國立宜蘭大學圖書資訊館113學年度第2次資訊領域館務會議會議紀錄

會議日期：114年3月3日（星期一）14時

會議地點：圖資大樓一樓會議室

主　　席：吳寂絹館長　　紀錄:吳新基

出 席 者：簡立仁組長、卓信宏組長、曾國旭、張建凱、張元福、游至皓(請假)、吳新基、陳怡君(請假)、游育豪、蔡雅芳、吳新凱、林子為、莊智傑、吳文達、林士堯、阮宜豐

壹、 主席致詞(略)

貳、 確認上次會議決議事項(追蹤附件1)

參、 報告事項

一、各組業務執行重點報告(詳見各組報告內容)

二、主席裁示:

(一)教職員證卡號資料盤點尚未完整一事，請系統組列入導師會議宣導事項（含卡片汙損時無法辨識之處理方式）。

(二)無線基地台汰換乙案，請網路組規劃是否可比照各院所分攤軟體採購經費方式辦理，並於資發會提案討論。

(三)有關微軟新全校授權合約，請網路組再和廠商確認全校教職員授權數認定方式。

(四)有關校網無障礙標章申請、系統程式修改升級、教育訓練、維護等網站平台維護之報價相關問題，請網路組跟廠商（黑快馬）再次針對各單項報價如何計價等相關問題進行釐清。

(五)請於本年度個資內部稽核前，於通知內附上前次的錯誤樣態資訊供受稽單位先行參考。

肆、 提案討論

案由一：本(114)年度資訊領域經費規劃及執行情形，提請審議。

說明：詳系統組及網路組提報經費規劃項目(略)，請討論。

擬辦：依會議決議辦理。

決議:114年度設備費及業務費經費運用規劃修正後通過,如附件1,未來若有變更或新增需求則再提出討論;系統組冷氣採購建議於四月辦理，避免暑假旺季缺工漲價等問題。

案由二：圖書資訊館網頁改版乙案，提請討論。

說明：

一、圖書資訊館網頁因許久未進行更版，目前由資訊網路組進行更版設計，設計版型與內容如網址(臨時頁面)：https://lic.niu.edu.tw/p/412-1010-6025.php

二、有關於資訊服務分類項目部份，資訊網路組已將相關連結更新，請系統組參閱有無新增之項目或連結。

擬辦：於114學年度第二次資訊領域館務會議後依需求進行調整。

決議：會議決議修改及調整項目如下：

一、個人資料保護專區公告，同步於圖資館最新消息公告。

二、原公告分類簡化並整合為[圖資服務]、[資訊服務]兩大類，降低使用者搜尋負擔。

三、[資訊服務申請]名稱修改為[表單申請]。

四、[推薦服務]待後續討論後決定名稱及內容資訊。

五、Menu Bar上的[臨時閱覽證申請]及[本館開放時間]因與[常用連結與快速檢索]中的[開館時間]及[臨時閱覽證]連結重覆，建議移除後評估新增其他項目。

六、[常用連結與快速檢索]及Menu Bar新增項目，請網路組思考師生最常詢問及使用項目為方向增益。

伍、 臨時動議

提案：有關圖資館一樓茶水間空間運用方式，提請討論。

決議：

一、規劃茶水間整修，採購烘碗機放置會議所需之杯子、筷子等；設備損壞漏水部分先提報修繕。

二、配合整修請網路組同仁洽購小型飲水機，並提報爾後納入全校飲水機維護合約。

三、後續清潔維護工作納入工讀生工作項目並定期檢查。

陸、 散會:16時40分

追蹤附件 1

國立宜蘭大學 113 學年度資訊領域館務會議
前次會議執行情形追蹤表
會議日期：113 年 9 月 26 日

追蹤日期：114 年 3 月 3 日

提案	案由及決議事項	執行情形
一	案由：113 年 10 月 31 日(四)受稽機關人員名單，提請討論。 決議：同意所擬受稽核人員名單，並於 113 年 9 月 27 日前以電子郵件回復教育部。另請網路組於 10 月中旬先提供策略面受訪準備資料送交館長。	一、已依決議事項辦理。 二、本校資通安全受稽核人員已於 113 年 12 月 2 日完成教育部到校接受稽核工作。
二	案由：網路通訊使用費支援學生宿舍無線網路建置案，提請討論。 決議：本案業經學務長回覆館長說明，因宿舍經費短絀問題，已確定本學期暫緩執行學生宿舍無線網路建置案，俟未來經費有賸餘時再予執行。	已依決議事項辦理。

提案	案由及決議事項	執行情形
三	案由：有關本校圖書資訊館資訊技術人員因業務需要，參與資訊安全相關領域訓練課程或專業證照考試等費用核銷問題，提請討論。 決議：請網路組會同系統組，先擬出簽呈草稿內容送館長核閱，俟簽呈內容取得主計室共識後，再正式陳報校長裁示列入通案。	本案業於 113/12/16 以文號 1131006088 簽准在案，後續有關資訊安全相關訓練課程及專業證照考試費用核銷事宜將依簽准內容辦理。(詳見追蹤附件 2)

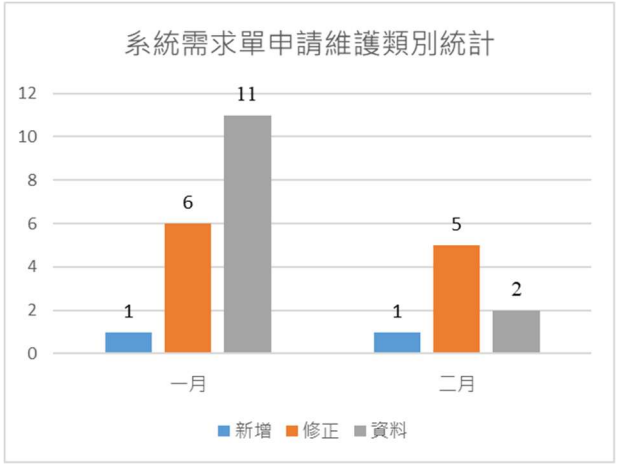
說明：請詳填執行情形，並於當次會議後自行下載存查, 謝謝大家協助。

承辦人簽章：　　單位主管簽章：

業務報告

系統設計組業務報告

1. 教務處「原民專班」、「碩士考試」、「智農專班」招生系統依期程進行作業維護；「教務暨學務行政資訊系統」各項系統功能維護；新增「超商繳費收據上傳平台」已於2/10上線。
2. 學務處「社團管理系統」開發中。
3. 圖資館「校務資訊入口網」維護 - 增加圖書館進出QRCode及借書BarCode功能開發，並依滲透初測報告進行系統安全性改善。
4. 圖資館應用程式LOG紀錄系統(Seq Server) 已完成建置，後續會將核心系統作業紀錄傳遞至Seq Server儲存。
5. 總務處「停車場承租管理系統」依滲透初測報告進行系統安全性改善維護；「教穡大樓電梯控管」時段控管設定；「場地預約系統」依新需求維護；學雜費繳費資訊即時化系統配合銀行端介接更新進程開發中。
6. 研發處「QS世界大學排名系統」、「教師人才庫/專案計畫查詢」維護；「校外實習平台」 維護。
7. 秘書室 - 新版「意見信箱」開發中。
8. 主計室「請購管理系統」配合開關帳作業，設定重新開機時段。
9. 國際處「境外招生報名系統」維護。
10. 「全國大專校院校長會議報名暨報到系統」建置並完成相關作業。
11. 教發中心「1131期末教學反應問卷」、「1131修課學生對教學助理協助教學反應問卷 」、「授課教師對教學助理評量 」統計。
12. 環安衛中心「實驗室安管系統」進行需求訪談。
13. NOC(臺灣學術網路-網路維運中心)網站開發，並依滲透初測報告進行系統安全性改善。
14. 114年度1~2月各單位系統需求(含新增、修正及資料維護)統計表：



業務單位	年度申請數	年度完成數	執行中單數
全校性	2	0	2
教務處	13	4	9
學務處	3	3	0
總務處	2	2	0
研發處	0	0	0
國際處	0	0	0
圖資館	5	1	4
教發中心	0	0	0
環安衛中心	0	0	0
人事室	0	0	0
主計室	0	0	0
合計	**25**	**10**	**15**

114 年度高深計畫分項二程式設計研習規劃

項次	時間	主題	講者	備註
1	3/5(三) 13:10~15:00	InnoServe 大賽雙料獎項-科技程設競賽經驗分享	蔡松霖、謝承恩、陳富翔	
2	3/11(二) 12:10~15:00	Cursor AI 編輯器簡介及構建 AI 助理應用雛形	黃安聖講師	
3	3/12(三) 12:10~15:00	MATLAB 使用統計與機器學習方法於資料分析的應用	MATLAB 講師	
4	3/13(四) 12:10~15:00	Cursor AI 編輯器生成 UI 設計、除錯及部署應用程式至雲端	黃安聖講師	
5	3/19(三) 12:10~15:00	如何使用 MATLAB 進行大數據分析	MATLAB 講師	
6	3/26(三) 12:10~15:00	MATLAB 於影像處理的應用	MATLAB 講師	
7	4/9(三) 12:10~15:00	待訂	張佑成講師	線上
8	4/11(五) 13:10~16:00	AI 發展概況與生成式 AI 簡介：打造自己的對話機器人	江尚瑀講師	
9	4/23(三) 12:10~15:00	待訂	張佑成講師	線上
10	4/25(五) 13:10~16:00	提示詞工程與大語言模型介紹：建置環境	江尚瑀講師	
11	4/30(三) 12:10~15:00	AI Agent 實作工作坊	高見龍老師	
12	5/9(五) 13:10~16:00	掌握 LLaMA 與檢索增強生成 (RAG) 基礎	江尚瑀講師	
13	5/14(三) 12:10~15:00	待訂	張佑成講師	線上
14	5/23(五) 13:10~16:00	RAG 的原理及實作：LlamaIndex 應用實戰	江尚瑀講師	

資訊網路組

業務報告

- 網路組經費執行情形
  - 設備費(260萬元，網路組編列229萬元)
    - 桌上型電腦60部：汰換電腦教室二。編列180萬元，實支158.1萬元。剩餘經費將進行經費變更支援購置儲存設備(暨大異地備份)
    - 垃圾郵件過濾系統：2年授權，編列25萬元，實支24萬元。
    - 無線基地台汰換：編列24萬元，下半年視經費狀況執行
  - 業務費19.6萬元：網路組10.6萬元，系統組9萬元
  - 113年圖儀設備費(150萬元)
    - 更換機房UPS，預估175萬元(網通費配合25萬元)
    - 已開始撰寫規格，3月中下旬可提出請購

- 網路組經費執行情形(續)
  - 網路設備作業系統更新(88萬元)
    - 防火牆第五期款，依合約規定於3月份付款
  - 軟體全校授權(200萬元)
    - 微軟授權第一期款，原合約9月結束，已和長峰資訊開始洽談新的三年合約
  - 網路通訊使用費(設備費210萬元)
    - 網路分流系統(編列100萬元)：第三期款98.2萬元，依合約規定於9月份付款
    - 備份系統(編列50萬元)：第二期款52.4萬元，依合約規定於6月份付款
    - 無線基地台汰換(編列60萬元)：下半年視經費狀況執行

- 網頁無障礙標章申請及教育訓練
  - 1月份與黑快馬業務洽詢網頁程式、系統升級、漏洞修補以及無障礙標章合規修改等相關費用。
    廠商報價：包含上述所列項目
    原價：30000/單一網站　優惠價：10000/單一網站
  - 目前站台數量統計為78U。
  - 網頁窗口教育訓練將由黑快馬協助辦理。
  - 1月份開始由文達及宜豐先針對秘書室、研發處進行修正，並提出申請，迄今尚未通過。
  - 全校網頁於114年需有50%通過無障礙標章，因申請過程繁複，包含各單位網頁調整，需耗費大量人力時間，若採用自行調整，則需投入網路組所有人力，造成業務排擠狀況。

- 個資保護作業
  - 本校修訂之「資通安全暨個人資料保護推動委員會設置要點」業於114年2月11日113學年度第9次行政會議審議通過並公告實施。
  - 預定於 3/26 將進行個資窗口專業教育訓練。
  - 預定於4月底檢查各單位個資盤點作業。
  - 本年度個資內部稽核預定於5月進行，受稽單位共11個單位。
  - 本學年度第2次個資保護推動委員會預定於6月進行。
  - 本年度個資外部重新驗證稽核作業預定於7月進行。

- 資安專章
  - 請全校各單位資訊窗口於3/5前回覆委外資通系統廠商聯絡資訊。
  - 預定於3-6月辦理4場資通安全暨個資保護通識課程講座，並辦理2場資安窗口專業教育訓練。
  - 預定於7-12月進行內部稽核及業務持續運作演練(單位網頁)，受稽單位為前兩年尚未執行的14個單位，委外查核場域再與經保組確認。
- 教育部稽核
  - 113/12/2資通安全實地稽核，共開出待改善事項12項、建議事項12項，並於114/2/13矯正預防填報完成，請各業務承辦人依待改善及建議事項之時程規劃日期完成相關業務，並提供佐證資料。

- 資安業務
  - 2/3-2/13 進行本校四項核心系統滲透測試初測，均有中高風險須修補，已將報告轉知郵件系統廠商與系統組進行後續修補作業，預計3月中下旬進行複測。
  - 弱點掃描已排程每3個月進行掃描本校伺服器群組，掃描後將產製相關報告，並將具有中高風險威脅之報告轉知給相關承辦人進行後續修補。

- 全校資訊設備調查
  - 3/14 前彙整資料後並填報主計處IBR系統。

- 區網中心相關計畫
  - NOC

    2/28-3/7　NOC網站功能測試
    3/3-3/7　社交工程演練功能測試
    3/10　至教育部資科司進行計畫成果匯報。
    3/31　前繳交計畫期末報告。

  - CDN

    2/27　協助建置區、縣市網DNS resolver（宜蘭、東華、中山）
- TWAREN維運計畫
  - 113年12月5日繳交第一期計畫，預計114年4月5日繳交第二期計畫。

- 校內基礎建設
  - 無線網路
    - ➔綜合教學大樓1F因應全國校長會議需求，已將1F無線網路重新佈線，並將AP移入教室改善訊號。
    - ➔2F以上區域將於暑假採相同作法進行新增AP及無線訊號改善作業，因應日後教學及TANET2025研討會之需。
    - ➔各大樓無線網路骨幹設備僅綜合大樓、生資大樓、工學院更換10G無線網路交換器設備，目前優先汰換學生宿舍，其他大樓將視預算逐步汰換。

- 2025年臺灣網際網路研討會TANET暨全國計算機會議NCS
  - 內部第1次籌備會議業於114年1月13日召開完竣。
  - 2025年TANET暨NCS研討會舉辦日期擇定於114/10/22-24（三天）舉行。
  - 本年大會主題為「智慧•創新•永續•韌性」。
  - 3月辦理招商作業事宜(擬訂贊助辦法、攤位配置等)。
  - 預定3月中旬前將計畫書陳報教育部申請大會經費。
  - 5月-7月底論文徵稿海報寄送及開放線上投稿。

- 2025年臺灣網際網路研討會TANET暨全國計算機會議NCS(續)
  - 7月辦理招商說明會。
  - 9月初-9月30日研討會報名開始。
  - 10月22-24日會議正式進行。
  - 11月~115年2月辦理結案工作。
  - 12月~115年2月辦理大會交接工作。

- 校內經費軟硬體集中採購
  - 因應校內經費支應各單位採買所需軟硬體，可能造成資源分散或閒置浪費之狀況，經討論後提出下列可行方案供參，期許達到資源與經費集中，並能妥善利用。
    1. 由研發處、教發中心統一調查各單位所需之軟硬體及經費，再由圖資館協助統整所需資源硬體與經費。
    2. 經費由校務基金統一投入建設，後續再透過雲端虛擬主機租用機制將經費逐年返還校務基金。
    3. 以GPU伺服器為例，除建置費用高昂外，因運算時會消耗大量電力及散熱，建置時需考量機房電力配置及散熱，額外成本需再評估。

- 校內經費軟硬體集中採購
  - 經與廠商詢價後，硬體建置費用粗估如下
    （不包含機房電力、散熱改建）
    以Nvidia L40S 48G(GPU) 為例，供應48人同時使用

Nutanix NX-3155-G9	*3 node	200萬/node
Nvidia L40S 48GB	*6	40~50萬/顯卡
Nvidia軟體授權費	*6	15萬/顯卡5Y(訂閱制)

    硬體建置粗估金額約為1000萬左右。

報告完畢

附件1

設備費(系統組)								
編號	項目別	數量	單價	預估金額	實支金額	順序		備註說明
1	Visual Studio Enterprise with MSDN 最新授權版(含三年維護合約)	1	61,000	61,000		1		8月份採購-續約財編:8060112-01-00004 (109年9月2日購入)
2	Spire Office for .NET Pro Edition Developer Subscription(含二年維護合約)	1	105,000	105,000	105,000	1	已採購	2月份採購-續約財編:83140601001-05663 (112年3月9日購入)
3	行動載具(手機)	1	38,840	38,840		3		開發及測試用行動載具 汰換財編:4050202-05-00275 (109年5月4日購入)
4	Apple Mac mini	1	33,900	33,900		2		開發用電腦 汰換財編:3140101-03-03886 (106年9月15日購入)
5	辦公用筆電	1	35,000	35,000		2		辦公用筆電 汰換財編:3140101-03-03621 (106年1月25日購入)
6	系統組辦公室冷氣(8.0KW)	1	45,900	45,900		2		已扣除補助金額一萬元 (統一採購尚未上架，先列建議售價) (103年7月9日購入)
7	系統組辦公室冷氣(4.3KW)	1	22,900	22,900		2		已扣除補助金額一萬元 (統一採購尚未上架，先列建議售價) (96年7月2日購入)
			合　計	342,540	105,000			

業務費(系統組)								
編號	項目別	數量	單價	預估金額		順序		備註說明
1	辦公文具用品、碳粉匣、電腦週邊...等	1	24,000	24,000		1		
2	教育訓練、線上課程費用	1	30,000	30,000		1		
3	差旅費	1	24,000	24,000		1		
4	空氣清淨機濾網	1	6,000	6,000		1		
5	會議活動便當	50	120	6,000		1		
			合　計	90,000				

設備費(網路組)								
編號	項目別	數量	單價	預估金額	實支金額	順序		備註說明
1	桌上型電腦(電二)	60	30,000	1,800,000	1,581,000	1	已下訂	剩餘經費變更支援購置儲存設備(暨大異地備份)
2	垃圾郵件過濾系統	1	250,000	250,000	240,000	1	已採購	
3	無線基地台汰換	8	30,000	240,000		2		下半年度視經費狀況執行
			合　計	2,290,000	1,821,000			

業務費(網路組)								
編號	項目別	數量	單價	預估金額		順序		備註說明
1	電腦教室文具用品	1	49,000	49,000		1		
2	辦公用品、耗材	1	48,000	48,000		1		
3	油電費	1	3,000	3,000		1		
4	會議活動便當	50	120	6,000		1		
			合　計	106,000				

追蹤附件2

檔　　號：901
保存年限：10年

簽　民國113年12月09日
於資訊網路組

主旨：有關本校圖書資訊館資訊技術人員參加資訊安全相關訓練課程及專業證照考試費用核銷事宜，簽請核示。

說明：

一、依據「資通安全責任等級分級辦法」之規定，本校列為資通安全責任等級C級之公務機關，並依據該辦法附表五-認知與訓練應辦事項辦理（如附件1)。

二、考量資訊領域課程訓練或(原廠)證照考試費用往往價格昂貴，且本館資訊同仁常以代墊或預支費用方式繳納課程或考試報名費用。~~→~~囿於是類證照考試皆有一定難度，倘因未取得專業證照以致無法核銷轉正訓練課程或考試相關費用，將造成同仁許多壓力與負擔，亦排擠同仁參訓意願，爰提核銷方式之建議。

三、另檢附數位發展部資通安全署113年11月6日修正發布之「資通安全專業證照清單」(如附件2)供參。

擬辦：

一、有關旨揭費用之核銷，擬辦理方式如下:

(一)訓練課程報名費用包含1次考試的方式收取者，得檢附完訓證明文件及支出憑證准予核銷轉正；另考試未通過者，以補考1次為限，得逕憑考試支出憑證准予核銷轉正該次考試費用。

(二)訓練課程與考試分開報名者，課程費用部分，得檢附完訓證明文件及支出憑證准予核銷轉正；考試費用部分，以考試次數2次內(含補考)，得逕憑支出憑證准予核銷轉正該次考試費用。

(三)前揭費用核銷之經費來源，擬由年度高等教育深耕計畫—資安專章經費支應。

資訊網路組
1131006088

二、如奉核可，依擬辦事項辦理。

會辦單位：人事室、主計室
第一層決行

承辦單位	會辦單位	決行
圖書資訊館 約用技術員 吳新凱 113/12/09 09:58:33 副教授兼資訊網路組組長 卓信宏 113/12/09 14:02:18 圖書資訊館館長 吳寂絹 113/12/09 17:13:02 **圖書資訊館** 增列經費來源 約用技術員 吳新凱 113/12/10 10:32:58 核稿秘書 蔡惠雅 113/12/16 11:14:06	**系統設計組** 系統設計組組長 簡立仁 113/12/09 16:41:37 **人事室** 一、依公務人員訓練進修辦法第12條規定略以，自行申請以公餘時間或部分辦公時間參加進修之公務人員，經服務機關學校認定與業務有關，並同意其前往進修且成績優良者，得給予部分費用補助。 二、經洽圖書資訊館承辦人吳新凱表示，案內補助對象係約用及計畫人員，且補助經費來源為高等教育深耕計畫，非屬上開法規適用範圍。爰本案是否妥適，請依主計室意見辦理。 人事室組員 陳志偉 113/12/13 08:34:37 人事室專員 游憶如 113/12/13 09:12:24代 **主計室** 主計室組員 楊瑞鵑 113/12/13 16:40:02 請業務單位於計畫預算可容納下，秉於合理原則下，本於權責核處。 主計室組長 王浩丞 113/12/16 09:49:52 主計室主任 邱聰祥 113/12/16 10:45:03	依主計室所擬 校長陳威戎(甲) 113/12/16 14:23:16

法規名稱：資通安全責任等級分級辦法

修正日期：民國 110 年 08 月 23 日

第 1 條

本辦法依資通安全管理法（以下簡稱本法）第七條第一項規定訂定之。

第 2 條

公務機關及特定非公務機關（以下簡稱各機關）之資通安全責任等級，由高至低，分為 A 級、B 級、C 級、D 級及 E 級。

第 3 條

1 主管機關應每二年核定自身資通安全責任等級。

2 行政院直屬機關應每二年提交自身、所屬或監督之公務機關及所管之特定非公務機關之資通安全責任等級，報主管機關核定。

3 直轄市、縣（市）政府應每二年提交自身、所屬或監督之公務機關，與所轄鄉（鎮、市）、直轄市山地原住民區公所及其所屬或監督之公務機關之資通安全責任等級，報主管機關核定。

4 直轄市及縣（市）議會、鄉（鎮、市）民代表會及直轄市山地原住民區民代表會應每二年提交自身資通安全責任等級，由其所在區域之直轄市、縣（市）政府彙送主管機關核定。

5 總統府、國家安全會議、立法院、司法院、考試院及監察院應每二年核定自身、所屬或監督之公務機關及所管之特定非公務機關之資通安全責任等級，送主管機關備查。

6 各機關因組織或業務調整，致須變更原資通安全責任等級時，應即依前五項規定程序辦理等級變更；有新設機關時，亦同。

7 第一項至第五項公務機關辦理資通安全責任等級之提交或核定，就公務機關或特定非公務機關內之單位，認有另列與該機關不同等級之必要者，得考量其業務性質，依第四條至第十條規定認定之。

第 4 條

各機關有下列情形之一者，其資通安全責任等級為 A 級：

一、業務涉及國家機密。

二、業務涉及外交、國防或國土安全事項。

三、業務涉及全國性民眾服務或跨公務機關共用性資通系統之維運。

四、業務涉及全國性民眾或公務員個人資料檔案之持有。

五、屬公務機關，且業務涉及全國性之關鍵基礎設施事項。

六、屬關鍵基礎設施提供者，且業務經中央目的事業主管機關考量其提供或維運關鍵基礎設施服務之用戶數、市場占有率、區域、可替代性，認其資通系統失效或受影響，對社會公共利益、民心士氣或民眾生命、身體、財產安全將產生災難性或非常嚴重之影響。

七、屬公立醫學中心。

第 5 條

各機關有下列情形之一者，其資通安全責任等級為 B　級：

一、業務涉及公務機關捐助、資助或研發之國家核心科技資訊之安全維護及管理。

二、業務涉及區域性、地區性民眾服務或跨公務機關共用性資通系統之維運。

三、業務涉及區域性或地區性民眾個人資料檔案之持有。

四、業務涉及中央二級機關及所屬各級機關（構）共用性資通系統之維運。

五、屬公務機關，且業務涉及區域性或地區性之關鍵基礎設施事項。

六、屬關鍵基礎設施提供者，且業務經中央目的事業主管機關考量其提供或維運關鍵基礎設施服務之用戶數、市場占有率、區域、可替代性，認其資通系統失效或受影響，對社會公共利益、民心士氣或民眾生命、身體、財產安全將產生嚴重影響。

七、屬公立區域醫院或地區醫院。

第 6 條

1　各機關維運自行或委外設置、開發之資通系統者，其資通安全責任等級為 C　級。

2　前項所定自行或委外設置之資通系統，指具權限區分及管理功能之資通系統。

第 7 條

各機關自行辦理資通業務，未維運自行或委外設置、開發之資通系統者，其資通安全責任等級為 D　級。

第 8 條

各機關有下列情形之一者，其資通安全責任等級為 E 級：

一、無資通系統且未提供資通服務。

二、屬公務機關，且其全部資通業務由其上級機關、監督機關或上開機關指定之公務機關兼辦或代管。

三、屬特定非公務機關，且其全部資通業務由其中央目的事業主管機關、中央目的事業主管機關所屬公務機關、中央目的事業主管機關所管特定非公務機關或出資之公務機關兼辦或代管。

第 9 條

各機關依第四條至前條規定，符合二個以上之資通安全責任等級者，其資通安全責任等級列為其符合之最高等級。

第 10 條

各機關之資通安全責任等級依前六條規定認定之。但第三條第一項至第五項之公務機關提交或核定資通安全責任等級時，得考量下列事項對國家安全、社會公共利益、人民生命、身體、財產安全或公務機關聲譽之影響程度，調整各機關之等級：

一、業務涉及外交、國防、國土安全、全國性、區域性或地區性之能源、水資源、通訊傳播、交通、銀行與金融、緊急救援與醫院業務者，其中斷或受妨礙。

二、業務涉及個人資料、公務機密或其他依法規或契約應秘密之資訊者，其資料、公務機密或其他資訊之數量與性質，及遭受未經授權之存取、使用、控制、洩漏、破壞、竄改、銷毀或其他侵害。

三、各機關依層級之不同，其功能受影響、失效或中斷。

四、其他與資通系統之提供、維運、規模或性質相關之具體事項。

第 11 條

1 各機關應依其資通安全責任等級，辦理附表一至附表八之事項。

2 各機關自行或委外開發之資通系統應依附表九所定資通系統防護需求分級原則完成資通系統分級，並依附表十所定資通系統防護基準執行控制措施；特定非公務機關之中央目的事業主管機關就特定類型資通系統之防護基準認有另為規定之必要者，得自行擬訂防護基準，報請主管機關核定後，依其規定辦理。

3 各機關辦理附表一至附表八所定事項或執行附表十所定控制措施，因技術限制、個別資通系統之設計、結構或性質等因素，就特定事項或控制措施之辦理或執行顯有困難者，得經第三條第二項至第四項所定其等級提交機關或同條第五項所定其等級核定機關同意，並報請主管機關備查後，免執行該事項或控制措施；其為主管機關者，經其同意後，免予執行。

4 公務機關之資通安全責任等級為 A 級或 B 級者，應依主管機關指定之方式，提報第一項及第二項事項之辦理情形。

5 中央目的事業主管機關得要求所管特定非公務機關，依其指定之方式提報第一項及第二項事項之辦理情形。

第 12 條

1 本辦法之施行日期，由主管機關定之。

2 本辦法修正條文自發布日施行。

法規名稱：資通安全責任等級分級辦法

修正日期：民國 110 年 08 月 23 日

第 1 條

本辦法依資通安全管理法（以下簡稱本法）第七條第一項規定訂定之。

第 2 條

公務機關及特定非公務機關（以下簡稱各機關）之資通安全責任等級，由高至低，分為 A 級、B 級、C 級、D 級及 E 級。

第 3 條

1 主管機關應每二年核定自身資通安全責任等級。

2 行政院直屬機關應每二年提交自身、所屬或監督之公務機關及所管之特定非公務機關之資通安全責任等級，報主管機關核定。

3 直轄市、縣（市）政府應每二年提交自身、所屬或監督之公務機關，與所轄鄉（鎮、市）、直轄市山地原住民區公所及其所屬或監督之公務機關之資通安全責任等級，報主管機關核定。

4 直轄市及縣（市）議會、鄉（鎮、市）民代表會及直轄市山地原住民區民代表會應每二年提交自身資通安全責任等級，由其所在區域之直轄市、縣（市）政府彙送主管機關核定。

5 總統府、國家安全會議、立法院、司法院、考試院及監察院應每二年核定自身、所屬或監督之公務機關及所管之特定非公務機關之資通安全責任等級，送主管機關備查。

6 各機關因組織或業務調整，致須變更原資通安全責任等級時，應即依前五項規定程序辦理等級變更；有新設機關時，亦同。

7 第一項至第五項公務機關辦理資通安全責任等級之提交或核定，就公務機關或特定非公務機關內之單位，認有另列與該機關不同等級之必要者，得考量其業務性質，依第四條至第十條規定認定之。

第 4 條

各機關有下列情形之一者，其資通安全責任等級為 A 級：

一、業務涉及國家機密。

二、業務涉及外交、國防或國土安全事項。

三、業務涉及全國性民眾服務或跨公務機關共用性資通系統之維運。

四、業務涉及全國性民眾或公務員個人資料檔案之持有。

五、屬公務機關，且業務涉及全國性之關鍵基礎設施事項。

六、屬關鍵基礎設施提供者，且業務經中央目的事業主管機關考量其提供或維運關鍵基礎設施服務之用戶數、市場占有率、區域、可替代性，認其資通系統失效或受影響，對社會公共利益、民心士氣或民眾生命、身體、財產安全將產生災難性或非常嚴重之影響。

七、屬公立醫學中心。

第 5 條

各機關有下列情形之一者，其資通安全責任等級為 B　級：

一、業務涉及公務機關捐助、資助或研發之國家核心科技資訊之安全維護及管理。

二、業務涉及區域性、地區性民眾服務或跨公務機關共用性資通系統之維運。

三、業務涉及區域性或地區性民眾個人資料檔案之持有。

四、業務涉及中央二級機關及所屬各級機關（構）共用性資通系統之維運。

五、屬公務機關，且業務涉及區域性或地區性之關鍵基礎設施事項。

六、屬關鍵基礎設施提供者，且業務經中央目的事業主管機關考量其提供或維運關鍵基礎設施服務之用戶數、市場占有率、區域、可替代性，認其資通系統失效或受影響，對社會公共利益、民心士氣或民眾生命、身體、財產安全將產生嚴重影響。

七、屬公立區域醫院或地區醫院。

第 6 條

1　各機關維運自行或委外設置、開發之資通系統者，其資通安全責任等級為 C　級。

2　前項所定自行或委外設置之資通系統，指具權限區分及管理功能之資通系統。

第 7 條

各機關自行辦理資通業務，未維運自行或委外設置、開發之資通系統者，其資通安全責任等級為 D　級。

第 8 條

各機關有下列情形之一者，其資通安全責任等級為 E 級：

一、無資通系統且未提供資通服務。

二、屬公務機關，且其全部資通業務由其上級機關、監督機關或上開機關指定之公務機關兼辦或代管。

三、屬特定非公務機關，且其全部資通業務由其中央目的事業主管機關、中央目的事業主管機關所屬公務機關、中央目的事業主管機關所管特定非公務機關或出資之公務機關兼辦或代管。

第 9 條

各機關依第四條至前條規定，符合二個以上之資通安全責任等級者，其資通安全責任等級列為其符合之最高等級。

第 10 條

各機關之資通安全責任等級依前六條規定認定之。但第三條第一項至第五項之公務機關提交或核定資通安全責任等級時，得考量下列事項對國家安全、社會公共利益、人民生命、身體、財產安全或公務機關聲譽之影響程度，調整各機關之等級：

一、業務涉及外交、國防、國土安全、全國性、區域性或地區性之能源、水資源、通訊傳播、交通、銀行與金融、緊急救援與醫院業務者，其中斷或受妨礙。

二、業務涉及個人資料、公務機密或其他依法規或契約應秘密之資訊者，其資料、公務機密或其他資訊之數量與性質，及遭受未經授權之存取、使用、控制、洩漏、破壞、竄改、銷毀或其他侵害。

三、各機關依層級之不同，其功能受影響、失效或中斷。

四、其他與資通系統之提供、維運、規模或性質相關之具體事項。

第 11 條

1 各機關應依其資通安全責任等級，辦理附表一至附表八之事項。

2 各機關自行或委外開發之資通系統應依附表九所定資通系統防護需求分級原則完成資通系統分級，並依附表十所定資通系統防護基準執行控制措施；特定非公務機關之中央目的事業主管機關就特定類型資通系統之防護基準認有另為規定之必要者，得自行擬訂防護基準，報請主管機關核定後，依其規定辦理。

3 各機關辦理附表一至附表八所定事項或執行附表十所定控制措施，因技術限制、個別資通系統之設計、結構或性質等因素，就特定事項或控制措施之辦理或執行顯有困難者，得經第三條第二項至第四項所定其等級提交機關或同條第五項所定其等級核定機關同意，並報請主管機關備查後，免執行該事項或控制措施；其為主管機關者，經其同意後，免予執行。

4 公務機關之資通安全責任等級為 A 級或 B 級者，應依主管機關指定之方式，提報第一項及第二項事項之辦理情形。

5 中央目的事業主管機關得要求所管特定非公務機關，依其指定之方式提報第一項及第二項事項之辦理情形。

第 12 條

1 本辦法之施行日期，由主管機關定之。

2 本辦法修正條文自發布日施行。

附表五　資通安全責任等級C級之公務機關應辦事項

制度面向	辦理項目	辦理項目細項	辦理內容
管理面	資通系統分級及防護基準		初次受核定或等級變更後之一年內，針對自行或委外開發之資通系統，依附表九完成資通系統分級；其後應每年至少檢視一次資通系統分級妥適性；並應於初次受核定或等級變更後之二年內，完成附表十之控制措施。
	資訊安全管理系統之導入		初次受核定或等級變更後之二年內，全部核心資通系統導入CNS 27001或ISO 27001等資訊安全管理系統標準、其他具有同等或以上效果之系統或標準，或其他公務機關自行發展並經主管機關認可之標準，並持續維持導入。
	資通安全專責人員		初次受核定或等級變更後之一年內，配置一人；須以專職人員配置之。
	內部資通安全稽核		每二年辦理一次。
	業務持續運作演練		全部核心資通系統每二年辦理一次。
技術面	安全性檢測	弱點掃描	全部核心資通系統每二年辦理一次。
		滲透測試	全部核心資通系統每二年辦理一次。
	資通安全健診	網路架構檢視	每二年辦理一次。
		網路惡意活動檢視	
		使用者端電腦惡意活動檢視	
		伺服器主機惡意活動檢視	
		目錄伺服器設定及防火牆連線設定檢視	
	資通安全弱點通報機制		一、初次受核定或等級變更後之二年內，完成資通安全弱點通報機制導入作業，並持續維運及依主管機關指定之方式提交資訊資產盤點資料。 二、本辦法中華民國一百十年八月二十三日修正施行前已受核定者，應於修正施行後二年內，完成資通安全弱點通報機制導入作業，並持續維運及依主管機關指定之方式提交資訊資產盤點資料。

	資通安全防護	防毒軟體	初次受核定或等級變更後之一年內，完成各項資通安全防護措施之啟用，並持續使用及適時進行軟、硬體之必要更新或升級。
		網路防火牆	
		具有郵件伺服器者，應備電子郵件過濾機制	
認知與訓練	資通安全教育訓練	資通安全專職人員	每人每年至少接受十二小時以上之資通安全專業課程訓練或資通安全職能訓練。
		資通安全專職人員以外之資訊人員	每人每二年至少接受三小時以上之資通安全專業課程訓練或資通安全職能訓練，且每年接受三小時以上之資通安全通識教育訓練。
		一般使用者及主管	每人每年接受三小時以上之資通安全通識教育訓練。
	資通安全專業證照及職能訓練證書		初次受核定或等級變更後之一年內，至少一名資通安全專職人員，分別持有證照及證書各一張以上，並持續維持證照及證書之有效性。

備註：

一、資通系統之性質為共用性系統者，由該資通系統之主責設置、維護或開發機關判斷是否屬於核心資通系統。

二、資通安全專職人員，指應全職執行資通安全業務者。

三、公務機關辦理本表「資通安全健診」時，除依本表所定項目、內容及時限執行外，亦得採取經主管機關認可之其他具有同等或以上效用之措施。

四、資通安全弱點通報機制，指結合資訊資產管理與弱點管理，掌握整體風險情勢，並協助機關落實本法有關資產盤點及風險評估應辦事項之作業。

五、資通安全專業證照，指由主管機關認可之國內外發證機關（構）所核發之資通安全證照。

資通安全專業證照清單

日期：113年11月6日修正公布

序	發證機構(單位)	管理類(22)	技術類(89)
1.	已簽署國際認證論壇(International Accreditation Forum, IAF)多邊相互承認協議(ISO/IEC 27006範圍)之認證機構(含TAF)所認證之資訊安全管理系統驗證機構、稽核員驗證或註冊之國際專業機構[1]	1. ISO/IEC 27001:2013 Information Security Management System (ISMS) Auditor/Lead Auditor (請於114年10月31日前完成轉版) 2. ISO/IEC 27001:2022 Information Security Management System (ISMS) Auditor/Lead Auditor 3. ISO 22301 Business Continuity Management System (BCMS) Auditor/Lead Auditor 4. ISO/IEC 27701:2019 Privacy Information Management System Lead Auditor Lead Auditor相關證照應具有效性，除提出證照外，尚須提供當年度至少有2次實際參與該證照內容有關之稽核經驗證明。	
2.	International Information System Security Certification Consortium (ISC2)[2]	1. Certified Information Systems Security Professional (CISSP)	1. Systems Security Certified Practitioner (SSCP) 2. Certified Cloud Security

資通安全專業證照清單

日期：113年11月6日修正公布

序	發證機構(單位)	管理類(22)	技術類(89)
		2. Information Systems Security Management Professional (CISSP-ISSMP) 3. Governance, Risk and Compliance Certification (CGRC)	Professional (CCSP) 3. Certified Authorization Professional (CAP)(認可至114年11月7日止) 4. Certified Secure Software Lifecycle Professional (CSSLP) 5. HealthCare Information Security and Privacy Practitioner (HCISPP)(認可至115年12月1日止) 6. Information Systems Security Architecture Professional (CISSP-ISSAP) 7. Information Systems Security Engineering Professional (CISSP-ISSEP)
3.	The Computing Technology Industry Association (CompTIA)[3]		1. CompTIA Security+ 2. CompTIA Cybersecurity Analyst (CompTIA CySA+) 3. CompTIA Advanced Security Practitioner (CompTIA

資通安全專業證照清單

日期：113年11月6日修正公布

序	發證機構(單位)	管理類(22)	技術類(89)
			CASP+) 4. CompTIA PenTest+
4.	CREST[4]		1. Penetration Testing (1) The CREST Practitioner Security Analyst (CPSA) (2) The CREST Certified Wireless Specialist (CCWS) (認可至114年11月7日止) (3) The CREST Certified Simulated Attack Specialist (CCSAS) (4) The CREST Certified Simulated Attack Manager (CCSAM) 2. Threat Intelligence (1) The CREST Registered Threat Intelligence Analyst (CRTIA) (2) The CREST Certified Threat Intelligence Manager (CCTIM) 3. Incident Response

資通安全專業證照清單

日期：113年11月6日修正公布

序	發證機構(單位)	管理類(22)	技術類(89)
			(1) The CREST Practitioner Intrusion Analyst (CPIA) (2) The CREST Registered Intrusion Analyst (CRIA) (3) The Certified Network Intrusion Analyst (CCNIA)（認可至114年11月7日止） (4) The CREST Certified Host Intrusion Analyst (CCHIA)（認可至114年11月7日止） (5) The CREST Certified Malware Reverse Engineer (CCMRE)（認可至114年11月7日止） (6) The CREST Certified Incident Manager (CCIM) 4. Security Architecture The CREST Registered Technical Security Architect Examination (CRTSA)（認可至114年11月7日止）
5.	EC-Council[5]	1. Certified Chief Information Security	1. Certified Network Defender Course (CND)

資通安全專業證照清單

日期：113年11月6日修正公布

序	發證機構(單位)	管理類(22)	技術類(89)
		Officer (CCISO) 2. EC-Council Information Security Management (EISM) (認可至114年11月7日止) 3. Associate Certified Chief Information Security Officer (Associate CCISO)	2. Certified Ethical Hacker (CEH) 3. Certified Ethical Hacker (CEH) Practical 4. CEH (Master) 5. EC-Council Certified Security Analyst (ECSA) (認可至114年11月7日止) 6. Computer Hacking Forensic Investigator (CHFI) 7. EC-Council Certified Incident Handler (ECIH) 8. EC-Council Disaster Recovery Professional (EDRP) 9. Certified Threat Intelligence Analyst (CTIA) 10. Certified Application Security Engineer (CASE) NET、JAVA 11. Certified Penetration

資通安全專業證照清單

日期：113年11月6日修正公布

序	發證機構(單位)	管理類(22)	技術類(89)
			Tester (CPENT) 12. Licensed Penetration Testing (LPT) 13. Certified SOC Analyst (CSA)
6.	Global Information Assurance Certification (GIAC)[6]	Management, Legal & Audit (1) GIAC Security Leadership (GSLC) (2) GIAC Systems and Network Auditor Certification (GSNA) (3) GIAC Law of Data Security & Investigations (GLEG) (4) GIAC Strategic Planning, Policy, and Leadership (GSTRT) (5) GIAC Information Security Professional Certification (GISP) (6) GIAC Critical Controls Certification (GCCC)	1. Cloud Security (1) GIAC Cloud Security Essentials Certification (GCLD) (2) GIAC Certified Web Application Defender (GWEB) (3) GIAC Cloud Security Automation (GCSA) (4) GIAC Public Cloud Security (GPCS) 2. Cyber Defense (1) GIAC Open Source Intelligence Certification (GOSI) (2) GIAC Certified Intrusion Analyst Certification

資通安全專業證照清單

日期：113年11月6日修正公布

序	發證機構(單位)	管理類(22)	技術類(89)
			(GCIA) (3) GIAC Certified Windows Security Administrator (GCWN) (4) GIAC Continuous Monitoring Certification (GMON) (5) GIAC Defensible Security Architecture Certification (GDSA) (6) GIAC Certified Detection Analyst (GCDA) (7) GIAC Security Operations Certified (GSOC) (8) GIAC Information Security Fundamentals (GISF) (9) GIAC Security Essentials (GSEC) (10) GIAC Certified Enterprise Defender (GCED) (11) GIAC Certified Incident Handler Certification (GCIH)

資通安全專業證照清單

日期：113年11月6日修正公布

序	發證機構(單位)	管理類(22)	技術類(89)
			(12) GIAC Foundational Cybersecurity Technologies (GFACT) (13) GIAC Defending Advanced Threats (GDAT) 3. Offensive Operations (1) GIAC Enterprise Vulnerability Assessor Certification (GEVA)（認可至114年11月7日止） (2) GIAC Penetration Tester Certification (GPEN) (3) GIAC Web Application Penetration Tester (GWAPT) (4) GIAC Python Coder (GPYC) (5) GIAC Mobile Device Security Analyst (GMOB) (6) GIAC Cloud Penetration Tester (GCPN) (7) GIAC Assessing and Auditing Wireless Networks (GAWN)

資通安全專業證照清單

日期：113年11月6日修正公布

序	發證機構(單位)	管理類(22)	技術類(89)
			(8) GIAC Exploit Researcher and Advanced Penetration Tester (GXPN) 4. Digital Forensics and Incident Response (1) GIAC Battlefield Forensics & Acquisition (GBFA) (2) GIAC Certified Forensic Examiner (GCFE) (3) GIAC Advanced Smartphone Forensic Certification (GASF) (4) GIAC Certified Forensic Analyst (GCFA) (5) GIAC Network Forensic Analyst (GNFA) (6) GIAC Cyber Threat Intelligence (GCTI) (7) GIAC Reverse Engineering Malware Certification (GREM) 5. Industrial Control Systems

資通安全專業證照清單

日期：113年11月6日修正公布

序	發證機構(單位)	管理類(22)	技術類(89)
			(1) GIAC Global Industrial Cyber Security Professional Certification (GICSP) (2) GIAC Response and Industrial Defense (GRID) (3) GIAC Critical Infrastructure Protection Certification (GCIP) 6. GSE GIAC Security Expert (GSE)
7.	Information Systems Audit and Control Association (ISACA)[7]	1. Certified Information Security Manager (CISM) 2. Certified in the Governance of Enterprise IT (CGEIT) 3. Certified Information Systems Auditor (CISA) 4. Certified in Risk and Information Systems Control (CRISC)	

資通安全專業證照清單

日期：113年11月6日修正公布

序	發證機構(單位)	管理類(22)	技術類(89)
8.	The International Society of Forensic Computer Examiners (ISFCE)[8]		Certified Computer Examiner (CCE)
9.	Offensive Security[9]		1. OffSec Certified Professional (OSCP) 2. Offensive Security Certified Expert (OSCE) 3. OffSec Wireless Professional (OSWP) 4. OffSec Exploitation Expert (OSEE) 5. OffSec Web Expert (OSWE) 6. OffSec Exploit Developer (OSED) 7. OffSec Experienced Penetration Tester (OSEP)
10.	Cisco[10]		1. Cisco Certified Network Associate (CCNA) 2. Cisco Certified CyberOps Associate (CBROPS)
11.	經濟部[11]		1. iPAS 資訊安全工程師中級能力鑑定

資通安全專業證照清單

日期：113年11月6日修正公布

序	發證機構(單位)	管理類(22)	技術類(89)
12.	International Society of Automation (ISA) [12]	1. ISA/IEC 62443 Cybersecurity Fundamentals Specialist 2. ISA/IEC 62443 Cybersecurity Risk Assessment Specialist	1. ISA/IEC 62443 Cybersecurity Design Specialist 2. ISA/IEC 62443 Cybersecurity Maintenance Specialist 3. ISA/IEC 62443 Cybersecurity Expert
13.	Hack The Box (HTB)[13]		1. HTB Certified Defensive Security Analyst (HTB CDSA) 2. HTB Certified Penetration Testing Specialist (HTB CPTS)

備註：

1. 針對發證機構（單位）已停止核發、規劃停止核發或刪除之證照，將提供緩衝配套措施，並於證照項目備註實際停止認可日期，說明如下：
   (1)已停止核發或刪除之證照，停止認可日期為本清單修正公告後1年。
   (2)規劃停止核發之證照：於1年後停止核發者，停止認可日期原則參考原廠建議訂定；於1年內停止核發者，停止認可日期為本清單修正公告後1年。
   (3)以上停止認可日期，得視資通安全專職（責）人員持有人數、證照職能內容等情形，經審定後酌予調整。
2. 以轉版方式取得ISO類證照版本更新者，其有效性應具備下列各項文件：
   (1)新版本之轉版證照(Transition Training Course Certificate)。
   (2)原版本之證照(Training Course Certificate)。

資通安全專業證照清單

日期：113 年 11 月 6 日修正公布

3. 本證照清單定期更新，各機關如有新增資通安全專業證照建議，請依數位發展部資通安全署網站公告之「資通安全專業證照認可審查作業流程」辦理。
4. 本證照清單於數位發展部資通安全署網站定期更新，機關如有任何疑問歡迎來電數位發展部資通安全署（02-2380-8500)反映。

資通安全專業證照清單

日期：113年11月6日修正公布

參考資料：

1. TAF：https://www.taftw.org.tw/
   IAF：https://www.iafcertsearch.org/search/certification-bodies?standards_id=4cb16367-3cd5-5a6c-a382-1f524564b9d9&standards_name=ISO%2027001
2. ISC2：https://www.isc2.org/
3. CompTIA：https://certification.comptia.org/
4. CREST：https://www.crest-approved.org
5. EC-council：https://www.eccouncil.org/
6. GIAC：https://www.giac.org/
7. ISACA：https://www.isaca.org/
8. ISFCE：https://www.isfce.com/
9. OffSec：https://www.offsec.com/
10. Cisco：https://www.cisco.com
11. iPAS：https://www.ipas.org.tw/ise
12. ISA：https://www.isa.org/
13. HTB：https://academy.hackthebox.com/