校內規範，無法律直接規範。

備註：防護需求等級分為「高」、「中」、「普」三級。

承辦人	二級單位主管	一級單位主管

[回目錄]

「學生宿舍門禁系統系統」資通系統分級評估表

表單編號：　　日期：111 年 03 月 25 日

系統網址：	IP：
軟體財產編號：	
系統建置方式：□自行開發 □自行委外 ■其他	系統屬性：□業務 ■行政
系統建置廠商：	系統維運廠商：
系統管理者(部門)：學務處生輔組	系統使用者(部門)：學務處生輔組
核心系統/非核心系統：□ Y ■ N(註 1)	是否含機敏資料：□ Y ■ N
最大可容忍中斷時間：	
本資產是否含有大陸元件：□ Y ■ N　註：「系統建置方式」為「主管/上級機關提供」得免填	
業務內容(功能)說明：屏商校區學生第二宿舍門禁系統	

註 1：核心系統-資通安全管理法施行細則第七條（參閱附件 3 核心系統定義）

影響構面				資通系統分級（影響構面最高者）
機密性	完整性	可用性	法律遵循性	
普	普	普	普	普

影響構面	防護需求等級		影響說明
機密性	初估	普	學生資料若發生資通安全事件，可能造成未經授權之資訊揭露，對學校之營運、信譽及學生權益等方面將產生影響。
完整性	初估	普	發生資通安全事件，可能造成資訊錯誤或遭竄改等情事，對機關之營運、信譽及學生權益等方面將產生影響。
可用性	初估	普	發生資通安全事件，可能造成系統之存取或使用之中斷，對機關之營運、信譽等方面將產生影響。
法律遵循性	初估	普	本系統含大量學生進出入人員影像，應遵個人資料保護法及相關規定，若發生發生資通安全事件，可能影響他人合法權益或機關執行業務之公正性及正當性，並使機關或其所屬人員受行政罰、懲戒或懲處。

備註：防護需求等級分為「高」、「中」、「普」三級。

承辦人	二級單位主管	一級單位主管
		111. 3. 28

[回目錄]

「電子公文線上簽核系統」資通系統分級評估表

表單編號：　　日期：111 年 03 月 28 日

系統網址：	IP：
軟體財產編號：	
系統建置方式：□自行開發 ■自行委外 □其他	系統屬性：□業務 ■行政
系統建置廠商：	系統維運廠商：
系統管理者(部門)：總務處文書組	系統使用者(部門)：總務處文書組
核心系統/非核心系統：□ Y ■ N(註 1)	是否含機敏資料：□ Y ■ N
最大可容忍中斷時間： 備註：8 小時為 1 工作天	
本資產是否含有大陸元件：□ Y■N　註：「系統建置方式」為「主管/上級機關提供」得免填	
業務內容(功能)說明：電子公文線上簽核、收發文管理、檔案管理、檔案借閱、公文稽催、郵件交寄管理等。	

註 1：核心系統-資通安全管理法施行細則第七條（參閱附件 3 核心系統定義）

影響構面				資通系統分級（影響構面最高者）
機密性	完整性	可用性	法律遵循性	
普	普	普	普	普

影響構面	防護需求等級		影響說明
機密性	初估	普	本系統為內部行政作業資料，機密及訴訟公文採紙本簽核，若系統資料外洩或遭竄改將造成學校業務輕微傷害。
完整性	初估	普	本系統目的在提供學校內部公文簽核、收發文作業、檔案管理、公文稽催、郵件交寄管理等服務，為學校行政作業之基本系統軟體之一。
可用性	初估	普	本系統服務中斷可能導致學校行政業務效能受到輕微影響。
法律遵循性	初估	普	本系統包含個人以及業務資料，依「個人資料保護法」規定辦理。系統內個人資料部分僅有姓名、服務單位、身分證字號及個人電子郵件帳號，不致影響個人權益；業務資料部分，機密及訴訟公文採紙本簽核，影響有限。

備註：防護需求等級分為「高」、「中」、「普」三級。

承辦人	二級單位主管	一級單位主管

[回目錄]

3. **資通系統防護基準檢查表：**以下以「卡務系統(安全等級普)」、「諮商輔導服務ｅ化系統(安全等級中)」為例。

版本號：1100823（修訂部分以紅字標示）

資通系統防護基準檢查表

系統名稱：卡務系統

安全等級：普

檢查日期： 111 年 3 月 24 日

檢查內容	檢查結果		備註
	符合	不符合	（若不符合，請加以說明）
一、存取控制			
(一) 帳號管理			
1. 建立帳號管理機制，包含帳號之申請、建立、修改、啟用、停用及刪除之程序	V		
(二) 最小權限			
(三) 遠端存取			
1. 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	V		
2. 使用者之權限檢查作業應於伺服器端完成	V		
3. 應監控遠端存取機關內部網段或資通系統後臺之連線	V		
4. 應採用加密機制	V		
二、事件日誌與可歸責性			
(一) 記錄事件			
1. 訂定日誌之記錄時間週期及留存政策，並保留日誌至少六個月	V		
2. 確保資通系統有記錄特定事件之功能，並決定應記錄之特定資通系統事件	V		
3. 應記錄資通系統管理者帳號所執行之各項功能	V		
(二) 日誌紀錄內容			
1. 資通系統產生之日誌應包含事件類型、發生時間、發生位置及任何與事件相關之使用者身分識別等資訊，採用單一日誌機制，確保輸出格式之一致性，並應依資通安全政策及法規要求納入其他相關資訊	V		
(三) 日誌儲存容量			
1. 依據日誌儲存需求，配置所需之儲存容量	V		
(四) 日誌處理失效之回應			
1. 資通系統於日誌處理失效時，應採取適當之行動	V		

版本號：1100823（修訂部分以紅字標示）

檢查內容	檢查結果		備註
	符合	不符合	（若不符合，請加以說明）
(一) 系統發展生命週期需求階段			
1. 針對系統安全需求（含機密性、可用性、完整性）進行確認	V		
(二) 系統發展生命週期設計階段			
(三) 系統發展生命週期開發階段			
1. 應針對安全需求實作必要控制措施	V		
2. 應注意避免軟體常見漏洞及實作必要控制措施	V		
3. 發生錯誤時，使用者頁面僅顯示簡短錯誤訊息及代碼，不包含詳細之錯誤訊息	V		
(四) 系統發展生命週期測試階段			
1. 執行「弱點掃描」安全檢測	V		計網中心協助檢測
(五) 系統發展生命週期部署與維運階段			
1. 於部署環境中應針對相關資通安全威脅，進行更新與修補，並關閉不必要服務及埠口	V		
2. 資通系統不使用預設密碼	V		
(六) 系統發展生命週期委外階段			
1. 資通系統開發如委外辦理，應將系統發展生命週期各階段依等級將安全需求（含機密性、可用性、完整性）納入委外契約	V		
(七) 獲得程序			
(八) 系統文件			
1. 應儲存與管理系統發展生命週期之相關文件	V		
六、系統與通訊保護			
(一) 傳輸之機密性與完整性			
(二) 資料儲存之安全			
七、系統與資訊完整性			
(一) 漏洞修復			
1. 系統之漏洞修復應測試有效性及潛在影響，並定期更新	V		
(二) 資通系統監控			
1. 發現資通系統有被入侵跡象時，應通報機關特定人員	V		
(三) 軟體及資訊完整性			

版本號：1100823（修訂部分以紅字標示）

檢查內容	檢查結果		備註
	符合	不符合	（若不符合，請加以說明）
檢查人員：		權責主管覆核：	

版本號：1100823（修訂部分以紅字標示）

資通系統防護基準檢查表

系統名稱：諮商輔導服務e化系統

安全等級：中

檢查日期：111 年 4 月 12 日

檢查內容	檢查結果		備註
	符合	不符合	（若不符合，請加以說明）
一、存取控制			
(一) 帳號管理			
1. 建立帳號管理機制，包含帳號之申請、建立、修改、啟用、停用及刪除之程序	✓		
2. 已逾期之臨時或緊急帳號應刪除或禁用	✓		
3. 資通系統閒置帳號應禁用	✓		
4. 定期審核資通系統帳號之申請、建立、修改、啟用、停用及刪除	✓		
(二) 最小權限			
1. 採最小權限原則，僅允許使用者（或代表使用者行為之程序）依機關任務及業務功能，完成指派任務所需之授權存取	✓		
(三) 遠端存取			
1. 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	✓		
2. 使用者之權限檢查作業應於伺服器端完成	✓		
3. 應監控遠端存取機關內部網段或資通系統後臺之連線	✓		
4. 應採用加密機制	✓		
5. 遠端存取之來源應為機關已預先定義及管理之存取控制點	✓		
二、事件日誌與可歸責性			
(一) 記錄事件			
1. 訂定日誌之記錄時間週期及留存政策，並保留日誌至少六個月	✓		
2. 確保資通系統有記錄特定事件之功能，並決定應記錄之特定資通系統事件	✓		
3. 應記錄資通系統管理者帳號所執行之各項功能	✓		
4. 應定期審查機關所保留資通系統產生之日誌	✓		
(二) 日誌紀錄內容			

版本號：1100823（修訂部分以紅字標示）

檢　查　內　容	檢查結果		備註
	符合	不符合	（若不符合，請加以說明）
1. 資通系統產生之日誌應包含事件類型、發生時間、發生位置及任何與事件相關之使用者身分識別等資訊，採用單一日誌機制，確保輸出格式之一致性，並應依資通安全政策及法規要求納入其他相關資訊	✓		
(三) 日誌儲存容量			
1. 依據日誌儲存需求，配置所需之儲存容量	✓		
(四) 日誌處理失效之回應			
1. 資通系統於日誌處理失效時，應採取適當之行動	✓		
(五) 時戳及校時			
1. 資通系統應使用系統內部時鐘產生日誌所需時戳，並可以對應到世界協調時間(UTC)或格林威治標準時間(GMT)	✓		
2. 系統內部時鐘應定期與基準時間源進行同步	✓		
(六) 日誌資訊之保護			
1. 對日誌之存取管理，僅限於有權限之使用者	✓		
2. 應運用雜湊或其他適當方式之完整性確保機制	✓		
三、營運持續計畫			
(一) 系統備份			
1. 訂定系統可容忍資料損失之時間要求	✓		
2. 執行系統源碼與資料備份	✓		
3. 應定期測試備份資訊，以驗證備份媒體之可靠性及資訊之完整性	✓		
(二) 系統備援			
1. 訂定資通系統從中斷後至重新恢復服務之可容忍時間要求	✓		
2. 原服務中斷時，於可容忍時間內，由備援設備或其他方式取代並提供服務	✓		
四、識別與鑑別			
(一) 內部使用者之識別與鑑別			
1. 資通系統應具備唯一識別及鑑別機關使用者(或代表機關使用者行為之程序)之功能，禁止使用共用帳號	✓		
(二) 身分驗證管理			

版本號：1100823（修訂部分以紅字標示）

檢　查　內　容	檢查結果		備註
	符合	不符合	（若不符合，請加以說明）
1. 使用預設密碼登入系統時，應於登入後要求立即變更	✓		
2. 身分驗證相關資訊不以明文傳輸	✓		
3. 具備帳戶鎖定機制，帳號登入進行身分驗證失敗達五次後，至少十五分鐘內不允許該帳號繼續嘗試登入或使用機關自建之失敗驗證機制	✓		
4. 使用密碼進行驗證時，應強制最低密碼複雜度；強制密碼最短及最長之效期限制	✓		
5. 密碼變更時，至少不可以與前三次使用過之密碼相同	✓		
6. 第四點及第五點所定措施，對非內部使用者，可依機關自行規範辦理	✓		
7. 身分驗證機制應防範自動化程式之登入或密碼更換嘗試	✓		
8. 密碼重設機制對使用者重新身分確認後，發送一次性及具有時效性符記	✓		
(三) 鑑別資訊回饋			
1. 資通系統應遮蔽鑑別過程中之資訊	✓		
(四) 加密模組鑑別			
1. 資通系統如以密碼進行鑑別時，該密碼應加密或經雜湊處理後儲存	✓		
(五) 非內部使用者之識別與鑑別			
1. 資通系統應識別及鑑別非機關使用者(或代表機關使用者行為之程序)	✓		
五、系統與服務獲得			
(一) 系統發展生命週期需求階段			
1. 針對系統安全需求（含機密性、可用性、完整性）進行確認	✓		
(二) 系統發展生命週期設計階段			
1. 根據系統功能與要求，識別可能影響系統之威脅，進行風險分析及評估	✓		
2. 將風險評估結果回饋需求階段之檢核項目，並提出安全需求修正	✓		
(三) 系統發展生命週期開發階段			
1. 應針對安全需求實作必要控制措施	✓		

版本號：1100823（修訂部分以紅字標示）

檢查內容	檢查結果		備註
	符合	不符合	（若不符合，請加以說明）
2. 應注意避免軟體常見漏洞及實作必要控制措施	✓		
3. 發生錯誤時，使用者頁面僅顯示簡短錯誤訊息及代碼，不包含詳細之錯誤訊息	✓		
(四) 系統發展生命週期測試階段			
1. 執行「弱點掃描」安全檢測	✓		
(五) 系統發展生命週期部署與維運階段			
1. 於部署環境中應針對相關資通安全威脅，進行更新與修補，並關閉不必要服務及埠口	✓		
2. 資通系統不使用預設密碼	✓		
3. 於系統發展生命週期之維運階段，應執行版本控制與變更管理	✓		
(六) 系統發展生命週期委外階段			
1. 資通系統開發如委外辦理，應將系統發展生命週期各階段依等級將安全需求（含機密性、可用性、完整性）納入委外契約	✓		
(七) 獲得程序			
1. 開發、測試及正式作業環境應為區隔	✓		
(八) 系統文件			
1. 應儲存與管理系統發展生命週期之相關文件	✓		
六、系統與通訊保護			
(一) 傳輸之機密性與完整性			
(二) 資料儲存之安全			
七、系統與資訊完整性			
(一) 漏洞修復			
1. 系統之漏洞修復應測試有效性及潛在影響，並定期更新	✓		
2. 定期確認資通系統相關漏洞修復之狀態	✓		
(二) 資通系統監控			
1. 發現資通系統有被入侵跡象時，應通報機關特定人員	✓		
2. 監控資通系統，以偵測攻擊與未授權之連線，並識別資通系統之未授權使用	✓		

版本號：1100823（修訂部分以紅字標示）

檢　　查　　內　　容	檢查結果		備註
	符合	不符合	（若不符合，請加以說明）
(三) 軟體及資訊完整性			
1. 使用完整性驗證工具，以偵測未授權變更特定軟體及資訊	✓		
2. 使用者輸入資料合法性檢查應置放於應用系統伺服器端	✓		
3. 發現違反完整性時，資通系統應實施機關指定之安全保護措施	✓		
檢查人員：		權責主管覆核：	

A1.K3 每年定期盤點物聯網設備(IoT)

本校每年進行全校物聯網設備盤點，111 年度於 6 月進行盤點，並持續更新清冊，以下為 111 年度本校物聯網設備盤點表，目前共 378 項，擷取教務處及資訊學院部分資料為例。

國立屏東大學111年度物聯網設備盤點表

序號	一級單位	二級單位	數量	類型	製造廠商/型號(伺服器必填)	維護廠商	作業系統版本(OS Version)	註記(用途)	管理員(Custodian)	IP位置	所在校區及大樓	位置
1	教務處		1	印表機	Epson AL-C300DN			事務列印使用				
2	教務處		1	黑白數位影印機	CANON image RUNNER ADVANCE DX4735i			事務列印使用				
3	教務處		1	網路附加儲存系統	QSAN XN3004T			儲存註冊組、課務組、綜合業務組、教務長室資料用				
4	教務處		1	印表機	HP M700/712dn			事務列印使用				
5	教務處		1	印表機	HP M700/712dn			事務列印使用				
6	教務處		1	彩色印表機	FUJI XEROX CP505D			事務列印使用				
7	教務處		1	影印機	FUJI XEROX DC-V5070			事務列印使用				
8	教務處		1	數位錄影主機	環名/HM-4LA AHD			監控器材室物品				
9	教務處		1	數位錄影主機	環名/HM-5LA AHD			監控器材室物品				
10	教務處		1	數位錄影主機	環名/HM-6LA AHD			監控器材室物品				
11	教務處		1	門禁系統	TOPWORLD/TW951L			知無涯電腦教室門禁系統				
12	教務處		1	雷射黑白數位式多功能複合式影印機	FUJI XEROX/DocuCentre-V 5070			事務列印使用				
13	教務處		1	印表機	EPSON/C9300N			事務列印使用				
14	教務處		1	雷射印表機	HP/5200TN			事務列印使用				

國立屏東大學111年度物聯網設備盤點表

序號	一級單位	二級單位	數量	類型	製造廠商/型號(伺服器必填)	維護廠商	作業系統版本(OS Version)	註記(用途)	管理員(Custodian)	IP位置	所在校區及大樓	位置
367	資訊學院		1	不斷電系統	飛碟/FT-2020DU機架型2000VA在線式			課程上課用				
368	資訊學院		1	不斷電系統	飛碟/FT-2030DU機架型3000VA在線式			課程上課用				
369	資訊學院		1	單槍投影機	EPSON/EB-1720含吊架			課程上課用				
370	資訊學院		1	單槍投影機	SANYO/PLC-XW300			研究報告使用				
371	資訊學院		1	高亮投影機	AAXA/M6			課程上課用				
372	資訊學院		1	複合機	EPSON/WF-C5790			事務列印使用				
373	資訊學院		1	影印機	Bizhub/C227			事務列印使用				
374	資訊學院		1	印表機	EPSON/EPL-N3000			事務列印使用				
375	資訊學院		1	印表機	EPSON/AL-M301DN			實驗室列印用				
376	資訊學院		1	印表機	EPSON/EPL-6200			研究使用				
377	資訊學院		1	印表機	OKI/ES41992			事務列印使用				
378	資訊學院		1	印表機	brother/MFC 9010			事務列印使用				

[回目錄]

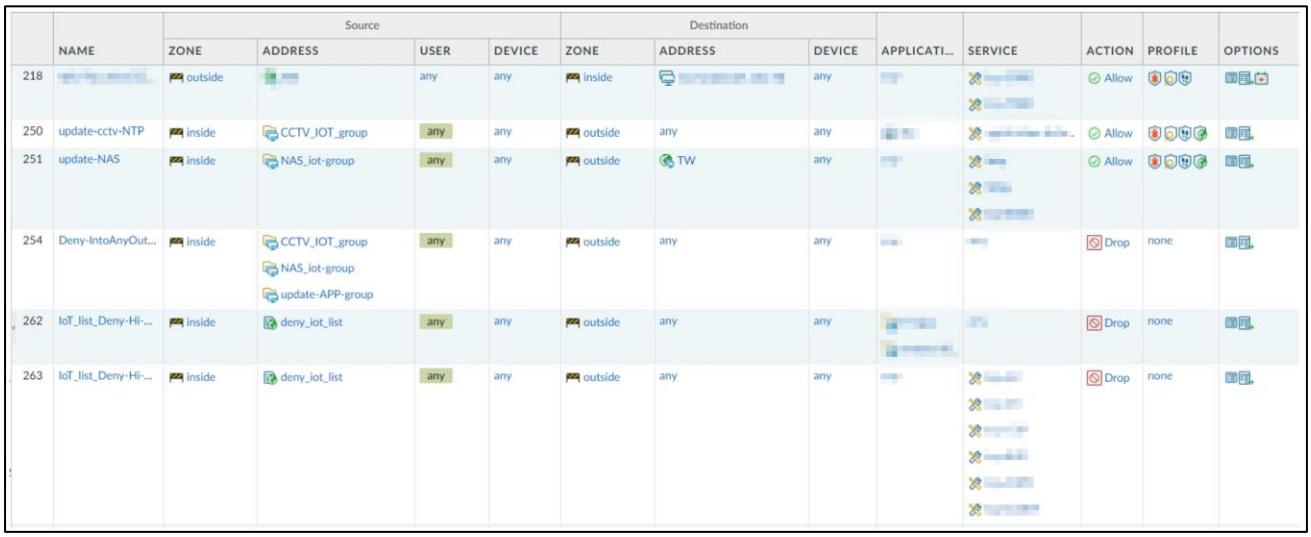
A1.K3 定期物聯網設備(IoT)安全性設定檢測及連線安全管控

物聯網盤點後資料將於防火牆內依設備屬性分類，並限制連線安全

(1) 內對外：IoT 設備進行分類，除開放必要更新外，原則禁止連線。

(2) 外對內：原則禁止，例外開放，並以 VPN 連線方式加強管控。

以下為本校防火牆物聯網設備群組之管理規則(Policy)



		Source				Destination							
	NAME	ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE	APPLICATI...	SERVICE	ACTION	PROFILE	OPTIONS
218	[redacted]	outside	[redacted]	any	any	inside	[redacted]	any	[redacted]	[redacted]	Allow	[redacted]	
250	update-cctv-NTP	inside	CCTV_IOT_group	any	any	outside	any	any	[redacted]	[redacted]	Allow	[redacted]	
251	update-NAS	inside	NAS_iot-group	any	any	outside	TW	any	[redacted]	[redacted]	Allow	[redacted]	
254	Deny-IntoAnyOut...	inside	CCTV_IOT_group NAS_iot-group update-APP-group	any	any	outside	any	any	[redacted]	[redacted]	Drop	none	
262	IoT_list_Deny-Hi-...	inside	deny_iot_list	any	any	outside	any	any	[redacted]	[redacted]	Drop	none	
263	IoT_list_Deny-Hi-...	inside	deny_iot_list	any	any	outside	any	any	[redacted]	[redacted]	Drop	none	

[回目錄]

A1.K4 落實資訊資產風險評估及風險處理

1.本校資產分類共可分為 5 類(實體、軟體、資料、人員及服務)，以下為本校 111 年度風險評鑑及風險處理計畫表，擷取實體及軟體部分頁面為例。

國立屏東大學

文件編號：ISMS-2-002-T01　　安全等級：限閱　　版次：1.0

風險評鑑及風險處理計畫表

表單編號：11101-3　　日期：111年08月03日

序號	資產識別碼	資產名稱	數量	資產型態	製造廠商/型號	維護廠商	註記(用途)	負責人(Owner)	管理員(Custodian)	C	I	A	資產價值(AV=C+I+A)	資產等級	風險來源	脆弱點	威脅	風險處理前：衝擊等級(Im)	風險處理前：發生機率等級(P)	風險處理前：風險值(R=AV*Im*P)	風險處理前：風險等級	現有管控	建議風險處理方式	建議控管項目	風險處理	處理人員	預定完成日期	實際完成日期	控制類型	風險處理後：衝擊等級	風險處理後：發生機率等級	風險處理後：風險值	風險處理後：風險等級
10	實體	無線網路控制器(VM-[illegible]	1		[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	中	缺乏軟硬體維護	設備故障	作業失效	[illegible]	[illegible]	[illegible]	低	保固、維護合約	接受風險										
	實體	無線網路控制器(VM-[illegible]	1		[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	中	人員資安意識、教育訓練不足	操作失當	誤用設備、系統、程式或資料	[illegible]	[illegible]	[illegible]	低	無	接受風險										
11	實體	L2 server switch	14		[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	中	缺乏軟硬體維護	設備故障	系統運作失能	[illegible]	[illegible]	[illegible]	中	備品、簽訂維護合約	降低風險	交換器SPF或SPF+光纖模組汰換	增購交換器SPF或SPF+光纖模組備品	[illegible]	111.7.10	111.7.4	A	[illegible]	[illegible]	[illegible]	低
12	實體	L2 edge switch	10		[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	中	管理活動及控制不足	設備故障	系統運作失能	[illegible]	[illegible]	[illegible]	低	備品、簽訂維護合約	接受風險										
13	實體	光纖 switch	6		[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	中	管理活動及控制不足	設備故障	系統運作失能	[illegible]	[illegible]	[illegible]	低	簽訂維護合約	接受風險										
14	實體	L2 edge switch(wifiAP)	1		[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	中	軟硬體過時	設備故障	系統運作失能	[illegible]	[illegible]	[illegible]	低	簽訂維護合約	接受風險										
15	實體	wifi AP	443		[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	中	人員資安意識、教育訓練不足	設備故障	系統運作失能	[illegible]	[illegible]	[illegible]	低	備品、簽訂維護合約	接受風險										
16	實體	[illegible] Log分析系統	1		[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	中	管理活動及控制不足	設備故障	系統運作失能	[illegible]	[illegible]	[illegible]	低	簽訂維護合約	接受風險										
17	實體	流量管理系統	2		[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	中	缺乏軟硬體維護	設備故障	作業失效	[illegible]	[illegible]	[illegible]	低	簽訂維護合約	接受風險										
18	實體	無線網路DHCP主機 [illegible]	3		[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	中	缺乏軟硬體維護	設備故障	作業失效	[illegible]	[illegible]	[illegible]	低	簽訂維護合約	接受風險										
19	實體	[illegible] mrtg(VM-[illegible]	1		[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	中	缺乏軟硬體維護	設備故障	作業失效	[illegible]	[illegible]	[illegible]	低	簽訂維護合約	接受風險										
20	實體	門禁系統、環控系統-監控伺服器	1		[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	中	管理活動及控制不足	設備故障	系統運作失能	[illegible]	[illegible]	[illegible]	低	簽訂維護合約	接受風險										

國立屏東大學

文件編號：ISMS-2-002-T01　　安全等級：限閱　　版次：1.0

風險評鑑及風險處理計畫表

表單編號：11101-2　　日期：111年08月03日

序號	資產識別碼	資產名稱	供應廠商	版本資訊	資產數量/授權數量	註記(軟體用途)	負責人(Owner)	管理員(Custodian)	負責單位	資產位置	C	I	A	資產價值(AV=C+I+A)	資產等級	風險擁有者	風險來源	脆弱點	威脅	風險處理前：衝擊等級(Im)	風險處理前：發生機率等級(P)	風險處理前：風險值(R=AV*Im*P)	風險處理前：風險等級	現有管控	建議風險處理方式	建議控管項目	風險處理	處理人員	預定完成日期	實際完成日期	控制類型	風險處理後：衝擊等級	風險處理後：發生機率等級	風險處理後：風險值	風險處理後：風險等級
1	軟體	Windows [illegible]	[illegible]	[illegible]	1	[illegible]	[illegible]	[illegible]	計網中心	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	中	許良政	作業或應用系統開發不安全	V29. 未檢視或修補系統運作上之技術弱點	遭受攻擊或入侵	[illegible]	[illegible]	[illegible]	低	自動更新	接受風險										
2	軟體	Windows [illegible]	[illegible]	[illegible]	2	[illegible]	[illegible]	[illegible]	計網中心	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	中	許良政	作業或應用系統開發不安全	V29. 未檢視或修補系統運作上之技術弱點	遭受攻擊或入侵	[illegible]	[illegible]	[illegible]	低	自動更新	接受風險										
3	軟體	Red Hat Enterprise Linux [illegible]		[illegible]		[illegible]	[illegible]	[illegible]	計網中心	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	中	許良政	作業或應用系統開發不安全	V29. 未檢視或修補系統運作上之技術弱點	遭受攻擊或入侵	[illegible]	[illegible]	[illegible]	低	自動更新	接受風險										
4	軟體	Windows [illegible]	[illegible]	[illegible]	授權版	[illegible]	[illegible]	[illegible]	計網中心	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	中	許良政	作業或應用系統開發不安全	V29. 未檢視或修補系統運作上之技術弱點	遭受攻擊或入侵	[illegible]	[illegible]	[illegible]	低	自動更新	接受風險										
5	軟體	[illegible]	[illegible]	[illegible]	1	[illegible]	[illegible]	[illegible]	計網中心	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	中	許良政	缺乏軟硬體維護	V29. 未檢視或修補系統運作上之技術弱點	軟體或程式作業失效	[illegible]	[illegible]	[illegible]	中	無	接受風險	加強系統紀錄檢視	持續監測，紀錄設備於維護合約內。	[illegible]	111.8.31	111.8.31	A	[illegible]	[illegible]	[illegible]	低
6	軟體	[illegible] QoS	[illegible]	[illegible]	1	[illegible]	[illegible]	[illegible]	計網中心	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	中	許良政	作業或應用系統開發不安全	V29. 未檢視或修補系統運作上之技術弱點	遭受攻擊或入侵	[illegible]	[illegible]	[illegible]	低	無	接受風險										
7	軟體	nagios	[illegible]	[illegible]	1	[illegible]	[illegible]	[illegible]	計網中心	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	中	許良政	管理活動及控制不足	V30. 未檢視或修補系統運作上之技術弱點	遭受攻擊或入侵	[illegible]	[illegible]	[illegible]	低	無	接受風險										
8	軟體	Cisco IOS	[illegible]	[illegible]	隨機版	[illegible]	[illegible]	[illegible]	計網中心	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	中	許良政	作業或應用系統開發不安全	V29. 未檢視或修補系統運作上之技術弱點	遭受攻擊或入侵	[illegible]	[illegible]	[illegible]	低	無	接受風險										
9	軟體	門禁AP	[illegible]	[illegible]	1	[illegible]	[illegible]	[illegible]	計網中心	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	中	許良政	管理活動及控制不足	A.10.9.6系統時鐘應予同步	資料稽核軌跡記錄錯誤	[illegible]	[illegible]	[illegible]	低	無	接受風險										
	軟體	門禁AP	[illegible]	[illegible]	1	[illegible]	[illegible]	[illegible]	計網中心	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	中	許良政	管理活動及控制不足	V18. 缺乏足夠的文件或程序指引	操作錯誤	[illegible]	[illegible]	[illegible]	低	無	接受風險										
10	軟體	環控軟體	[illegible]	[illegible]	1	[illegible]	[illegible]	[illegible]	計網中心	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	中	許良政	缺乏軟硬體維護	V29. 未檢視或修補系統運作上之技術弱點	軟體或程式作業失效	[illegible]	[illegible]	[illegible]	低	無	接受風險										
11	軟體	電腦機房監視器軟體	[illegible]	[illegible]	3	[illegible]	[illegible]	[illegible]	計網中心	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	中	許良政	管理活動及控制不足	A.10.9.6系統時鐘應予同步	資料稽核軌跡記錄錯誤	[illegible]	[illegible]	[illegible]	低	定時校時、檢測	接受風險										
	軟體	電腦機房監視器軟體	[illegible]	[illegible]	3	[illegible]	[illegible]	[illegible]	計網中心	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	中	許良政	人員資安意識、教育訓練不足	V18. 缺乏足夠的文件或程序指引	操作錯誤	[illegible]	[illegible]	[illegible]	低	無	接受風險										
12	軟體	Windows [illegible]	[illegible]	[illegible]	授權版	[illegible]	[illegible]	[illegible]	計網中心	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	低	許良政	作業或應用系統開發不安全	V29. 未檢視或修補系統運作上之技術弱點	遭受攻擊或入侵	[illegible]	[illegible]	[illegible]	低	自動更新	接受風險										

[回目錄]

2. 以下為本校 111 年度全校風險評鑑報告，擷取部份內容如下圖

國立屏東大學
文件編號：ISMS-2-002-A01　　安全等級：限閱　　版次：1.1

風險評鑑報告

參、 風險評鑑結果分析

風險評鑑日期為民國111年07月01日至08月03日間，執行風險評鑑作業之結果如下：

一、 資訊資產辨識與價值評估結果

此次風險評鑑階段，各組之資訊資產權責單位依據「ISMS-2-002 資訊資產及風險管理程序書」辨識出資訊資產風險等級如下表：

項次	資產類別	風險等級			總計
		高	中	低	
1	資料資產	0	0	56	56
2	軟體資產	0	2	65	67
3	實體／環境資產	0	1	123	124
4	人員資產	0	0	20	20
5	服務資產	0	0	14	14
合計		0	3	278	281

二、 不可接受風險評鑑彙整表

資產識別碼	資產名稱	管理員 (Custodian)	C	I	A	資產價值 (AV=C+I+A)	資產等級	脆弱點	威脅	風險處理前			
										衝擊等級(Im)	發生機率等級(P)	風險值 (R=AV*Im*P)	風險等級
無	無												

三、 重點改善建議

1. 本次風險評鑑作業結果，各類資訊資產無高風險項目;另外針對3項中風險等級項目(軟體類2項、實體／環境類1項)，為求業務精進，亦在有限資源下執行風險處理作業，降低營運威脅，後續應持續監控運作狀況，若因不預期因素造成風險值升高，且高於55(含)以上時，則依接受、降低、移轉及迴避等方式與原則採取適切的對應措施，以降低風險，維持重要營運系統持續運作。
2. 鑒於不可接受風險值設定於「55」已經超過5年了，且目前各項資訊資產在有效管控與維運下，僅有極少數為「中」風險等級，在考量有限資源暨精益求精目標下，建議明年度不可接受風險降為「50(含)」。風險等級級距同步建議調整如下：

［回目錄］

3.資訊資產及風險管理程序書擷取部分內容如下圖，適用範圍為全校之所有資訊處理作業及資訊機房。

國立屏東大學

名稱	資訊資產及風險管理程序書	安全等級	限閱
編號	ISMS-2-002	版次	1.1

1　目的

本文件規範國立屏東大學(以下簡稱本校)資訊資產及其風險之管理程序，藉此方法評估其資訊之機密性、完整性與可用性，與其在作業執行時的風險及處理風險的方式，並採取有效的控制措施，使本校資訊資產受到適當保護，以確保業務持續運作。

2　適用範圍

適用本校之所有資訊處理作業及資訊機房，包括作業人員、軟體、資料、服務及實體設備等資訊資產。

A1.K4 落實全校個人資料檔案風險評估及風險處理

1.以下為本校個人資料保護管理程序書部分內容，適用範圍為全校各項業務流程中涉及個資蒐集、處理及利用所產生之紙本與電子資料。

名稱	個人資料保護管理程序書	安全等級	限閱
編號	PIMS-2-001	版次	1.4

1　目的

為使本校各項作業遵循中華民國個人資料保護法（以下簡稱個人資料保護法）、個人資料保護法施行細則及相關法令規範之要求，強化個人資料管理與保護，免於遭受內、外部的蓄意或意外之威脅，特訂定個人資料保護管理程序書。

2　適用範圍

本校各項業務相關流程中涉及個人資料蒐集、處理及利用所產生之紙本與電子型式資料（包括備份檔案）。

2.本校每年進行全校個資盤點及風險評鑑，以下為擷取教務處部分 111 年度個資盤點清冊暨風險評鑑表為例。

國立屏東大學
文件編號：PIMS-2-001-T02　　安全等級：限閱　　版次：1.2

個資盤點清冊暨風險評鑑表

表單編號：　　日期：111.6.16

項目 / 單位名稱	一、個人資料檔案名稱及檔案形式(資料庫、電子檔、紙本、單據、清冊..)	二、保有依據	三、特定目的	四、個人資料類別	五、是否含特種個資	六、是否含未成年人員個資	七、規範行為(蒐集、處理、利用)	八、資料流與保存地點				九、保存年限	影響及衝擊				風險發生機率等級	風險值	風險等級	改善措施(如風險等級為中、高時)
								共同控制者	資料控制者	資料處理者	保管人及保存地點		蒐集處理利用範圍	個資數量	敏感程度	評估項目最大值(即為影響及衝擊等級)				
教務處課務組	學生選課資料	大學法	158學生（員）(含畢、結業生)資料管理	C001辨識個人者、C051學校紀錄、C057學生(員)、應考人紀錄、學號	否	是	蒐集、處理					10					2	低	
教務處課務組	教師授課時數表、明細表	大學法	109教育或訓練行政	C001辨識個人者、C054職業專長	否	否	蒐集、處理					10					2	低	
教務處課務組	工讀學生資料	依業務需求辦理	158學生（員）(含畢、結業生)資料管理	C001辨識個人者、C051學校紀錄、C057學生(員)、應考人紀錄、學號	否	否	蒐集、處理					10					2	低	
教務處課務組	張鳳燕獎學金得獎學生資料	大學法	158學生（員）(含畢、結業生)資料管理	C001辨識個人者、C002識別財務、C003政府資料中之辨識者、C051學校紀錄、C057學生(員)、應考人紀錄、學號	否	否	蒐集、處理					15					2	低	
教務處綜合業務組	考生基本資料（含成績）	大學辦理招生規定審核作業要點、國立屏東大學各項招生規定、簡章	158學生（員）(含畢、結業生)資料管理	C001、C003、C011、C038、C051、C052、C057、C061	否	是	蒐集、處理					10					2	低	

［回目錄］

3.本校 111 年個資數量共計 755 項，下圖為 111 年本校個人資料保護風險評鑑報告部分內容。

個人資料保護風險評鑑報告

二、 個資盤點與風險評鑑結果

此次風險評鑑階段，全校各單位依據「PIMS-2-001個人資料保護管理程序書」辨識與評鑑出的個資數量及風險等級如下表：

項次	單 位 別	風險等級			個資數量總計
		高	中	低	
1	秘書室	0	0	19	19
2	教務處	0	0	145+1	146
3	學務處	0	0	70	70
4	總務處	0	0	15	15
5	研究發展處	0	0	16	16
6	國際事務處	0	0	46	46
7	實習就業輔導處	0	0	13	13
8	圖書館	0	0	31	31
9	人事室	0	0	41	41
10	主計室	0	0	2	2
11	體育室	0	0	5	5
12	計算機與網路中心	0	0	14-1	13
13	管理學院	0	0	81-1	80
14	資訊學院	0	0	56	56
15	教育學院	0	0	42	42
16	人文社會學院	0	0	52-1	51
17	理學院	0	0	71	71
18	國際暨創新學院	0	0	4+2	6
19	大武山學院	0	0	15	15
20	師資培育中心	0	0	17	17
合計		0	0	755+0	755

［回目錄］

A1.K5 辦理內部資通安全稽核

本校每年度辦理二次資通安全內部稽核，一次為**資訊安全內部稽核**作業，稽核範圍包含計算機與網路中心及涉及核心資通系統之 ISO27001 驗證範圍；另一次為**個資安全內部稽核作業**，本稽核範圍為全校各行政與教學單位。

1. 資訊安全內部稽核計畫

國立屏東大學

文件編號：ISMS-2-003-A01　安全等級：限閱　　版次：1.0

111 年資訊安全內部稽核計畫

一、計畫依據：

依據本校資訊安全稽核作業程序書對ISMS監控及審查之要求，執行年度資訊安全作業活動內部稽核作業。

二、稽核日期：

111年 08 月 17 日

三、稽核人員：

組長：[redacted]

組員：[redacted]

四、稽核時程：(稽核項目包含稽核啟始會議、執行稽核審查、稽核人員討論與報告撰寫、稽核結束會議)

時間	稽核項目	稽核員	受稽單位(人員)	地點
09：00～09：30	稽核啟始會議	All	All (計網中心)	計網中心B1會議室
09：30～12：00	執行稽核審查 1.機房管理 2.網路管理 3.電子郵件系統管理	[redacted]	[redacted]	計網中心
10：30～12：00	執行ISMS稽核審查	[redacted]	ALL	計網中心
13：30～16：00	執行稽核審查 1. 校務行政系統(學籍、選課、成績、招生)管理	[redacted]	[redacted]	計網中心

國立屏東大學

文件編號：ISMS-2-003-A01　安全等級：限閱　　版次：1.0

	2. 學校首頁網站管理			
14：30～16：00	執行ISMS稽核審查		ALL	計網中心
16：00～16：30	稽核人員討論與報告撰寫			計網中心B1會議室
16：30～17：00	稽核結束會議	All	All (計網中心)	計網中心B1會議室

稽核重點內容：

■ 根據資訊安全內部稽核表檢查項目審查。

五、執行：經資安管理代表核准後執行

承辦人：　　主管：　　資安管理代表：

［回目錄］

2.個人資料保護內部稽核計畫

國立屏東大學

文件編號：ISMS-2-003-A01　安全等級：限閱　　版次：1.0

111 年個人資料保護內部稽核計畫

一、計畫依據：

依據個人資料保護法、個人資料保護法施行細則、相關法令規範、本校個人資料保護管理要點及內部稽核查檢表之要求及各單位111年7月所產出「PIMS-2-001-T02個資盤點清冊暨風險評鑑表」進行查核。

防疫個人資料跟據嚴重特殊傳染性肺炎中央流行疫情指揮中心「防疫個人資料稽核指引」進行查核。

各單位資通系統根據「資通安全責任等級分級辦法」附表十資通系統防護基準進行查核。

二、稽核日期：

111年10月20日、10月27日

三、稽核人員：

組長：[redacted]

組員：[redacted]

四、稽核時程：(稽核項目包含稽核啟始會議、執行稽核審查、稽核人員討論與報告撰寫、稽核結束會議)

受稽單位	稽核日期	稽核時間
總務處文書組	10/20	上午 9:00~12:00
總務處事務組	10/20	上午 9:00~12:00
總務處營繕組	10/20	上午 9:00~12:00
總務長室	10/20	上午 9:00~12:00
學生事務處衛生保健組(民生校區)	10/20	上午 9:00~12:00
總務處環安組	10/20	上午 9:00~12:00
體育室(屏師)	10/20	下午 14:00~17:00
原住民族學生資源中心(屏師)	10/20	下午 14:00~17:00
華語教學中心(屏師)	10/20	下午 14:00~17:00
教務處專案業務組(屏師)	10/20	下午 14:00~17:00

國立屏東大學

文件編號：ISMS-2-003-A01　安全等級：限閱　　版次：1.0

教務處推廣教育中心(屏師)	10/20	下午 14:00~17:00
音樂學系(屏師)	10/20	下午 14:00~17:00
視覺藝術學系(屏師)	10/20	下午 14:00~17:00
學生事務處學生諮商中心	10/27	上午 9:00~12:00
人事室	10/27	上午 9:00~12:00
教育學系	10/27	上午 9:00~12:00
教育行政研究所	10/27	上午 9:00~12:00
教育心理與輔導學系	10/27	上午 9:00~12:00
幼兒教育學系	10/27	上午 9:00~12:00
特殊教育學系	10/27	上午 9:00~12:00
特殊教育中心	10/27	上午 9:00~12:00
學生事務處衛生保健組(屏商校區)	10/27	下午 14:00~17:00
國際經營與貿易學系	10/27	下午 14:00~17:00
企業管理學系	10/27	下午 14:00~17:00
財務金融學系	10/27	下午 14:00~17:00
會計學系	10/27	下午 14:00~17:00
不動產經營學系	10/27	下午 14:00~17:00
休閒事業經營學系	10/27	下午 14:00~17:00
行銷與流通管理學系	10/27	下午 14:00~17:00
商業自動化與管理學系	10/27	下午 14:00~17:00

備註：受稽單位除表定外，視稽核狀況，可另隨機抽測未表列之單位。

稽核重點內容：

- 110年內部稽核共同發現事項及建議審查。
- 根據**PIMS-2-001-T03個人資料保護稽核查檢表**檢查項目審查。
- 防疫個人資料稽核。
- 「資通安全責任等級分級辦法」附表十資通系統防護基準(適用有資通系統之單位)。

國立屏東大學

文件編號：ISMS-2-003-A01　安全等級：限閱　　版次：1.0

五、執行：經個資保護稽核小組召集人核准後執行

承辦人：　　主管：　　資安管理代表：

3.以下為 111 年度本校資通系統內部稽核，以人事室保費整合管理系統之矯正處理單為例。

國立屏東大學

文件編號：ISMS-2-012-T01　安全等級：限閱　　版次：1.0

矯正處理單

表單編號：

提出單位	稽核小組	提出人員	盧有志 魏佑恩	提出日期	111.10.20
缺失權責單位	人事室	處理人員	[redacted]	填寫日期	111.11.30
事件來源： ■內部稽核 □外部稽核□自行提出 □其他_____					
稽核項目 (內外部稽核時才需填寫)	111 年資通系統內部稽核				
缺失事項：	保費整合管理系統 1. [redacted] 2. 請依資通安全責任等級分級辦法附表十資通系統防護基準，完成本系統各項控制措施。				
根因分析：	經檢討上述稽核所發現缺失係因前建立 ISMS 機制實施，仍有部分程序未能完全符合。				
矯正措施：	1. [redacted] 2. [redacted] 3. [redacted]				
預定完成日期：111.11.30		實際完成日期：111.11.30			
備註：					
追蹤人員：	追蹤單位主管：	追蹤日期：	確認結果：		

［回目錄］

A1.K5 資通安全稽核提報管理審查

以下為 111 年 8 月 31 日召開之管理審查會議簡報，擷取有關 111 年度資通安全內部稽核部分，稽核相關事件說明及後續矯正措施均提報會議。

國立屏東大學 National Pingtung University

參、資訊安全的績效回饋

■ 矯正措施之來源

- ➢資安內部稽核小組負責追踪
- ➢矯正處理單-其他（1件）
- ➢資訊安全內部稽核本年度內部稽核(111年8月17日)
  - ●觀察事項(WP/OBS)：0項，改善建議(OFI)：3項
- ➢已處理完成並填寫矯正處理單。

國立屏東大學 National Pingtung University

參、資訊安全的績效回饋

■ 矯正措施之來源

➢ 資訊安全內部稽核-資安內部稽核小組負責追踪

111年內部稽核矯正處理單

表單編號	事件說明	稽核項目	備註（完成日期）
111002	OFI-1 稽核發現：	A.6.1.2 職務的區隔	111/08/18
111003	OFI-2 稽核發現：	A.10.1.2 金鑰管理	111/08/22

[回目錄]

A1.K5 辦理委外服務供應商稽核

以下為本校 111 年度辦理之委外服務供應商稽核，以本校某資訊系統平台為例，惟本年度因疫情採書面稽核方式進行，後續將規劃安排以實地訪查方式稽核。

國立屏東大學

文件編號：ISMS-2-011-T02　安全等級：限閱　　版次：1.0

委外廠商資安查核表

表單編號:

廠商名稱	[redacted]	統一編號	[redacted]	廠商負責人	[redacted]
廠商承辦人（自評人）	[redacted]	廠商連絡電話	[redacted]	自評/查核日期	2022/08/24

查核項目	查核內容	說明	查核結果		查核紀錄
			廠商自評	計網中心複評	
1.設置資安推動組織	1.1 單位是否已組成資訊安全推動組織，同時可清楚說明資通安全責任分工?是否具備完善之資通安全管理措施或通過第三方驗證?	公司指定適當高階主管擔任資安長，且有資安責任分工組織表(處理、通報…等角色)	☑符合 ☐部分符合 ☐不符合 ☐不適用	☐未發現不符合現象 ☐限期改善	參考 ISMS-04-05_資安暨個資管理組織人員對照表_V2.0
	1.2 單位是否指派專人或專責單位，負責辦理資通安全管理措施等事項？	公司指派專員負責辦理資通安全管理措施	☑符合 ☐部分符合 ☐不符合 ☐不適用	☐未發現不符合現象 ☐限期改善	ISMS-04-05_資安暨個資管理組織人員對照表_V2.0 ISMS-02-02_資安與個資組織及管理審查作業程序書_V2.1
	1.3 單位是否對資通安全管理措施之適切性及有效性定期做必要之審查及調整？	定期檢視新修訂資安相關法規規範與新興風險，進行調整相關資安管理措施	☑符合 ☐部分符合 ☐不符合 ☐不適用	☐未發現不符合現象 ☐限期改善	每年召開一次管理審查會議
	單位是否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？	專案資安人力及本專案團隊人員中，是否有相關的專業資安證照？	☑符合 ☐部分符合 ☐不符合 ☐不適用	☐未發現不符合現象 ☐限期改善	內部稽核小組，[redacted]擁有 ISO-27001 稽核員證照
2.資安管理措施推動	組織之資通安全管理措施是否由管理階層核准並正式發布且轉知所有同仁？	確認資安措施發布流程與宣傳方式(如定期教育訓練)	☑符合 ☐部分符合 ☐不符合 ☐不適用	☐未發現不符合現象 ☐限期改善	參考一、二階規範、程序書 ISMS-04-31-資訊安全及個資目標量測表-

第 1 頁，共 5 頁

國立屏東大學

文件編號：ISMS-2-011-T02　安全等級：限閱　　版次：1.0

查核項目	查核內容	說明	查核結果		查核紀錄
			廠商自評	計網中心複評	
	是否隨時公告資安相關訊息?	資安訊息如何宣導(公佈欄、Mail、網頁…等)，並確保所有同仁及本案有關之委外廠商皆知悉。	☑符合 ☐部分符合 ☐不符合 ☐不適用	☐未發現不符合現象 ☐限期改善	參考一、二階規範、程序書
3.實體環境安全	人員進入重要實體區域，是否訂有安全控制措施？	公司(組織)是否訂有門禁管制措施？ 重要實體區域(如機房)之人員進出活動是否有監視器或相關紀錄表。	☑符合 ☐部分符合 ☐不符合 ☐不適用	☐未發現不符合現象 ☐限期改善	ISMS-03-07_實體與環境安全作業規範_V1.0
	重要實體區域的進出權限，是否定期審查並更新？	重要實體區域進出是否有相關管理措施並定期檢視更新相關清單？人員、設備進出是否取得授權？(離職人員之權限是否已刪除)	☑符合 ☐部分符合 ☐不符合 ☐不適用	☐未發現不符合現象 ☐限期改善	每週確認設備 ISMS-03-07_實體與環境安全作業規範_V1.0
	第三方支援服務人員進入重要實體區域是否經過授權並陪同或監視？	第三方支援服務人員是否取得授權並依照門禁規範記錄出入，必要時配合監視器觀察，是否有違規之行為。無卡人員如何進出機房，確認是否有相關紀錄。	☑符合 ☐部分符合 ☐不符合 ☐不適用	☐未發現不符合現象 ☐限期改善	需相關授權人員陪同確認 ISMS-03-07_實體與環境安全作業規範_V1.0
	各項安全設備(如消防設備)是否定期檢查？同仁有否施予適當的安全	依規定定期檢查並按時提供同仁安全設備之使用訓	☑符合	☐未發現不符合現象	每季量測同仁電腦 ISMS-04-31-資訊安全

第 2 頁，共 5 頁

國立屏東大學

文件編號：ISMS-2-011-T02　安全等級：限閱　　版次：1.0

查核項目	查核內容	說明	查核結果		查核紀錄
			廠商自評	計網中心複評	
	設備使用訓練？	練紀錄？ 機房設備維護紀錄，以及教育訓練紀錄(包含消防)。	☐部分符合 ☐不符合 ☐不適用	☐限期改善	及個資目標量測表-V1.1-2022-1
4.資通安全管理措施之實施情況	是否全面使用防毒軟體並即時更新病毒碼？	防毒軟體應設自動更新並檢查為最新防毒碼	☑符合 ☐部分符合 ☐不符合 ☐不適用	☐未發現不符合現象 ☐限期改善	ISMS-04-27_辦公室資訊安全檢查表_V1.0
	執行本案所使用之設備，是否定期執行各項系統漏洞修補程式？	確認系統漏洞修補情形，如 Windows Update 等	☑符合 ☐部分符合 ☐不符合 ☐不適用	☐未發現不符合現象 ☐限期改善	ISMS-04-27_辦公室資訊安全檢查表_V1.0
	是否要求電子郵件附件及下載檔案在使用前需檢查有無惡意軟體(含病毒、木馬或後門等程式)？	公司電子郵件保護機制，是否有 SPAM、防毒等機制過濾信件	☑符合 ☐部分符合 ☐不符合 ☐不適用	☐未發現不符合現象 ☐限期改善	使用 office365，進行電子郵件防護
	執行本案所使用之設備，電腦或終端機不使用時，是否有上鎖或密碼等管制措施？(個人電腦設定開機密碼及設定螢幕保護程式，啟動時間建議設定15分鐘以內為宜，並設定密碼保護)	如螢幕保護程式。檢視是否未將密碼記錄在書面上或張貼在個人電腦、螢幕或其他容易洩漏秘密之場所。	☑符合 ☐部分符合 ☐不符合 ☐不適用	☐未發現不符合現象 ☐限期改善	整合 AD，並設定 10 分鐘未操作進行保護程式 ISMS-04-27_辦公室資訊安全檢查表_V1.0
	密碼應至少為8碼，需有大小寫字母、數字或符號組成（建議前述規則4者取3者或以上為宜)？	抽查密碼規則設定	☑符合 ☐部分符合 ☐不符合 ☐不適用	☐未發現不符合現象 ☐限期改善	ISMS-04-27_辦公室資訊安全檢查表_V1.0
	檢視與本案相關資訊設備是否安裝或使用來路不明、未經授權或影響電腦網路環境安全之電腦軟體。	抽查是否有違法使用軟體(如破解版盜版軟體、或具資安疑慮的產品)	☑符合 ☐部分符合 ☐不符合	☐未發現不符合現象 ☐限期改善	ISMS-04-27_辦公室資訊安全檢查表_V1.0

第 3 頁，共 5 頁

國立屏東大學

文件編號：ISMS-2-011-T02　安全等級：限閱　　版次：1.0

查核項目	查核內容	說明	查核結果		查核紀錄
			廠商自評	計網中心複評	
			□不適用		
	與本案相關之資料，若需依規定或本校要求銷毀者，是否有安全的方式清除，例如燒毀、以碎紙機處理、或將資料從媒體中完全清除?	是否訂有資料銷毀流程?(紙本檔案、電子檔案)	☑符合 □部分符合 □不符合 □不適用	□未發現不符合現象 □限期改善	ISMS-02-01_文件與紀錄管理作業程序書_V2.1 ISMS-04-19_資產報廢文件銷毀單_V1.0
	與本案相關人員工作調整時，權限是否立即異動?離職或退休是否中止其使用權限?(若無人員異動則不適用)	抽查本案執行期間之異動人員資料、帳號等	☑符合 □部分符合 □不符合 □不適用	□未發現不符合現象 □限期改善	ISMS-03-02_人力資源安全作業規範_V1.1 ISMS-03-04_存取控制作業規範_V1.0 ISMS-04-02_存取權限審查表_V1.0-2022
5.訂定資通安全事件通報及應變之程序及機制	是否建立資通安全事件發生之通報應變程序？	是否訂定資安事件之通報應變，日常需建立所有利害關係人清單及聯絡窗口，並定期檢視更新。	☑符合 □部分符合 □不符合 □不適用	□未發現不符合現象 □限期改善	ISMS-02-08_資安與個資事故管理作業程序書_V2.1 ISMS-04-04_資安與個資通報暨矯正措施單_V2.0
	本案專案成員是否知悉，本案資安事件通報應變程序？	抽查宣導是否包含本案資安事件通報應變程序	☑符合 □部分符合 □不符合 □不適用	□未發現不符合現象 □限期改善	
	是否留有資通安全事件處理之紀錄文件，紀錄中並有改善措施？	如曾發生資安事件，則檢視相關文件。 如未曾發生過資安事件則不適用。	□符合 □部分符合 □不符合 ☑不適用	□未發現不符合現象 □限期改善	
	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，是否	抽查是否有本案聯繫窗口資訊	☑符合 □部分符合	□未發現不符合現象 □限期改善	

國立屏東大學

文件編號：ISMS-2-011-T02　安全等級：限閱　　版次：1.0

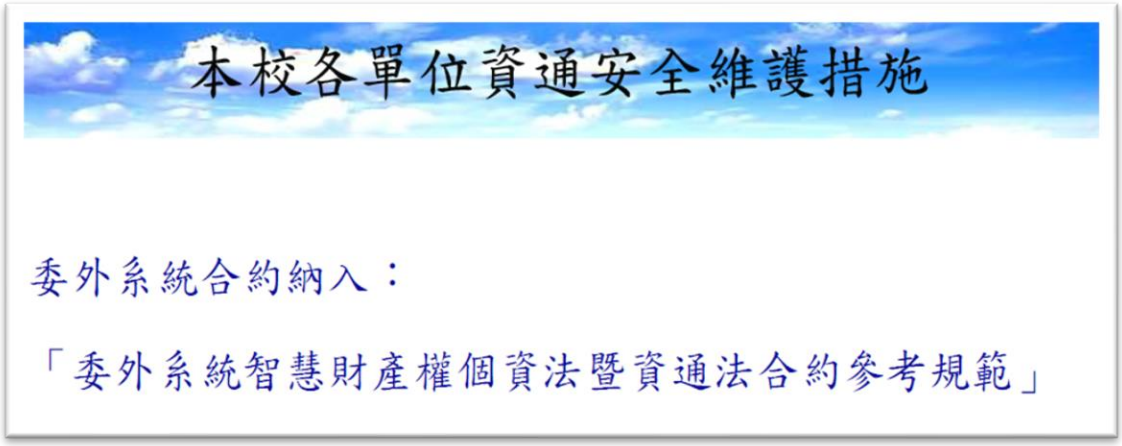
查核項目	查核內容	說明	查核結果		查核紀錄
			廠商自評	計網中心複評	
	有立即通知本校及採行之補救措施?		□不符合 □不適用		
6.定期辦理資通安全認知宣導及教育訓練	是否定期辦理資通安全認知宣導及評量?	資安宣導及評量之頻率，相關文件或紀錄	☑符合 □部分符合 □不符合 □不適用	□未發現不符合現象 □限期改善	
7.資通安全績效管考機制	是否追蹤過去缺失之改善情形？(若尚無發生過缺失則不適用)	檢視過去其他單位委商稽核、廠商內部稽核、系統弱掃或滲透測試報告等紀錄及改善情形	☑符合 □部分符合 □不符合 □不適用	□未發現不符合現象 □限期改善	
	是否定期召開持續改善之會議(如管理審查會議)?	是否至少一年開一次會議檢視全年資安辦理情況及各項缺失改善情形	☑符合 □部分符合 □不符合 □不適用	□未發現不符合現象 □限期改善	每年召開管理審查會議 ISMS-04-31-資訊安全及個資目標量測表-V1.1-2022-1
審查結果	☑合格□不合格□待改善	審查意見	[redacted]		
廠商代表	[redacted]	稽核人員	[redacted]	權責主管	[redacted]

備註： 本次查核係採抽樣方式進行，查核結果「符合」者，僅表抽樣標的符合規定，未被抽樣查核者，不以本結果論之。

［回目錄］

A1.K5 辦理委外資通系統承辦人員講習，以維護資訊作業委外安全

1.本校訂立委外資通系統(含資通服務)與涉及智慧財產權、個資法暨資通法合約條款參考規範，並於 111 年 6 月 2 日辦理之教育訓練講習進行宣導，以下為及**6 月 2 日講習簡報檔**及**委外合約參考規範**。未來將規劃特別針對委外資通系統承辦辦理委外資訊安全專題講習。



本校委外資通系統(含資通服務)與涉及智慧財產權、個資法暨資通法合約條款參考規範

111.09.02

一、保證責任與賠償義務

廠商保證交付之履約標的或提供服務時，不得侵害他人智慧財產權並恪遵個人資料保護法及資通安全管理法，如有侵害他人權利，悉由廠商自負法律上責任。

本校使用廠商交付之履約標的或服務時，致遭第三人主張涉及侵害他人智慧財產權及個人資料保護法或違反資通安全管理法，廠商應協助本校為必要之答辯及提供相關資料，並負擔本校因此所生訴訟費、律師費用及其他衍生之費用，並應負相關損害賠償責任。

二、使用資料之義務與責任

廠商執行本校委外採購案(以下簡稱本案)時有關人員應簽立保密切結書，並承諾於本契約有效期間內及終止後，廠商因執行本案而知悉或持有一切本校未標示得對外公開之公務秘密，以及本校依契約或法令對第三人負有保密義務之業務秘密，必須嚴格保密，並限於本契約目的範圍內，於本校指定之處所內使用。契約履約或終止後，廠商應刪除或銷毀執行服務所持有本校之相關資料，或依本校之指示返還或移交之。非經本校事前書面同意，廠商不得為本人或任何第三人之需要而複製、保有、利用該等資料或將之洩漏、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資料，亦不得攜至非校方所指定以外之處所，如有違反，廠商需負一切相關法律責任，並賠償校方所有損失（如負擔校方因此所生訴訟費、律師費用、損害賠償及其他衍生之費用），本案結束後亦同。

三、稽核監督之權利

本校依據資通安全管理法第9條及資通安全管理法施行細則第4條、個人資料保護法第4條及個人資料保護法施行細則第8條之規定，廠商需有完善之資通安全管理措施及個人資料保護機制，包括個人資料外洩事件之通知程序及採行補救措施，本校並得隨時稽核監督廠商及其分包廠商，如有發現任何缺失，廠商應無條件配合改善。

四、資通安全應辦事項

廠商須遵循「資通安全管理法」及相關子法、「個人資料保護法」及其主管機關相關規定並配合本校 ISMS 規範，提供與協助本系統各項資通安全應辦事項及防護控制措施。

廠商須協助本校執行資通系統各項安全性更新與設定(如作業系統、資料庫)，並配合本校執行安全性檢測 (如弱點掃描、滲透測試)、資通安全健診之系統改善及各項安全性更新與設定。

本系統依資通安全責任等級分級辦法－附表九資通系統防護需求分級原則，防護需求等級為____（普／中／高），廠商須配合本校需求完成附表十之控制措施，維護期間亦需依相關法規修訂完成各項控制措施。

廠商需協助本校執行系統(含源碼、檔案、資料庫)備份及還原作業，並配合本校執行持續營運演練。

合約期間廠商須協助填報各項資通系統或資通服務相關調查。

本案涉及資通訊軟體、硬體或服務等相關事務，廠商執行本案之團隊成員不得為陸籍人士，並不得提供及使用大陸廠牌資通訊產品。廠商不得以經濟部投資審議委員會網站公告之陸資資訊服務業者為分包廠商。

五、資通安全事件通報與應變

廠商於履行本案知悉資通安全事件時，應於1小時內向本校委託單位所屬之權責人員進行通報；本受託業務相關之資通安全事件，廠商需於規定時限內完成損害控制或復原事項（依本校資通安全事件通報及應變管理程序）。

［回目錄］

2.本校各單位簽辦資通系統委外合約時，由計算機與網路中心協助檢視其中資安規範，規範包含得隨時稽核監督廠商(委商外稽)，以下是文書組**電子公文系統維護合約**及保管組**財產管理系統維護合約**為例，擷取其中資安相關規範。

<table>
<tr>
<td>

國立屏東大學
「112 年度電子公文線上簽核系統維護」招標規範
一、維護目的：
維持本校電子公文線上簽核系統之正常運作，並接受系統使用者之操作諮詢服務、系統作業功能項目之增修事項及諮詢服務，以利業務之順利進行及推展。
二、維護標的物：
「電子公文線上簽核系統」(以下簡稱本系統)係指本校現使用[redacted]電子公文線上簽核系統及其相關附屬程式之所有內容。
三、維護期間：自 112 年 1 月 1 日起至 112 年 12 月 31 日止。
四、維護項目及需求：
(一)系統管理：
1. 視系統運轉狀況不定期實施系統效能調校，調整資料庫索引值，以確保本系統之正常運轉。
2. 異常狀況之診斷、系統故障排除。
3. 維護期間內若伺服主機、資料庫需異動或需建立備援主機時(相關軟、硬體由機關提供)，免費提供系統資料庫移機或建立備援主機服務(以上免費服務以 1 次為限)，並維持資料之完整性。
4. 系統備份相關軟硬體由本校提供，廠商須協助以下設定：
(1)每日系統備份設定。
(2)定期系統異地備份設定。
5. 配合機關需求進行災害復原演練，以驗證備份資訊之可靠性及完整性。(維護期間至少 1 次，但以 2 次為上限)
(二)操作與諮詢：

</td>
<td>

七、智慧財產權、個資法暨資通法合約條款
1、保證責任與賠償義務
廠商保證交付之履約標的或提供服務時，不得侵害他人智慧財產權並恪遵個人資料保護法及資通安全管理法，如有侵害他人權利，悉由廠商自負法律上責任。本校使用廠商交付之履約標的或服務時，致遭第三人主張涉及侵害他人智慧財產權及個人資料保護法或違反資通安全管理法，廠商應協助本校為必要之答辯及提供相關資料，並負擔本校因此所生訴訟費、律師費用及其他衍生之費用，並應負相關損害賠償責任。
2、使用資料之義務與責任
廠商執行本校委外採購案(以下簡稱本案)時有關人員應簽立保密切結書，廠商因執行本案而知悉或持有一切本校未標示得對外公開之公務秘密，以及本校依契約或法令對第三人負有保密義務之業務秘密，必須嚴格保密，並限於本契約目的範圍內，於本校指定之處所內使用。契約履約或終止後，廠商應刪除或銷毀執行服務所持有本校之相關資料，或依本校之指示返還或移交之。非經本校事前書面同意，廠商不得為本人或任何第三人之需要而複製、保有、利用該等資料或將之洩漏、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資料，亦不得攜至非校方所指定以外之處所，如有違反，廠商需負一切相關法律責任，並賠償校方所有損失（如負擔校方因此所生訴訟費、律師費用、損害賠償及其他衍生之費用），本案結束後亦同。
3、稽核監督之權利
本校依據資通安全管理法第 9 條及資通安全管理法施行細則第 4 條、個人資料保護法第 4 條及個人資料保護法施行細則第 8 條之規定，廠商需有完善之資通安全管理措施及個人資料保護機制，包括個人資料外洩事件之通知程序及採行補救措施，本校並得隨時稽核監督廠商，如有發現任何缺失，廠商應無條件配合改善。
4、資通安全應辦事項

</td>
</tr>
<tr>
<td>文書組電子公文線上簽核系統
112 年度維護合約招標規範</td>
<td>電子公文線上簽核系統，招標規範第七條為資安相關規範</td>
</tr>
<tr>
<td>

國立屏東大學
「112 年度網路版財產管理系統維護」勞務採購案
招標規範
第一條　合約說明
一、 合約名稱：112 年度網路版財產管理系統維護。
二、 廠商(以下簡稱乙方)維護國立屏東大學(以下簡稱甲方)本招標規範所列應用軟體系統，願於合約有效期間，依本合約之議定，提供最佳服務。
三、 系統名稱：網路版財產管理系統。
四、 設置地點：民生校區五育樓 1 樓保管組、B1 計算機與網路中心。
五、 有效期限：自民國 112 年 1 月 1 日起至民國 112 年 12 月 31 日止。
第二條　請款方式
一、 付款方式：[redacted]
二、 乙方應於[redacted]寄送當期發票及該季維護紀錄向甲方請款，甲方於收到乙方發票及維護紀錄經審核無誤後 20 日內付清。
第三條　維護範圍
一、 服務範圍
（一）系統執行之中斷錯誤：屬於系統語言範圍內之任何錯誤。
（二）數字運算、流程錯誤：系統量值運算有任何誤差，非資料建檔之錯誤；因程式更改而產生之關連性錯誤。

</td>
<td>

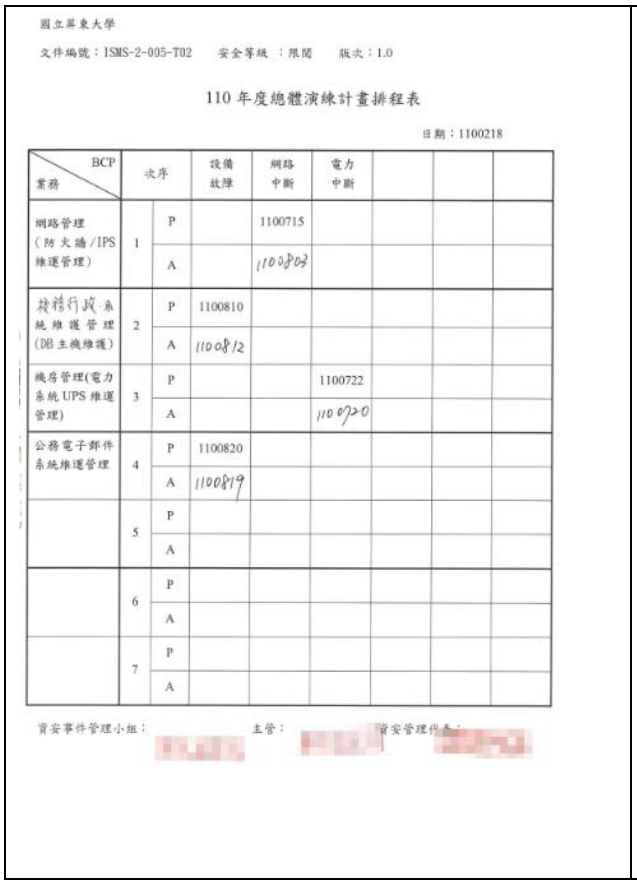
七、 本合約如有任何疑義時，雙方應以誠實信用之原則協議之。
八、 本合約所生一切訴訟，雙方同意以甲方所在地之地方法院為第一審管轄法院。
第七條　智慧財產權、個資法暨資通法合約條款
一、 保證責任與賠償義務
乙方保證交付之履約標的或提供服務時，不得侵害他人智慧財產權並恪遵個人資料保護法及資通安全管理法，如有侵害他人權利，悉由乙方自負法律上責任。
甲方使用乙方交付之履約標的或服務時，致遭第三人主張涉及侵害他人智慧財產權及個人資料保護法或違反資通安全管理法，乙方應協助甲方為必要之答辯及提供相關資料，並負擔甲方因此所生訴訟費、律師費用及其他衍生之費用，並應負相關損害賠償責任。
三、 稽核監督之權利
甲方依據資通安全管理法第9條及資通安全管理法施行細則第4條、個人資料保護法第4條及個人資料保護法施行細則第8條之規定，乙方需有完善之資通安全管理措施及個人資料保護機制，包括個人資料外洩事件之通知程序及採行補救措施，甲方並得隨時稽核監督乙方及其分包廠商，如有發現任何缺失，乙方應無條件配合改善。
四、 資通安全應辦事項
乙方須遵循「資通安全管理法」及相關子法、「個人資料保護法」及其主管機關相關規定並配合甲方 ISMS 規範，提供與協助本系統各項資通安全應辦事項及防護控制措施。

</td>
</tr>
<tr>
<td>保管組財產管理系統
112 年度維護合約招標規範</td>
<td>財產管理系統，招標規範第七條為資安相關規範</td>
</tr>
</table>

[回目錄]

A1.K6 定期辦理全部核心資通系統之業務持續運作演練 (演練情境：機密性、完整性、可用性；單位：計網中心及業管單位聯合演練)

1. 本校依年度總體演練計畫排程表定期辦理業務持續運作演練，以下為 110、111 年度演練計畫排程表。



國立屏東大學

文件編號：ISMS-2-005-T02　安全等級 ：限閱　版次：1.0

110 年度總體演練計畫排程表

日期：1100218

BCP 業務	次序		設備故障	網路中斷	電力中斷			
網路管理（防火牆/IPS 維運管理）	1	P		1100715				
		A		1100803				
校務行政系統維護管理（DB 主機維護）	2	P	1100810					
		A	1100812					
機房管理(電力系統 UPS 維運管理)	3	P			1100722			
		A			1100720			
公務電子郵件系統維運管理	4	P	1100820					
		A	1100819					
	5	P						
		A						
	6	P						
		A						
	7	P						
		A						

資安事件管理小組：　主管：　資安管理代表：

國立屏東大學

文件編號：ISMS-2-005-T02　安全等級 ：限閱　版次：1.0

111 年度總體演練計畫排程表

日期：1110210

BCP 業務	次序		設備故障	網路中斷				
校園網路服務（校園網路骨幹維運管理-核心交換器）	1	P		1110727				
		A		1110726				
校園網路服務(校園網路骨幹維運管理-路由器)	2	P		1110803				
		A		1110809				
校務行政系統維護管理(AP 主機維護)	3	P	1110722					
		A	1110816					
學校首頁網站維運管理	4	P	1110812					
		A	1110812					
	5	P						
		A						
	6	P						
		A						
	7	P						
		A						

資安事件管理小組：　主管：　資安管理代表：

[回目錄]

2. 以下為 111 年度**演練紀錄表**，以 Web 主機設備故障之演練為例

國立屏東大學

文件編號：ISMS-2-005-T03　安全等級：限閱　　版次：1.0

業務永續運作計畫演練紀錄表-設備故障

日期：111.08.16

1.演練狀況：

本中心模擬設備故障，依業務衝擊面來判斷，必須在 13 小時內完成問題確認與復原，確認的設備為 Web 主機。本次演練以模擬與實機進行演練。

2.演練紀錄

2.1 緊急應變作業

時間	111.08.16 -08:30	負責人員	[redacted]
執行單位	處理程序	演練結果	建議事項或改善措施
系統組	確認 Web 應用程式主機或資料庫主機設備故障，經報告資安事件管理小組事件狀況，並填寫資安事件通報暨處理單。	1. 確認 Web 主機硬體故障。 2. 由[redacted]向資安事件管理小組組長報告 Web 主機毀損。 3. 模擬填寫資安事件通報暨處理單。 (30 分鐘)	
緊急搶救小組 資安事件管理小組	判斷事件等級並報告資安管理代表/執行秘書。	1. Web 主機無法正常啟動。 2. 連絡維護廠商檢測支援修復，廠商([redacted])。 3. 通知廠商準備備用設備至校更替。 4. [redacted]與資安事件管理小組討論相關問題。 5. 判斷事件等級 3 級(核心業務運作遭影響或系統停頓，無法於可容忍中斷時間內回復正常運作)，符合啟動條件，通報資安管理代表。 (30 分鐘)	
資安管理代表/ 執行秘書	經確認為第 3、4 級重大資安事項並由資安管理委員會召集人宣布啟動業務永續運作程序	確認為第 3 級重大資安事項，並由資安管理委員會召集人劉英偉副校長 宣布啟動業務永續運作程序。 (10 分鐘)	

1

國立屏東大學

文件編號：ISMS-2-005-T03　安全等級：限閱　　版次：1.0

緊急搶救小組	連絡業務負責人、系統管理員、設備管理員、網路管理員、機房管理員、設備維護廠商會合完畢	[redacted]通知各系統管理員、設備管理員，因校務系統Web主機故障造成校務系統中斷服務，並公告周知。 (10 分鐘)	
緊急搶救小組	• 研判事件原因，必要時聯繫廠商協助資料採證或事件根因分析，將事件及分析結果紀錄於資安事件通報暨處理單 • 設備故障造成關鍵系統無法運作，由主機設備管理員啟動緊急備用作業。 • 通報資安管理代表/執行秘書	1. 由Web主機管理人員[redacted]與緊急搶救小組先確認服務中斷原因並問題研判，其服務中斷原因為Web主機故障(主機板異常)，將事件的處理過程紀錄在資安事件通報暨處理單。 2. 設備管理員[redacted]啟動緊急備用作業。 3. 通報資安管理代表[redacted]主任。 (30 分鐘)	
資安管理代表/執行秘書	回報資安管理委員會召集人執行狀況。	由資安管理代表[redacted](主任)，回報資安管理委員會召集人執行狀況。 (10 分鐘)	

國立屏東大學

文件編號：ISMS-2-005-T03　安全等級：限閱　　版次：1.0

2.2 緊急備用作業（本次演練以狀況二:備用主機無法正常運作，廠商備用設備支援）

執行單位	處理程序	演練結果	建議事項或改善措施
緊急搶救小組 資安事件管理小組	狀況二:備用主機無法正常運作 1. 檢測學校備用主機，發現異常。 2. 廠商備用設備支援 3. 準備 OS、應用程式及 DB 備份檔案 4. 廠商備用設備到校，安裝 OS 及系統環境設定。 5. 進行備用主機測試、更新(1.服務測試(IIS)2.資料庫連線測試) 6. 進行安裝(參考Web應用程式主機安裝手冊、資料庫系統建置手冊) 7. 進行備援設備啟動之測試 8. 回報資安管理代表/執行秘書執行結果。	1. 檢測學校備用主機，發現異常。 2. 廠商設備備品到校支援(故障通知 5 小時) 3. 作業系統及 IIS 安裝設定。 4. 發布最新版應用程式。 5. 系統及資料庫連線帳號權限確認。 6. 掃毒軟體更新。 7. 作業系統更新。 8. 設備上線測試 (1)檢查設備狀態及測試網路。 (2)測試 web 應用程式是否可以對資料庫進行連線。 9. 回報資安管理代表許良政(主任)執行結果。 (8 小時)	
資安管理代表/執行秘書	回報資安管理委員會執行狀況	由資安管理代表[redacted]，向資安管理委員會召集人回報，設備備品已上線，校務系統恢復正常運作。 (10 分鐘)	
緊急搶救小組召集人	召開檢討會議，撰寫報告(重大事故處理報告大綱)；演練時僅填寫演練紀錄表	(略)	

3.演練結果檢討

服務中斷時間	緊急備用作業完成時間	花費時間	RTO	是否符合要求
8:30	18:40	10 小時 10 分	13 小時	符合復原目標時間要求

緊急搶救小組：[redacted]　主管：[redacted]　資安管理代表：[redacted]

3

3. 演練結果提報資安管理委員會，以下為會議紀錄(擷取工作報告有關演練結果部分)。

國立屏東大學 111 年度第 1 次資安管理委員會會議紀錄

時間：中華民國 111 年 8 月 31 日(星期三)下午 2 時 0 分

地點：本校民生校區五育樓四樓第四會議室

主席：劉副校長英偉　　紀錄：魏佑恩

出席委員：(名單如會議通知)

業務單位工作報告：

…

13. 111 年度業務永續運作演練，業依總體演練計畫完成演練，本年度演練項目如下:

(1) 網路中斷-本次演練核心交換器故障復原演練，啟動緊急應變作業、緊急備用作業。本演練結果符合復原目標時間要求(花費時間 9 小時 15 分，符合 RTO:10 小時)。

(2) 網路中斷-本次演練路由器故障復原演練，啟動緊急應變作業、緊急備用作業。本演練結果符合復原目標時間要求(花費時間 8 小時 40 分，符合 RTO:10 小時)。

(3) 設備故障-校務系統 AP 主機設備故障復原演練，啟動緊急應變作業、緊急備用作業。本演練結果符合復原目標時間要求(花費時間 10 小時 10 分，符合 RTO:13 小時)。

(4) 設備故障-學校首頁網站設備故障復原演練(啟用備援系統)，啟動緊急應變作業、緊急備用作業。本演練結果符合復原目標時間要求(花費時間 5 小時，符合 RTO:16 小時)。

［回目錄］

A1.K6 網頁遭竄改納入業務持續運作演練情境

以下為本校網頁如遭竄改時，切換之維護公告頁面示意圖

［回目錄］

A1.K7 ISMS 導入範圍

1.依本校資通安全維護計畫(如下圖，擷取適用範圍部分)，適用範圍為全校所有單位。

國立屏東大學

資通安全維護計畫

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

本計畫適用範圍國立屏東大學（以下簡稱本校）所有單位。

參、 核心業務及重要性

1、 核心業務及重要性

請參閱本校「ISMS-2-005 業務永續運作管理程序書」、「ISMS-2-005-T01-1.0 業務衝擊分析(BIA)表」。

[回目錄]

2.依本校 **ISMS-1-001-T01 適用性聲明書**，驗證範圍為本校全部核心資通系統及重要資訊服務系統，包含校務行政系統(學籍、選課、成績、招生)、電子郵件系統、學校首頁網站及主機房相關網路等基礎設施之管理作業。

國立屏東大學

文件編號：ISMS-1-001-T01　　安全等級：限閱　　版次：2.0

適用性聲明書

表單編號：02　　日期：110年05月20日

驗證範圍：國立屏東大學校務行政系統(學籍、選課、成績、招生)、電子郵件系統、學校首頁網站及主機房相關網路等基礎設施之管理作業。

控制目標		控制措施		適用Y/N	適用/不適用理由	相關參考文件
A.5 安全政策						
A.5.1	安全政策	A.5.1.1	資訊安全政策文件	Y	「資訊安全管理政策」為本中心資訊安全最高指導原則，為確保資訊作業安全能順利運作，需制訂「資訊安全管理政策」並公告週知。	資訊安全管理政策
		A.5.1.2	資訊安全政策之審查	Y	為維持「資訊安全管理政策」適用性及正確性，需定期於「資安管理委員會」管理審查會議中進行檢討修訂。	資訊安全管理政策
A.6 資訊安全的組織						
A.6.1	內部組織	A.6.1.1	資訊安全的角色與責任	Y	為清楚顯示管理階層對資訊安全之責任，特成立資訊安全組並制定相關程序以利執行。	資訊安全組織章程
		A.6.1.2	職務的區隔	Y	為維持資訊安全管理系統於本單位與跨單位運作正常，相互衝突的職務與責任領域加以區隔，以降低組織資產遭未經授權或非故意的修改或誤用之機會。	資訊安全組織章程
		A.6.1.3	與權責機關的聯繫	Y	為確保資訊安全相關事件發生時能立即得到相關之建議或緊急之處理，應與主管機關或消防單位維持適當之聯繫。	資訊安全組織章程
		A.6.1.4	與特殊利害相關團體的聯繫	Y	為取得新技術或相關資訊安全知識，應與資訊安全專家提供資訊安全相關建議。	資訊安全組織章程

第 1 頁，共 12 頁　　適用性聲明書

［回目錄］

3.本校持續通過 ISO 27001 驗證，ISO 驗證範圍為本校全部核心資通系統及重要資訊服務系統，包含校務行政系統(學籍、選課、成績、招生)、電子郵件系統、學校首頁網站及主機房相關網路等基礎設施之管理作業。

afaq

Certificate

Certificat

Certificate of Registration

TTI15219-02

國立屏東大學

驗證範圍：國立屏東大學校務行政系統(學籍、選課、成績、招生)、電子郵件系統、學校首頁網站及主機房相關網路等基礎設施之管理作業。
依據適用性聲明書，版次 2.0，發行日期：110 年 05 月 20 日。

90003 屏東市民生路 4-18 號

之資訊安全管理系統通過艾法諾國際（AFNOR ASIA）之驗證
符合下列國際資訊安全管理系統標準

Information Security Management Systems
ISO/IEC 27001：2013 (CNS 27001：2014)

證書認可日	證書發行日	證書有效日
03-NOV-2015	14-JAN-2022	02-NOV-2024

APPROVED BY

TAF
Management System
Certification
MS012

IAF

Trevor Wilmer
Director for Certification
ON BEHALF OF
AFNOR ASIA

[回目錄]

A1.K8 技術面安全性檢測

1.弱點掃描：本校全部核心資通系統及重要資訊服務系統，每年辦理一次網站安全弱點檢測，111 年度共掃描 22 台伺服主機。下圖為 111 年度**重要資訊主機弱點掃描處理彙整表**，以下擷取核心資通系統(校首頁系統、校務行政系統、電子郵件系統)為例。

111年度重要資訊主機弱點掃描處理彙整表

序號	伺服器名稱	網址/IP	疑似弱點名稱(Vulnerability)	風險等級(高/中/低)	弱點(誤判 OR確定)	處理結果	弱點修補執行(完成)日期	接受風險(無	複測結果	備註(新增配套機制)
1	Rpage校首頁系統		Cross site scripting	高	確定	拒絕不符合規範的輸入，並將其轉換為符合規範的內容。	111/06/16 111/06/24		通過	
			SQL injection	高	確定	拒絕不符合規範的輸入，並將其轉換為符合規範的內容。	111/06/16 111/06/24 111/08/02		通過	
			Application error messages	中	確定	拒絕不符合規範的輸入，並將其轉換為符合規範的內容。	111/06/16 111/06/24		通過	
3	校務系統網站		TLS 1.0 enabled	高	誤判	WAF增加排除TLS1.0	111/08/02 111/08/04			
			TLS 1.1 enabled	中	誤判	WAF增加排除TLS1.1	111/08/02 111/08/04			
			Clickjacking: CSP frame-ancestors missing	低	誤判	web.config 已加入判讀	111/08/02			
			Clickjacking: X-Frame-Options header	低	誤判	web.config 已加入判讀	111/08/02			
5	教職員工電子郵件主機		Clickjacking: X-Frame-Options header	低	確定		111/06/23	接受風險		加強系統監控與紀錄檢視
			TLS/SSL certificate about to expire	低	確定		111/06/23	接受風險		為SSL憑證到期問題，已更新SSL憑證，有效期間為111/07/19-112/08/18。

[回目錄]

2.滲透測試：本校每 2 年辦理一次滲透測試，最近一期為 110 年 7-8 月，委由中華資安辦理。初測結果共有 7 個風險漏洞(2 個高風險、2 個中風險及 3 個低風險)，複測結果已全數成功修補。

<table>
<tr>
<td> 
</td>
<td> 
</td>
</tr>
<tr>
<td>110 年滲透測試初測報告</td>
<td>初測結果有 2 個高風險、2 個中風險</td>
</tr>
<tr>
<td> 
</td>
<td> 
</td>
</tr>
<tr>
<td>110 年滲透測試複測報告</td>
<td>複測結果 0 個風險(已修補完畢)</td>
</tr>
</table>

［回目錄］

3.資安健診：本校每 2 年辦理一次資安健診，最近一期為 111 年 7-8 月，委由中華資安辦理。以下為 111 年度**資安健診處理結果彙整表**，針對健診檢測各項事項處理彙整表。

國立屏東大學111年資安健診-處理結果彙整表

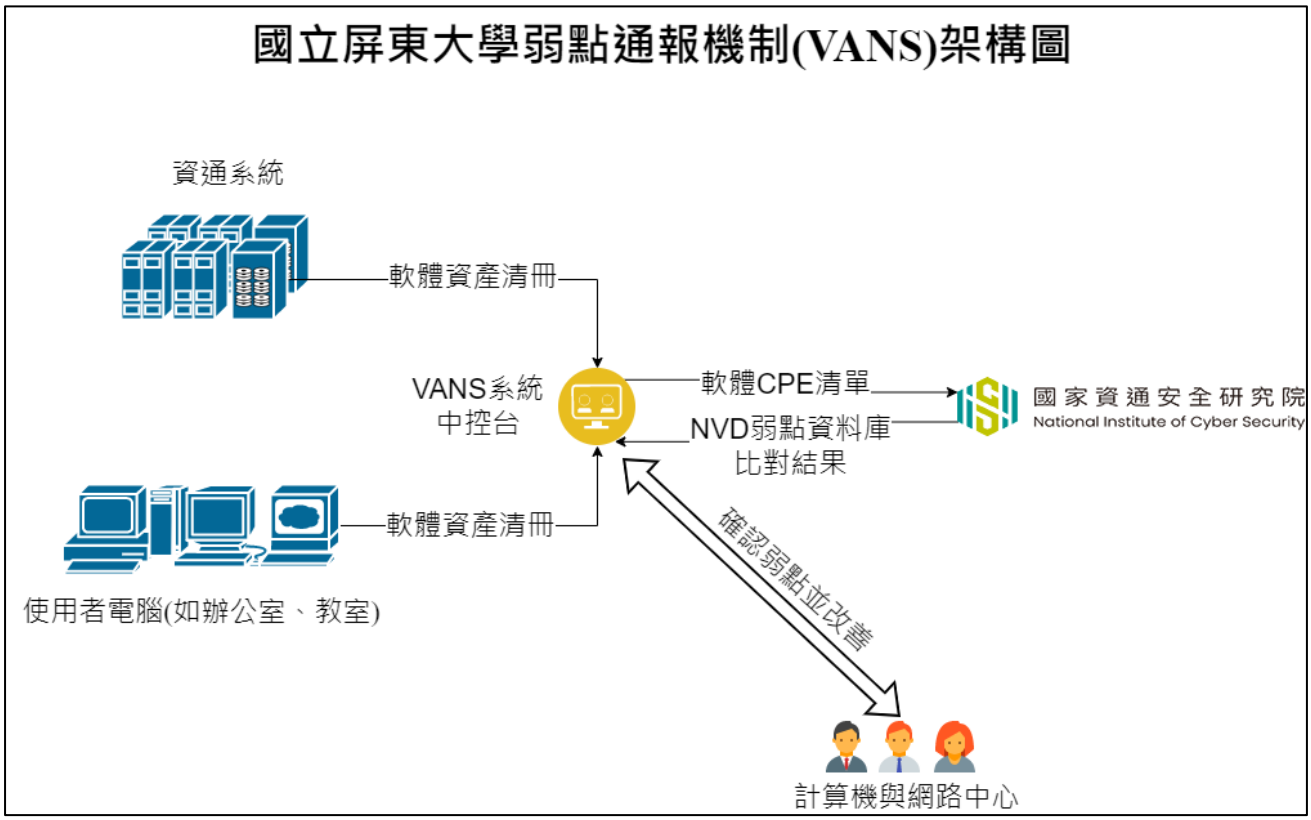
1110831

序號	檢測事項	事件說明	風險等級	處理結果	後續追蹤
網路架構檢視-備援機制設計檢視					
1	防火牆與Core Switch未規劃HA機制	若網路設備發生障礙易造成服務中斷	低風險	考量建置成本及已簽訂維護合約，可於復原目標時間(RTO)完成，接受此風險。	
網路架構檢視-網路存取管控檢視					
1	Server主機[redacted]未限制Internet連線	可能會增加感染惡意程式或被當跳板風險	低風險	為資安考量及避免誤擋封包，除必要更新外，將逐步限縮對Internet 連線。	
網路惡意活動檢視(有線)-資安設備紀錄檔分析，側錄位置[redacted] (側錄時間:111/07/06~111/07/07)					
1	無異常行為，但有發現一定數量的遠端作業([redacted])連線行為，此類工具易遭駭客作為主機滲透後遠端操控使用，建議進行限縮管制(原則禁止、例外許可)	無異常主機		為考量資通安全與教學需求，本校目前階段僅關閉伺服器及行政區域網段遠端控制軟體連線服務；為資通安全考量將評估逐步禁止(限縮管制)遠端控制軟體連線。	
使用者端電腦惡意活動檢視(檢測日期:111/07/06)					
1	作業系統更新 Office應用程式更新 防毒軟體更新 Adobe Reader更新 Adobe Flash Player更新 Java更新 作業系統是否停止支援 Office應用程式是否停止支援 惡意程式	檢測43台PC，發現異常事件如下 作業系統未更新:0件 Office應用程式未更新:0件 防毒軟體未更新:0件 Adobe Reader未更新:5件 Adobe Flash Player未更新:0件 Java未更新:2件 作業系統停止支援:0件 Office應用程式停止支援:4件 惡意程式:0件 (詳細請參閱附件一_3)		1.使用者PC已由業管人員或駐校工程師協助更新或移除完成。[redacted]	
伺服器主機檢視(檢測日期:111/07/06)					
1	作業系統更新 Office應用程式更新 防毒軟體更新 Adobe Reader更新 Adobe Flash Player更新 Java更新 作業系統是否停止支援 Office應用程式是否停止支援 惡意程式	檢測23台伺服器主機，發現異常事件如下 作業系統未更新:0件 Office應用程式未更新:0件 防毒軟體未更新:0件 Adobe Reader未更新:0件 Adobe Flash Player未更新:1件 Java未更新:4件 作業系統停止支援:0件 Office應用程式停止支援:3件 惡意程式:0件 (詳細請參閱附件一_4)		1.伺服器主機已由業管單位人員協助更新或移除完成。	

4.逐步全校導入資安弱點通報機制(VANS)，目前持續測試架構

目前本校針對各 VANS 產品或國家資通安全研究院(原技服中心)所開發的工具進行測試評估，衡量各產品所需建置經費與人力。預計以功能性、可用性及系統安全三個面向作為考量，評估是否能正確蒐集與比對資訊資產、是否支援資產的風險評估與修補、使用流程的順暢性與穩定性，系統是否有足夠的安全防護措施。

以下是本校 VANS 架構。



［回目錄］

A1.K9 核心系統持續通過 ISO27001 驗證

本校目前為資通安全等級 C 級機關，以下為本校 **ISO 27001 證書**，核心資通系統納入驗證範圍。

afaq

Certificate

Certificat

Certificate of Registration

TTI15219-02

國立屏東大學

驗證範圍：國立屏東大學校務行政系統(學籍、選課、成績、招生)、電子郵件系統、學校首頁網站及主機房相關網路等基礎設施之管理作業。
依據適用性聲明書，版次 2.0，發行日期：110 年 05 月 20 日。

90003 屏東市民生路 4-18 號

之資訊安全管理系統通過艾法諾國際（AFNOR ASIA）之驗證
符合下列國際資訊安全管理系統標準

Information Security Management Systems
ISO/IEC 27001：2013 (CNS 27001：2014)

證書認可日	證書發行日	證書有效日
03-NOV-2015	14-JAN-2022	02-NOV-2024

APPROVED BY

TAF
Management System
Certification
MS012

IAF

Trevor Wilmer
Director for Certification
ON BEHALF OF
AFNOR ASIA

［回目錄］

A2 強化學校人員資通安全認知與訓練

A2.K1 配置資通安全專職人員 1 名

本校因現有人力不足，目前以正職人員兼辦資通安全業務，承辦人員皆取得專業證照及職能證書，且維持其有效性；為符合資通安全法規定，健全本校資通安全組織架構，將配置資通安全專職人員，並增聘任專案人員協助辦理 ISMS 業務。

姓名	魏佑恩
職稱	技士
業務職掌	1.校園網路規劃、管理與維護(屏商校區)。 2.宿舍網路規劃、管理(屏商校區)。 3.教職員工E-mail、FTP、DNS等伺服器管理維護。 4.資訊安全管理系統（ISMS）維運。 5.個資法綜合業務。 6.校園網路智慧財產權管理。 7.校園資安防治與資安回報。 8.機房管理與維護(屏商校區)。 9.其他臨時交辦事項
聯絡方式	分機21302 yuen@mail.nptu.edu.tw

[回目錄]

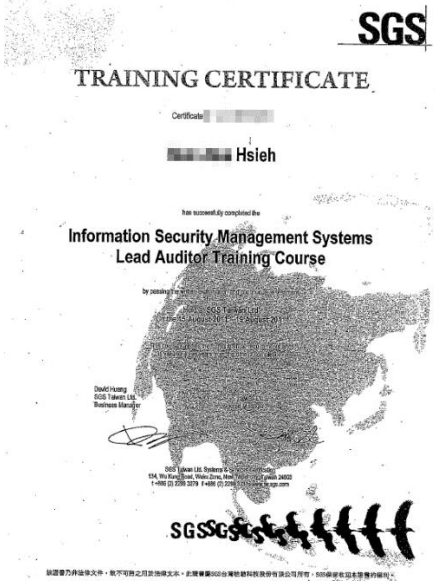
A2.K2 資通安全專職人員暨資訊人員資安專業證照、資安職能訓練證書

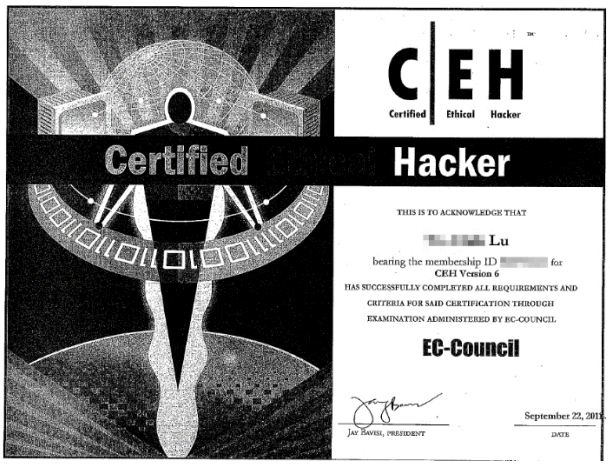
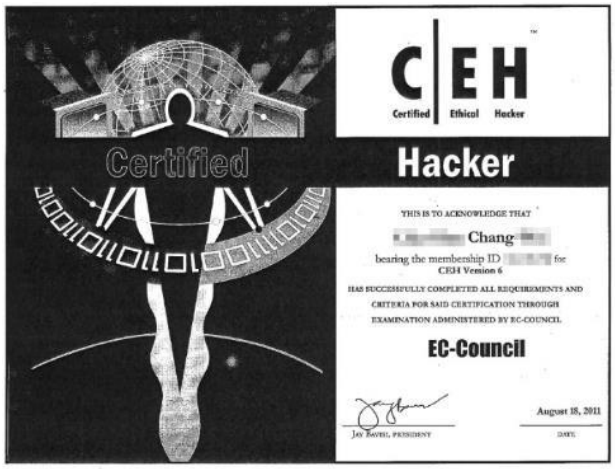
本校資安(訊)專業人員皆積極取得相關資通安全專業證照及資通安全職能訓練，以下為證照(證書)。

本校資安(訊)專業人員證照(證書)

姓名	職稱(務)	證照(證書)
魏○○	資安人員、網路管理	ISO 27001:2013 LA 安全系統發展生命週期.NET 職能評量證書 Web 應用程式安全職能評量證書
盧○○	資安人員、網路管理	ISO 27001:2013 LA CEH(Certified Ethical Hacker) 資安健診職能評量證書
朱○○	資安人員、網路管理	ISO 27001:2013 LA 安全系統發展生命週期.NET 職能評量證書
謝○○	資訊人員	ISO 27001:2013 LA
吳○○	資訊人員	Web 應用程式安全職能評量證書、行動裝置安全職能評量證書
張○○	資訊人員	CEH(Certified Ethical Hacker)
曹○○	資訊人員	Web 應用程式安全職能評量證書
顏○○	資訊人員	政府資訊作業委外安全管理職能評量證書

以下為本校計算機網路中心人員(資安專職人員暨資訊人員)資通安全專業證照

	
ISO 27001 LA(魏先生)	ISO 27001 LA(盧先生)
	
ISO 27001 LA(朱先生)	ISO 27001 LA(謝先生)

	
CEH(盧先生)	CEH(張先生)

以下為本校計算機網路中心人員(資安專職人員暨資訊人員)資安職能評量證書

	
安全系統發展生命週期(.Net)(魏先生)	資安健診(盧先生)
	
Web 應用程式安全(魏先生)	安全系統發展生命週期(.Net)(朱先生)

	
政府資訊作業委外安全管理(顏先生)	行動裝置安全(曹先生)
	
Web 應用程式安全(吳先生)	行動裝置安全(吳先生)

[回目錄]

A2.K2 資通安全專責人員以外之資訊人員完成資通安全專業課程教育訓練

本校持續維持資訊人員每 2 年完成 3 小時以上資通安全專業課程教育訓練，以下截取 2 位同仁資通安全專業課程學習時數供參考。

[redacted] 111 年度學習時數資料

點選列印

通過總學習時數	98 小時
數位課程總學習時數	80 小時
實體課程總學習時數	9 小時
混成課程總學習時數	0 小時
遠距課程總學習時數	9 小時
自行申請公假學習總時數	0 小時
與業務相關總學習時數	55 小時
性別主流化基礎課程類學習總時數	1 小時
性別主流化進階課程類學習總時數	6 小時
每年必須完成之課程總學習時數(10小時)	21 小時
當前政府重大政策(1小時)	1 小時
環境教育(4小時)	8 小時
性別主流化、廉政與服務倫理、人權教育、行政中立、多元族群文化、公民參與(5小時)	12 小時

課程名稱	期別	學習機關(構)	上課期間	時數	服務機關	職稱	官職等	假別	學習類別	業務相關
環境風水師的防災妙計	111	行政院人事行政總處公務人力發展學院	起: 1110101 迄: 1111231 登: 1110903	1 小時	國立屏東大學	[redacted]	[redacted]		[redacted]	
政府資訊委外安全	111	行政院人事行政總處公務人力發展學院	起: 1110614 迄: 1111231 登: 1110617	6 小時 (專業)	國立屏東大學	[redacted]	[redacted]		[redacted]	
網站應用程式安全	111	行政院人事行政總處公務人力發展學院	起: 1110415 迄: 1111231 登: 1110901	5 小時	國立屏東大學	[redacted]	[redacted]		[redacted]	

[redacted]111 年度學習時數資料

點選列印

通過總學習時數	63 小時
數位課程總學習時數	40 小時
實體課程總學習時數	7 小時
混成課程總學習時數	0 小時
遠距課程總學習時數	16 小時
自行申請公假學習總時數	0 小時
與業務相關總學習時數	36 小時
性別主流化基礎課程類學習總時數	0 小時
性別主流化進階課程類學習總時數	3 小時
每年必須完成之課程總學習時數(10小時)	12 小時
當前政府重大政策(1小時)	1 小時
環境教育(4小時)	4 小時
性別主流化、廉政與服務倫理、人權教育、行政中立、多元族群文化、公民參與(5小時)	7 小時

課程名稱	期別	學習機關(構)	上課期間	時數	服務機關	職稱	官職等	假別	學習類別	業務相關
政府資訊委外安全	111	行政院人事行政總處公務人力發展學院	起: 1110614 迄: 1111231 登: 1110617	6 小時	國立屏東大學	[redacted]	[redacted]		[redacted]	
網站應用程式安全	111	行政院人事行政總處公務人力發展學院	起: 1110415 迄: 1111231 登: 1110901	5 小時	國立屏東大學	[redacted]	[redacted]		[redacted]	
產業創新計畫-行政院人事行政總處公務人力發展學院提供	111	臺北市政府公務人員訓練處	起: 1110101 迄: 1111231 登: 1110505	1 小時	國立屏東大學	[redacted]	[redacted]		[redacted]	
[環境教育]認識蔬菜分類及繁殖技巧	111	臺北市政府公務人員訓練處	起: 1110101 迄: 1111231 登: 1110511	2 小時	國立屏東大學	[redacted]	[redacted]		[redacted]	
[性別主流化]運動與性別議題 - 運動最美	111	臺北市政府公務人員訓練處	起: 1110101 迄: 1111231 登: 1110506	3 小時	國立屏東大學	[redacted]	[redacted]		[redacted]	
基礎台語好好學(一)	111	臺北市政府公務人員訓練處	起: 1110101 迄: 1111231 登: 1110511	3 小時	國立屏東大學	[redacted]	[redacted]		[redacted]	
廉政三護，阻斷圖利-法務部廉政署提供	111	臺北市政府公務人員訓練處	起: 1110101 迄: 1111231 登: 1110506	1 小時	國立屏東大學	[redacted]	[redacted]		[redacted]	
111年度教育體系資安專業訓練課程-資安事件通報與應變	1	國立中山大學	起: 1110610 迄: 1110610 登: 1110613	5 小時	國立屏東大學	[redacted]	[redacted]		[redacted]	
		[redacted]	起: 1110101							

［回目錄］

A2.K3 每年辦理資通安全通識教育訓練 3 小時課程

本校 111 年度共辦理 3 場次資通安全通識教育訓練(3/31、5/20、6/2)供全校教職員工同仁研習，並將課程製作為數位課程供當日因公不克出席同仁學習。以下為本校數位學習網站相關課程擷圖。

A3 確保資通系統管理量能

A3.K1 資通系統集中化管理

本校各單位網站，均集中建置於統一平台(R-Page)，以下為本校**<u>各單位網址清單</u>**截圖。

首頁 / RPAGE建置與維護 / 各單位網址清單

網站負責人若有異動，請填寫 此表單回報

行政單位

序號	網站名稱	RPAGE網址	網站負責人	Email	分機	備註
E001	校首頁	www.nptu.edu.tw	吳			
E002	校首頁英文版	eng.nptu.edu.tw	吳			
E003	校長室	president.nptu.edu.tw	謝			
E004	副校長室	vicepresident.nptu.edu.tw	劉			
E005	秘書室	secretary.nptu.edu.tw	萬			
E006	校務研究辦公室	iro.nptu.edu.tw	林			
E007	性別平等教育委員會	geec.nptu.edu.tw	郭			
E008	教務處	oaa.nptu.edu.tw	吳 黃			

學術單位

序號	網站名稱	RPAGE網址	網站負責人	Email	分機	備註
E055	大武山學院	dawu.nptu.edu.tw				
E054	博雅教育中心	gec.nptu.edu.tw				
E056	共同教育中心	geccce.nptu.edu.tw				
E057	跨領域學程中心	cis.nptu.edu.tw				
E058	EMI發展中心	emi.nptu.edu.tw				
E131	大武山社會實踐暨永續發展中心	usr.nptu.edu.tw				
E154	新媒體創意應用碩士學位學程	nm.nptu.edu.tw				
E059	師資培育中心	cte.nptu.edu.tw				
E060	管理學院	ccm.nptu.edu.tw				
E061	商業自動化與管理學系	cam.nptu.edu.tw				
E062	行銷與流通管理學系	mdm.nptu.edu.tw				
E063	休閒事業經營學系	leisure.nptu.edu.tw				
E064	不動產經營學系	rem.nptu.edu.tw				
E065	企業管理學系	mba.nptu.edu.tw				
E066	國際貿易學系	business.nptu.edu.tw				

[回目錄]

A3.K1 行政用伺服器(或 VM)統一集中管理

1.本校設有雲端虛擬主機服務管理要點，提供校內需求單位依規定申請新增虛擬主機，以下為**雲端虛擬主機服務管理要點。**

國立屏東大學雲端虛擬主機服務管理要點

107 年 7 月 19 日本校第 42 次行政會議審議通過

一、本校計算機與網路中心（以下簡稱計網中心）為支援教師教學研究與校務行政業務執行所需，提供虛擬主機申請服務，特訂定「國立屏東大學雲端虛擬主機服務管理要點」（以下簡稱本要點）。

二、適用單位與用途：

(一)學術單位之教學研究。

(二)行政單位需資訊化之校務行政工作。

三、申請與使用期限：

(一)申請人須為課程之授課教師或校務行政工作承辦人員。

(二)申請人需填寫虛擬主機申請單，送至計網中心系統組辦理，經審核同意後，始得提供服務使用。

(三)教學用途每次申請使用期限以一年為限；校務行政用途期限，以申請起迄時間為原則。

四、服務延續與終止：

(一)如欲延續本服務時，應於服務終止日前一星期，重新提出申請，經審核同意後得延續服務。服務屆滿且未再提出服務延續之申請，視為自動終止服務。

(二)提前終止服務，須於預定終止日前一星期，提出書面申請；申請者如有違反本要點第五點第一項第一款相關規範時，計網中心得即時中斷系統服務。

五、虛擬主機維護管理

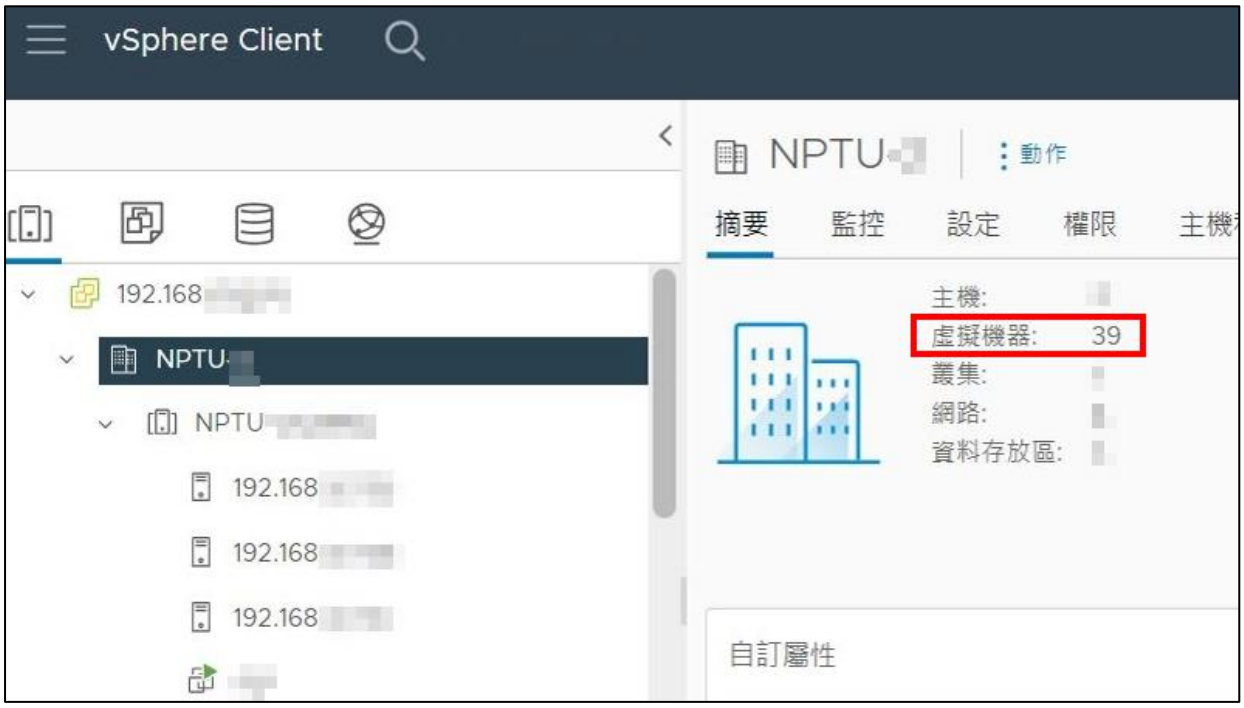
(一)申請人對所提供之虛擬主機應配合計網中心資訊安全管理系統(ISMS)相關規定進行管理，並遵守本校「校園網路管理規範」、「校園伺服器管理要點」及相關資訊法規。

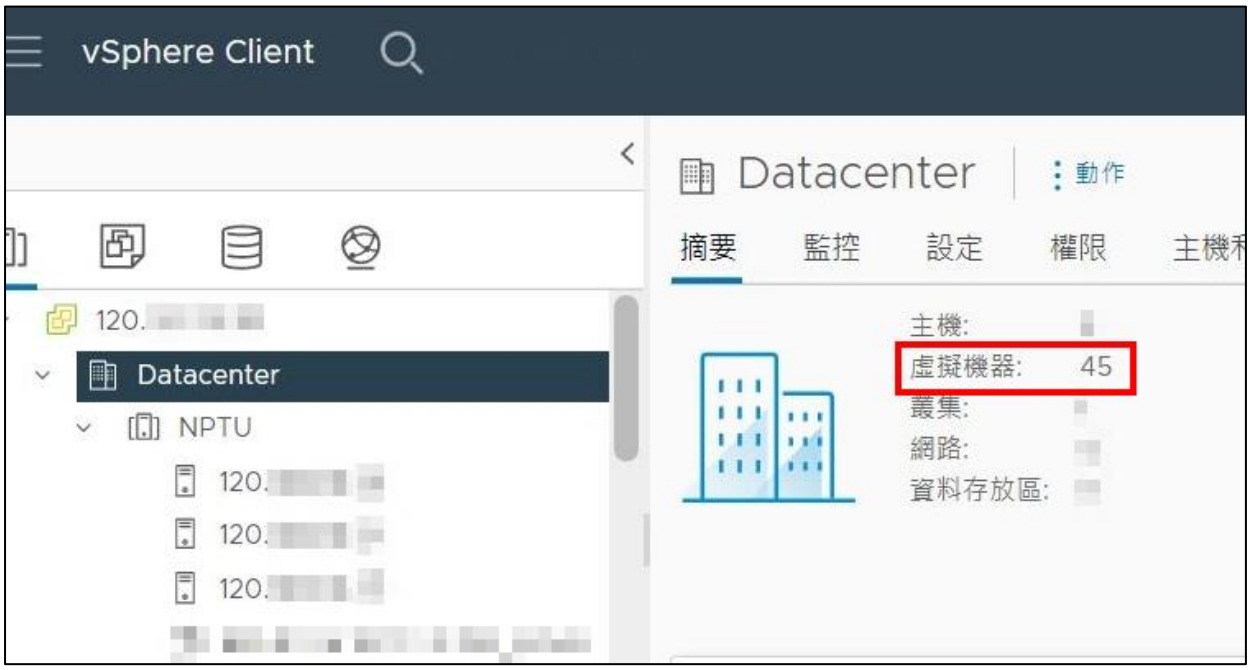
(二)申請人須提供作業系統軟體合法授權證明交計網中心備查後，由計網中心協助安裝完成。

(三)虛擬主機資料備份、應用軟體設定及系統安全維護機制由申請人自行

［回目錄］

2. 以下為**虛擬主機管理平台(VMware vCenter)實際畫面**，可提供完善的安全實體環境，分別為支援**行政單位**各類資訊系統之環境，以及提供**學術單位**教學研究測試之環境，並規劃專屬網段，提升系統與設備安全性；目前共有 84 台虛擬主機納入虛擬環境。

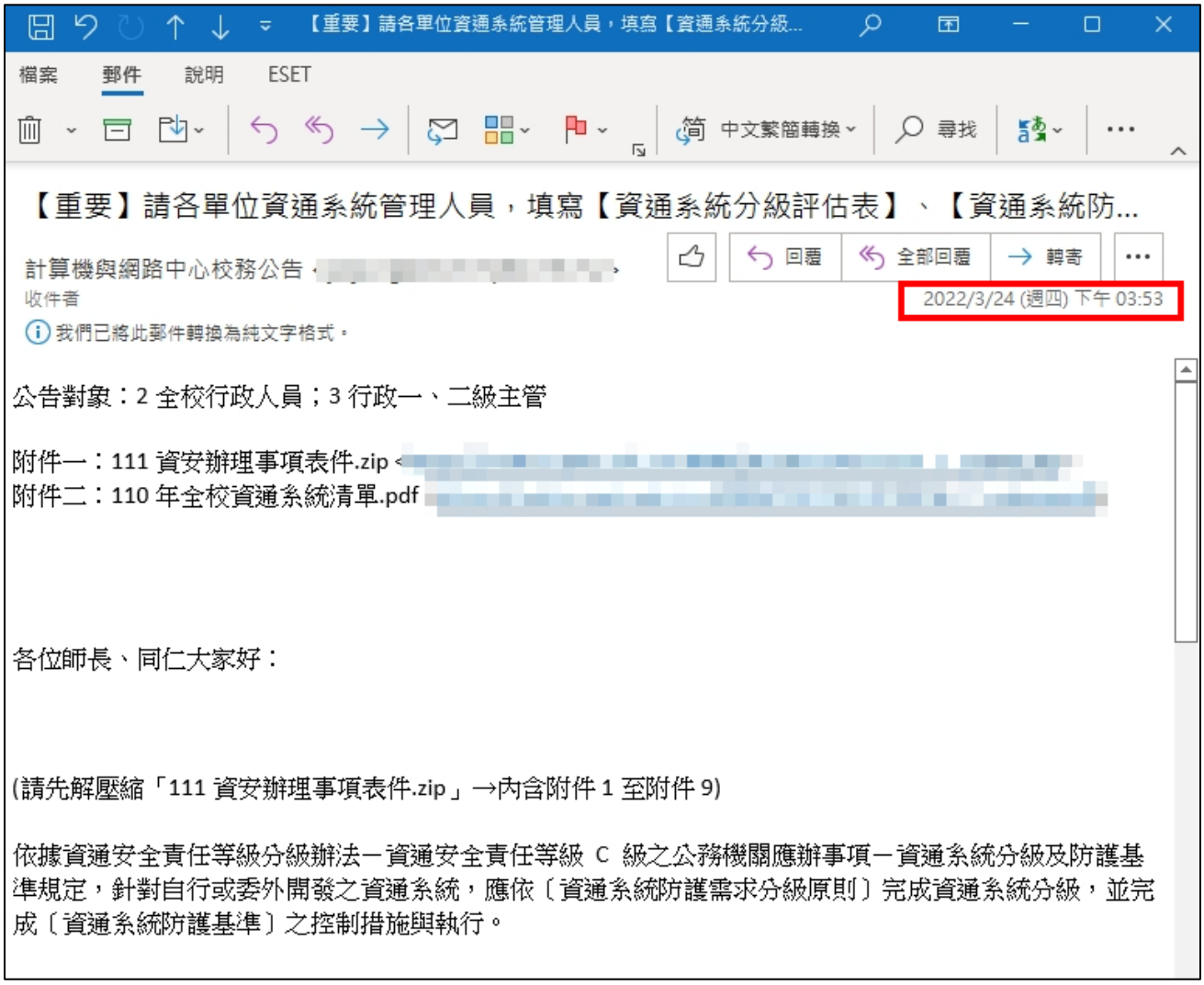




[回目錄]

A3.K2 每年檢視校內閒置或一次性活動網站，依需求下架或限制存取

本校每年依規定盤點全校資通系統，並請資通系統業管單位依防護需求分級原則填寫分級評估表，如有校內閒置或一次性活動網站則下架或限制存取，以下為 111 年 3 月 24 日**調查盤點資通系統 mail**。


【重要】請各單位資通系統管理人員，填寫【資通系統分級...

檔案 郵件 說明 ESET

中文繁簡轉換 尋找

【重要】請各單位資通系統管理人員，填寫【資通系統分級評估表】、【資通系統防...

計算機與網路中心校務公告 [redacted]

回覆 全部回覆 轉寄

收件者

2022/3/24 (週四) 下午 03:53

我們已將此郵件轉換為純文字格式。

公告對象：2 全校行政人員；3 行政一、二級主管

附件一：111 資安辦理事項表件.zip [redacted]

附件二：110 年全校資通系統清單.pdf [redacted]

各位師長、同仁大家好：

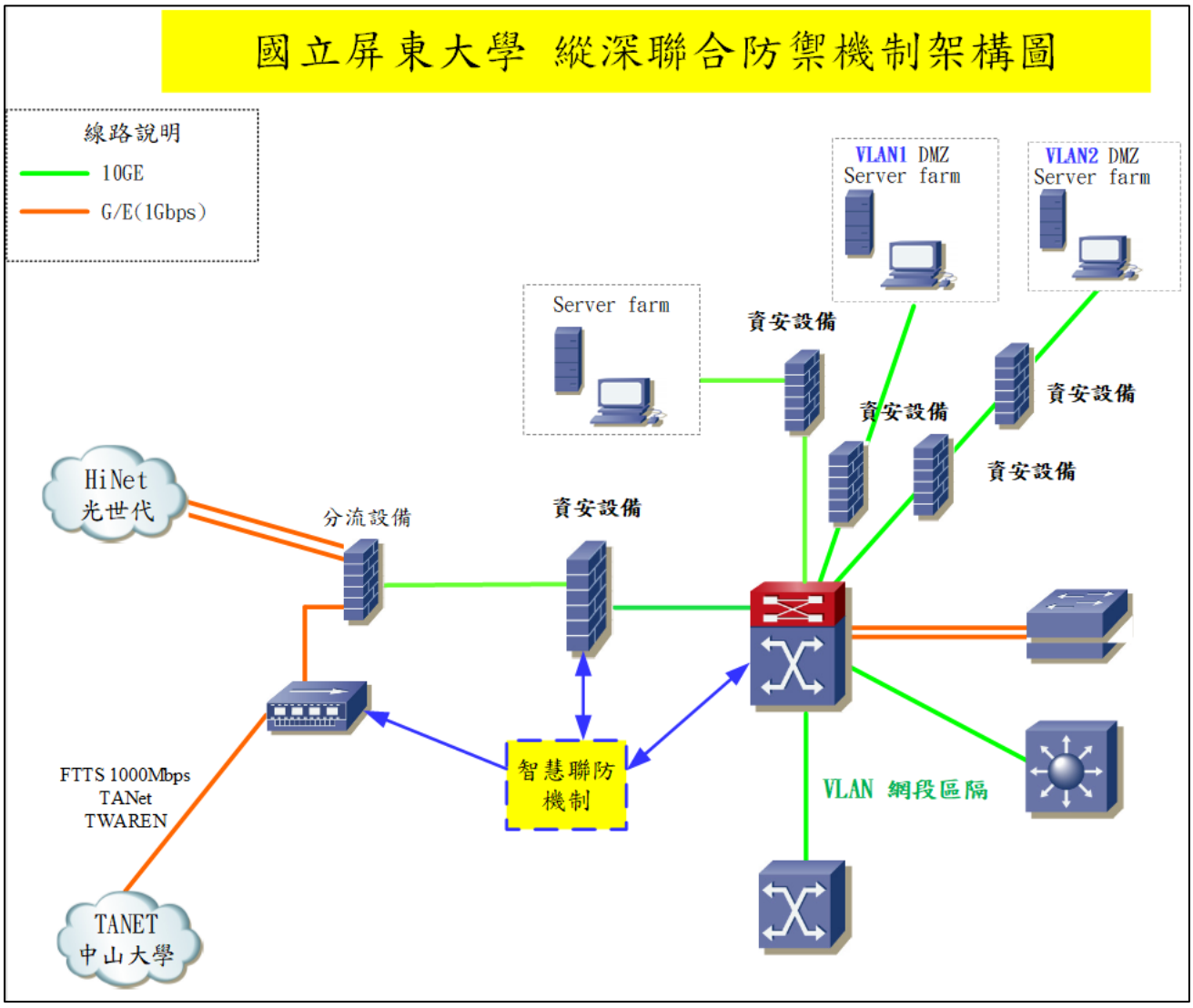
(請先解壓縮「111 資安辦理事項表件.zip」→內含附件 1 至附件 9)

依據資通安全責任等級分級辦法－資通安全責任等級 C 級之公務機關應辦事項－資通系統分級及防護基準規定，針對自行或委外開發之資通系統，應依〔資通系統防護需求分級原則〕完成資通系統分級，並完成〔資通系統防護基準〕之控制措施與執行。

［回目錄］

A3.K3 建置網路縱深防禦機制

本校目前藉由多台資安設備，針對不同網段不同需求，配置有防火牆、負載分流設備、應用程式防火牆 WAF、log 分析系統等多層防禦，建置全校網路縱深防禦機制，惟網路攻擊能量日趨增強，部分設備效能逐漸不堪負荷，急需更新升級已維護完善的校園資安防護網。

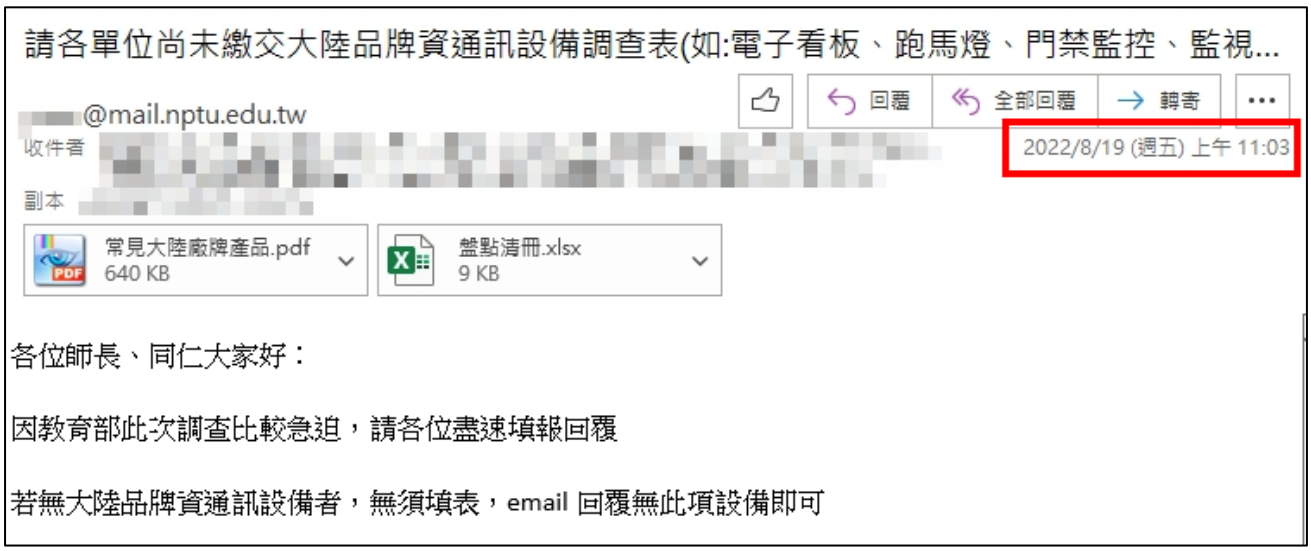


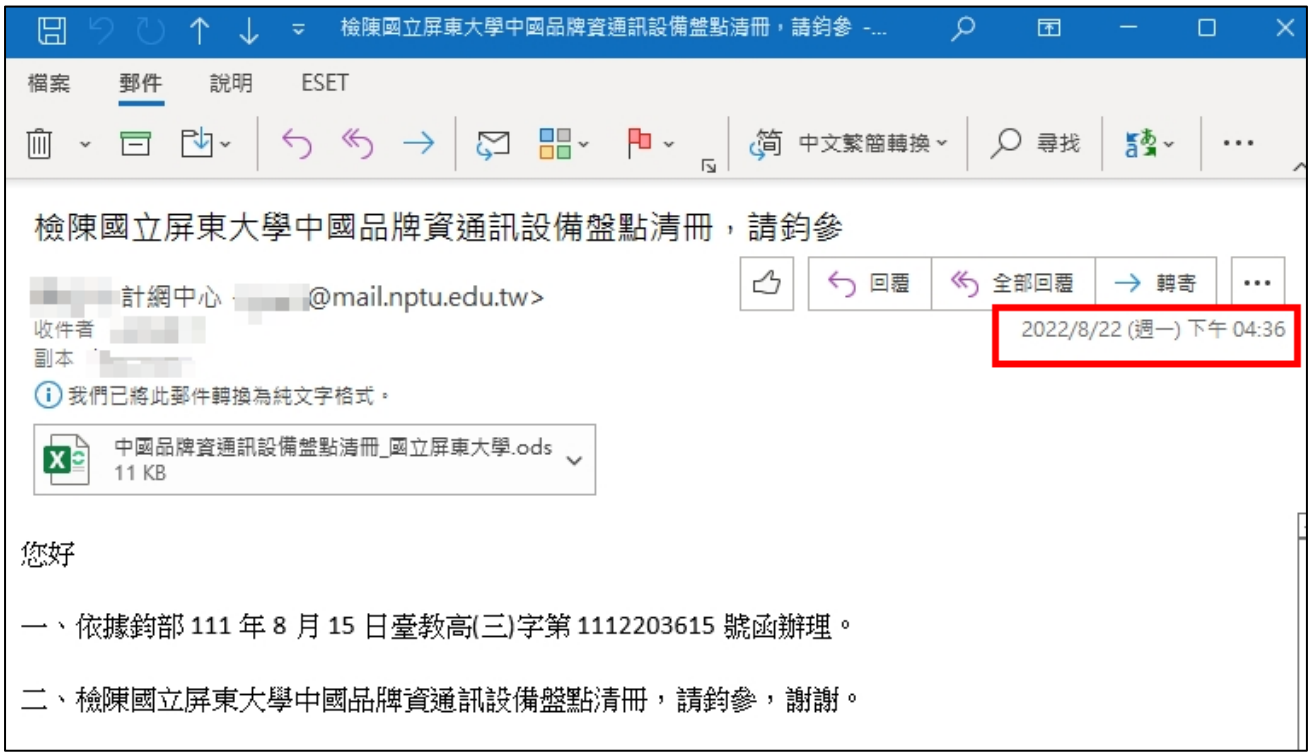
［回目錄］

A4 落實管理危害國家資通安全產品

A4.K1 每年定期調查 1 次大陸廠牌資通訊產品

本校依規定每年進行 1 次大陸廠牌資通訊產品調查，下面為 **2022/8/19 調查大陸廠牌 mail**，及 **8/22 檢陳清冊至教育部之 mail**。





[回目錄]

A4.K1 列管已使用大陸廠牌之單位盡速汰換或停用

本校每年盤點後之大陸品牌資通訊設備清冊如下，擷取部分內容為例，均依規定停止與公務環境介接並列管在案，俟報廢年限後依規定進行設備報廢。

中國品牌資通訊設備盤點清冊

注意事項：
1.盤點說明：機關使用中國廠牌資通訊產品。
2.盤點範圍：本機關場域及出租場域 (出租場域應於契約內納入相關限制使用要求)。
3.盤點品項：含電子看板、跑馬燈、門禁監控、監視器等；類別包含：硬體、軟體及韌體。
4.使用中之中國廠牌資通訊產品，因存有潛在的資安風險，請儘速規劃替代方案或汰換。

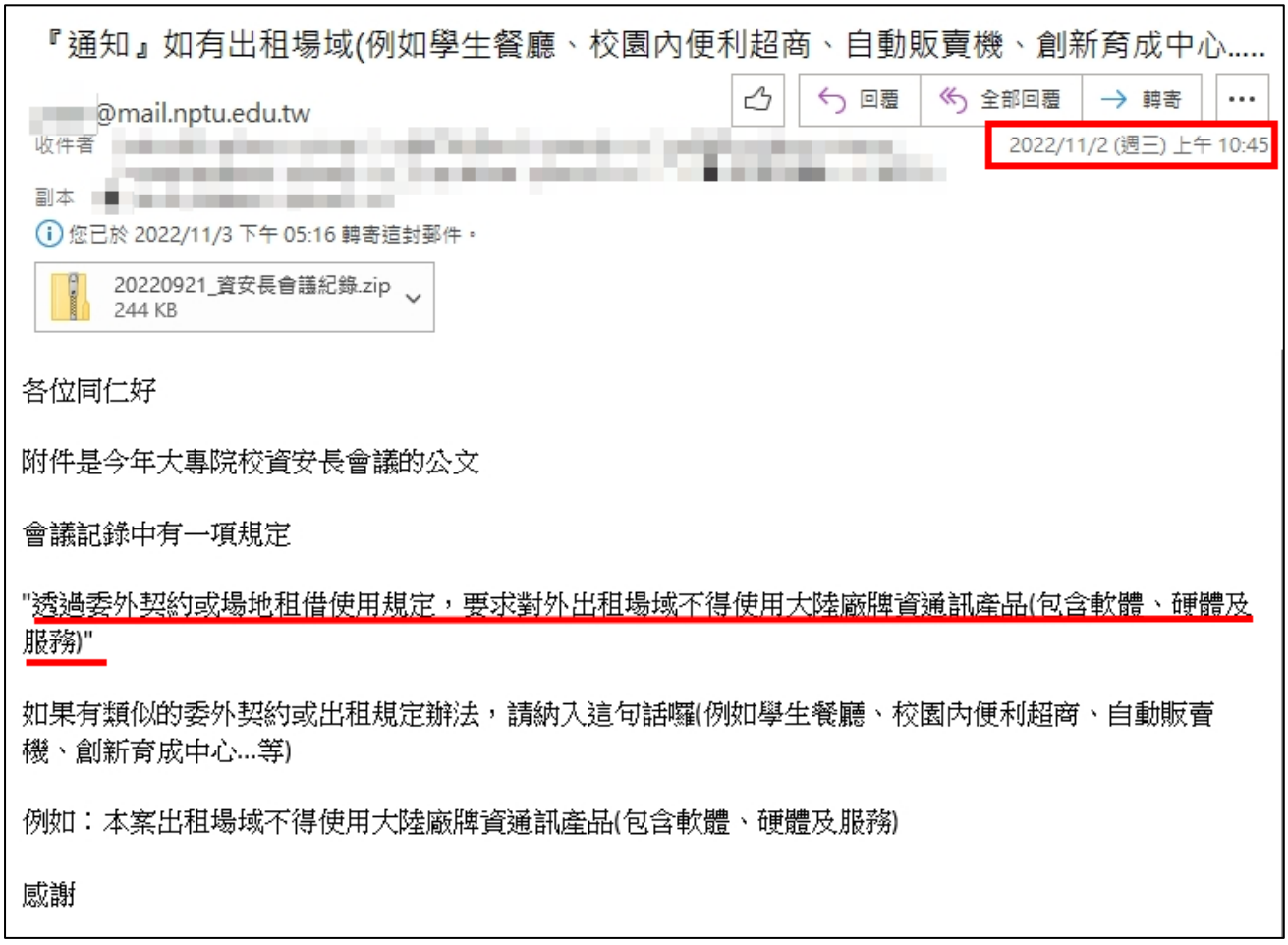
校名：國立屏東大學

填表人姓名/單位：[redacted]計算機與網路中心　　電子信箱：[redacted]@mail.nptu.edu.tw　　連絡電話：[redacted]

項次	單位名稱	類別	廠牌名稱(全銜)	資通訊產品名稱	產品型號或版本	是否使用中	是否委外標案(含分包項目)產品	委外標案(含分包項目)是否有陸籍人員	委外標案名稱	委外或分包學校/廠商名稱	尚未汰換原因(請敘明原因或正當理由)	預計汰換時間(年/月/日)	目前是否與公務環境介接	汰換前配套措施或相關作為(含緊急應變措施)	汰換前配套措施或相關作為-其他說明	備註
1	[redacted]	硬體	[redacted]	四核平板	[redacted]	否	否	否	無	無	未與公務設備連結	111/8/31 (已申請報	否	停止與公務環境介接	未與公務設備連結	
2	[redacted]	硬體	[redacted]	空拍機	[redacted]	否	否	否	無	無	僅供外型展示與機構教學	113/12/31	否	無法開機僅供展示教學	無法開機僅供展示教學	
3	[redacted]	硬體	[redacted]	大型空拍機	[redacted]	否	否	否	無	無	僅供外型展示與機構教學	113/12/31	否	無法開機僅供展示教學	無法開機僅供展示教學	
4	[redacted]	硬體	[redacted]	空拍相機	[redacted]	否	否	否	無	無	僅供外型展示與機構教學	113/12/31	否	無法開機僅供展示教學	無法開機僅供展示教學	
5	[redacted]	硬體	[redacted]	筆記型電腦	[redacted]	否	否	否	無	無	無法開機使用預計報廢	111.12.31 報廢	否	無法開機使用預計報廢	無法開機使用預計報廢	
6	[redacted]	硬體	[redacted]	空氣清淨機	[redacted]	否	否	否	無	無	未與公務設備連結	111/12/31	否	停止與公務環境介接	未與公務影像設備連結	
7	[redacted]	硬體	[redacted]	筆記型電腦	[redacted]	否	否	否	無	無	報廢年限未到	111/12/31	否	停止與公務環境介接	未與公務影像設備連結	
8	[redacted]	硬體	[redacted]	筆記型電腦	[redacted]	否	否	否	無	無	報廢年限未到	111/12/31	否	停止與公務環境介接	未與公務影像設備連結	
9	[redacted]	硬體	[redacted]	伺服器	[redacted]	否	否	否	無	無	因應資料轉移及儲存等因素，暫	114/12/31	否	停止與公務環境介接	未與公務影像設備連結	
10	[redacted]	硬體	[redacted]	空氣清淨機	[redacted]	否	否	否	無	無	未與公務設備連結	111/12/31	否	停止與公務環境介接	未與公務影像設備連結	
11	[redacted]	硬體	[redacted]	筆記型電腦	[redacted]	否	否	否	無	無	報廢年限未到	112/12/31	否	停止與公務環境介接	未與公務影像設備連結	

A4.K2 學校新簽訂委外契約內，明訂不得使用大陸廠牌資通訊產品

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危害國家資安之產品，相關規定於 11/2 日 mail 並電話通知相關單位，亦公告於學校網站。以下為 mail 公告及學校網站公告訊息。



『通知』如有出租場域(例如學生餐廳、校園內便利超商、自動販賣機、創新育成中心.....

[redacted]@mail.nptu.edu.tw

回覆 全部回覆 轉寄 ...

收件者 [redacted] 2022/11/2 (週三) 上午 10:45

副本 [redacted]

您已於 2022/11/3 下午 05:16 轉寄這封郵件。

20220921_資安長會議紀錄.zip
244 KB

各位同仁好

附件是今年大專院校資安長會議的公文

會議記錄中有一項規定

"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(包含軟體、硬體及服務)"

如果有類似的委外契約或出租規定辦法，請納入這句話囉(例如學生餐廳、校園內便利超商、自動販賣機、創新育成中心...等)

例如：本案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)

感謝

國立屏東大學 National Pingtung University 計算機與網路中心 Computer and Network Center

回首頁(另開新視窗) 網站地圖 校首頁 中文 EN

首頁 / 最新消息

【資安訊息】轉知111年全國大專校院資安長會議紀錄，請各單位依會議紀錄辦理

會議結論如下，請各單位依會議紀錄規定辦理

(一)學校所轄管系統網站內容遭竄改時，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(Business Continuity Plan, BCP)演練情境。

(二)落實盤點全校物聯網設備，採取適當管控機制，如連線控管、變更預設帳密、修補漏洞等，以強化資安防護作為。

(三)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(包含軟體、硬體及服務)。

(四)落實「國立大專校院資通安全維護作業指引」，私立大專校院得參照辦理，強化資安事件應變機制及相關防護措施。

瀏覽數: 352

友善列印

［回目錄］

2.本校各單位簽辦資通系統委外合約時，由計算機與網路中心協助檢視其中資安規範，規範中包含不得使用大陸廠牌資通訊產品，以下是文書組**電子公文系統維護合約**及計算機與網路中心**全校電腦硬體暨網路設備維護合約**為例，擷取其中資安相關規範。

<table>
<tr>
<td>
國立屏東大學
「112 年度電子公文線上簽核系統維護」招標規範
一、維護目的：
維持本校電子公文線上簽核系統之正常運作，並接受系統使用者之操作諮詢服務、系統作業功能項目之增修事項及諮詢服務，以利業務之順利進行及推展。
二、維護標的物：
「電子公文線上簽核系統」(以下簡稱本系統)係指本校現使用 [redacted] 電子公文線上簽核系統及其相關附屬程式之所有內容。
三、維護期間：自 112 年 1 月 1 日起至 112 年 12 月 31 日止。
四、維護項目及需求：
(一)系統管理：
1. 視系統運轉狀況不定期實施系統效能調校，調整資料庫索引值，以確保本系統之正常運轉。
2. 異常狀況之診斷、系統故障排除。
3. 維護期間內若伺服主機、資料庫需異動或需建立備援主機時(相關軟、硬體由機關提供)，免費提供系統資料庫移機或建立備援主機服務(以上免費服務以 1 次為限)，並維持資料之完整性。
4. 系統備份相關軟硬體由本校提供，廠商須協助以下設定：
(1)每日系統備份設定。
(2)定期系統異地備份設定。
5. 配合機關需求進行災害復原演練，以驗證備份資訊之可靠性及完整性。(維護期間至少 1 次，但以 2 次為上限)
(二)操作與諮詢：
</td>
<td>
4、資通安全應辦事項
廠商須遵循「資通安全管理法」及相關子法、「個人資料保護法」及其主管機關相關規定並配合本校 ISMS 規範，提供與協助本系統各項資通安全應辦事項及防護控制措施。
廠商須協助本校執行資通系統各項安全性更新與設定(如作業系統、資料庫)，
3
[redacted]
並配合本校執行安全性檢測 (如弱點掃描、滲透測試)、資通安全健診之系統改善及各項安全性更新與設定。
本系統依資通安全責任等級分級辦法－附表九資通系統防護需求分級原則，防護需求等級為普，廠商須配合本校需求完成附表十之控制措施，維護期間亦需依相關法規修訂完成各項控制措施。
廠商需協助本校執行系統(含源碼、檔案、資料庫)備份及還原作業，並配合本校執行持續營運演練。
合約期間廠商須協助填報各項資通系統或資通服務相關調查。
本案涉及資通訊軟體、硬體或服務等相關事務，廠商執行本案之團隊成員不得為陸籍人士，並不得提供及使用大陸廠牌資通訊產品。廠商不得以經濟部投資審議委員會網站公告之陸資資訊服務業者為分包廠商。
5、資通安全事件通報與應變
</td>
</tr>
<tr>
<td>文書組電子公文線上簽核系統
112 年度維護合約招標規範</td>
<td>電子公文線上簽核系統，招標規範包含不得使用大陸廠牌資通訊產品</td>
</tr>
<tr>
<td>
國立屏東大學
「112年全校電腦硬體暨網路設備維護」招標規範
一、履約期限
自112年1月1日起至112年12月31日止，共計12個月。
二、維護地點
國立屏東大學。
三、維護標的物
（一）依本校各校區「110年度電腦硬體暨網路設備維護清冊」所列標的物（含附屬之週邊設備），及校方110年度各單位使用電腦硬體暨網路設備維修標的物說明總則處理（如附件一）。
（二）提供校方應用軟體使用諮商、簡易教學、網路及伺服器系統維修設定，與合法授權軟體安裝。
四、維護要求:
（一）廠商在本校辦公時間內，需派至少[redacted]名維護人員駐校服務並須成立專案維護工作小組支援維護工作，並於事前造名冊（含警察刑事紀錄證明）送校方同意，更換時亦同，其資格條件如下表。
<table>
<tr><th>名稱/人數</th><th>具備要件</th><th>工作經驗及能力</th></tr>
<tr><td>[redacted]</td><td>[redacted]</td><td>1. 需具備校方所列網路主幹設備及網路服務主機系統維護及緊急處理問題能力。</td></tr>
</table>
</td>
<td>
需負一切相關法律責任，並賠償校方所有損失（如負擔校方因此所生訴訟費、律師費用、損害賠償及其他衍生之費用），本案結束後亦同。
（三）稽核監督之權利
本校依據資通安全管理法第9條及資通安全管理法施行細則第4條、個人資料保護法第4條及個人資料保護法施行細則第8條之規定，廠商需有完善之資通安全管理措施及個人資料保護機制，包括個人資料外洩事件之通知程序及採行補救措施，本校並得隨時稽核監督廠商及其分包廠商，如有發現任何缺失，廠商應無條件配合改善。
（四）資通安全配合事項
廠商須配合本校 ISMS 規範、「資通安全管理法」、「個人資料保護法」及其主管機關相關規定，協助本校各項資通安全應辦事項及防護控制措施。
本案涉及資通訊軟體、硬體或服務等相關事務，廠商執行本案之團隊成員不得為陸籍人士，並不得提供及使用大陸廠牌資通訊產品。廠商不得以經濟部投資審議委員會網站公告之陸資資訊服務業者為分包廠商。
（五）資通安全事件通報與應變
廠商於履行本案知悉資通安全事件時，應於1小時內向本校委託單位所屬之權責人員進行通報；本受託業務相關之資通安全事件，廠商需
</td>
</tr>
<tr>
<td>計算機與網路中心
112 年度全校電腦硬體暨網路設備維護維護合約招標規範</td>
<td>全校電腦維護合約，招標規範包含不得使用大陸廠牌資通訊產品</td>
</tr>
</table>