

國立彰化師範大學圖書與資訊處

104 學年度第二學期第 5 次主管會議會議紀錄

時間：105 年 06 月 16 日 下午 12:00

地點：圖書與資訊處一樓會議室

主持人：蕭圖資長如淵

記錄：林志銘

出席人員：蔡惠玲組長、詹益禎組長、陳仁德組長、陳婉佳組長、鍾錦雲專員

壹、主持人致詞：略。

貳、各組業務報告：

一、綜合業務組

- (1) 上個月會議圖資長裁示：本棟外牆之「總圖書館」字樣保留，並參考校內其他大樓名稱形式與字樣大小，及圖書館入口橫軸需替換上新名稱「圖資大樓」，並請廠商提供相關字樣形式及大小，進行評估與討論。

圖資長裁示：

- I. 圖資大樓字樣以橫式方式呈現
- II. 圖資大樓字樣放置於正門位置（如下圖）

一、正門



- III. 原側門「電子計算機中心」字樣已卸下，未來待電腦教室移至B1後，側門將變更為緊急逃生口，毋需另行標示。
- IV. 「圖資大樓」，請廠商提供多種字樣形式，可再由同仁票選決定。
- V. 圖資大樓字樣完成後，委請總務處針對校園路線指標進行變更。

- (2) 空調設備開關標準流程，靜宜已整理完成，現將資料放於門禁人員處供參。
- (3) 本處空調品質改善工程於6月15日上午完成驗收。
- (4) B1二手書區樓梯漏水處灌注防漏PU填縫劑(聚氨酯)。但經過端午連日來的降雨，樓梯兩側滲水依然嚴重，天花板採光罩的部份兩年半前曾經有進行過防漏處理工程（保固期兩年），今年已經超過保固期了，這次也嚴重漏水。

圖資長裁示：

- I. 滲水問題因建築物年代已久，為不可避免的問題。
- II. 相關問題應會請總務處，偕同專業技師進行會勘，由專業人員提供解決方案後，再行討論。
- III. 二手書交流區因地處偏僻，除有空氣不流通問題，更加目前出現的滲水問題，再者其利用率甚低，未來是否仍保留此區或另移至它處，再行討論。
- IV. 滲水問題尚未修繕完畢前，為避免使用者誤認行政團隊未積極處理，應在該區域豎立告示牌，提醒使用者此處滲水問題已提請報修，請小心行走。（後續採編組補充已在該區豎立告示「目前二手書交流區因滲水問題整理中，暫停開放」）

(5) 最近一個月本處修繕工作有：

1. B1空調面板壓克力保護盒破裂修復。
2. B1地下一樓演講廳電燈損壞維修共計更新23盞。
3. 5F無障礙女廁(東)沖水量不夠，沖水器更換。
4. 1-3F窗簾故障共修復三窗。
5. 1F 電梯超載導致著床裝置故障，已更換光電式著床開關。

圖資長裁示：

I. 請電梯維護廠商將超載警示音音量調大

II. 因電梯建置年份已久，且其使用量大，務必與營繕組及維護廠商確認是否有安全疑慮？應如何調校。

- (6) 105年5月26日至國教署辦理104學年度第2學期高國中小有聲教科書驗收會議，更正3本教科書，補2位錄音人員資料，逾期罰款349元，已於5月30日寄出補正版。並於6月6日行文補充資料及補正配發表至國教署。
- (7) 105年5月21日辦理「視障有聲圖書錄音人員培訓營」，參加學員計42人。
- (8) 105學年度大專校院身心障礙學生人文社會學科上課必要用書之有聲書製作計畫，6月14日第一次流標(醒吾科大資訊訊傳播系參與投標)，第二次預計在6月29日上午開標，在投標價格需要再考量，等投標價格確認後，將儘快進行投標程序。
- (9) 本處設備費及業務費執行率皆已達五成以上，目前設備費結餘為一佰五十七萬八千元，業務處結餘為兩佰二十萬。電腦汰換費尚餘一佰九十九萬元。

圖資長裁示：

I. 本期台銀標結束在即，請確認電腦教室更換設備的執行期程。

II. 確認新增線路執行期程。

III. 請概算明年度工讀金費用，並確認相關經費。

(10)本學期進修學院共回饋三十萬二千八百五十二元。目前共結餘九十四萬三千一百八十一元。

二、 讀者服務組

- (1) 完成圖資長指示辦理寶山校區圖書館分館暑假期間週五閉館事宜簽呈，於5月27日奉校長核定，從今年(105年)暑假起寶山分館暑假週五閉館，並已進行暑假開館時間公告。
- (2) 因應門禁同仁異動，協助撰寫開閉館作業流程文件，以利本次及往後新到任門禁同仁學習相關事宜。
- (3) 因應勞基法重要修正降低基本工時，但本館開館時間維持不變，未來因基本工時降低門禁同仁工時超出基本工時將需要支付加班費用，為減少加班費用支出，經過全年輪班試算及與門禁同仁溝通協調，擬調整部分值班時間，總館週六、日第二班值班時間改為16:30-20:30，於今年6月起試行。
- (4) 5月中旬起開始辦理大學部班級統一離校手續，完成系統事先設定條件，以利迅速完成手續。今年與國際暨兩岸事務處溝通協調，由本組以清冊送交國際處使國際交換生統一離校手續，免除學生逐一個人辦理離校手續及櫃台擁塞狀況。
- (5) 為便利本校師生利用暑假期間從事研究或休閒閱讀自6月6日(一)起所借閱圖書到期日設定開學後9月26日(一)歸還，以網頁公告鼓勵讀者借書。
- (6) 完成主計室同仁會同總務處同仁查核本處104-105年圖書業務收據。
- (7) 協調採編組與世杰，將新書、新片在分館展示，以饗寶山分館在地讀者，新片部分已於本月份開始；新書部分將在下一梯次新書近館並於總館展示後再開始。
- (8) 舉辦105年第一次志工會議，於會議中完成「國立彰化師範大學圖書與資訊處圖書館志工值勤管理辦法」修正。
- (9) 辦理四場研究生論文上傳說明會，計125人參加。
- (10) 完成華藝資料庫研究生授權資料及電子全文轉轉檔資料送交(104年9月1日至105年5月27日)計16件。

- (11) 近期博碩士論文系統向廠商反映系統問題或修正計 7 件，包括轉出 MARC21 檔亂碼、隱藏摘要論文轉出 xml 檔錯誤、國圖授權書輸出畫面、暫存檔轉檔、本校授權書及審核通過畫面文字修正等問題，已全部處理完畢。
- (12) 總館 3 樓監視系統數只類比監視鏡頭同時故障，經請廠商查修並於 4 月中旬更換三樓供電箱之無熔線斷路器後，發現仍有一具 2 樓中庭之攝影鏡頭故障，為鏡頭本身問題，已由廠商另行於 5 月初修復完成。
- (13) 總館數位監視系統主機校時功能故障，請廠商修復完成。
- (14) 目前討論室乙供學生使用之投影機因燈泡故障無法使用，該投影機為 101 年 12 月採購入館，已超過保固年限，而經上網詢價，該款投影機燈泡更換費用約需 7,000 元（新機約需 2 萬餘元），因年初館內監視鏡頭故障維修，加上辦公區整修、防盜系統紅外線感應器維修等零星維護案，故本年度本組預算編列之相關設備維護經費已用罄，請示是否可於今年度進行投影機維修，或待明年再編列經費進行維修？

圖資長裁示：

- i. 以維持正常使用為目標，請廠商儘快報價維修。

- (15) 本館視聽資料館藏原以公播版影片為主，自 104 年開始採購非公播版影片，因非公播版影片價錢低廉，可採購之視聽資料較往年多，可大幅增加館藏量服務讀者。但目前視聽室館藏空間有限，經詢問採編組承辦人，預計每年採購 600 件視聽資料，而目前視聽室架位約尚可容納 2,900 件視聽資料，依此推估，若維持每年採購 600 件以下視聽資料的策略，不新製陳列櫃時，視聽室之館藏架位空間約於 5 年滿架。

圖資長裁示：

- i. 為服務讀者，視聽媒體採購重點仍以讀者薦購為主。
- ii. 如有需要，仍需採買陳列櫃。
- iii. 舊式錄影帶（VHS）因其甚少相關設備可供播放，可視情況進行報廢。

三、採錄編目組

(1) 持續進行 104 年度「購置教學研究相關圖書儀器及設備改

經費別	項目	核定經費	執行進度	餘額
	IEL	2,919,000	2,872,633	46,367
	EBSCOhost	1,931,000	1,879,378	51,622
教育部補助款	中文圖書	400,000	484,970	(-84,970)
	西文圖書	600,000	170,622	429,378
	視聽媒體	150,000	139,197	10,803
	合計	6,000,000	5,546,800	453,200
本校配合款	CEPS電子期刊	308,700	303,975	4,725
	JCR期刊引用評鑑	401,300	400,649	651
	合計	710,000	704,624	5,376

善計畫」教育部補助款 600 萬計畫，執行率達 85%，持續進行圖書與視聽媒體採購。各項經費使用狀況如下：

(2) 期刊業務

- I. 106 年系所期刊薦購調查於 5/10~6/15 進行，至截止日為止共 25 個系所回覆，其餘未回覆之系所將再個別聯繫。
- II. 進行現有紙本期刊轉訂電子期刊之評估作業。

(3) 電子資源業務

- I. 本校加入 2016 上半年 TEBSO 台灣電子書供給合作社聯盟，委託逢甲大學辦理共購共享 iRead eBook 華藝電子書，於 5 月 23 日決標，共 21 校聯盟，每校分擔 284,000 元。
- II. EndNote 書目管理，辦理 2 次開標作業，已於 6 月 14 日決標。

(4) 電子資源查詢平台雙語化，預計於 6/24 進行系統升級，屆時中西文電子資源可達個別呈現之效益。

四、 網路與資訊系統管理組

- (1) 為增加校園網路對外頻寬的線路負載平衡器採購案已獲校長批准，目前已進入總務處辦理招標程序，預計新學期開學前完成此案。
- (2) 新圖書館自動化系統採購經費已通過校務基金管理委員會審核，目前健彥撰寫招標文件中。
- (3) 有關教育體系資通安全(ISMS)與個人資料(PIMS)管理制度聯合輔導意願申請，申請文件已完成，若無修正意見預計 6/30 前送出申請。申請通過後，將派請桂綺及健彥前往上課，除此之外，因個資為全校性業務，屆時將會請祕書室派員參與課程。

圖資長裁示：

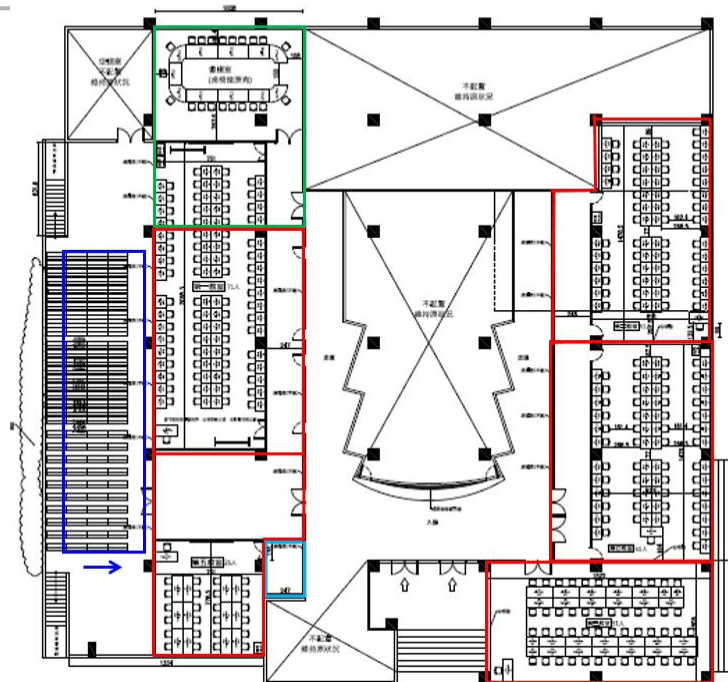
- I. 圖資處為 ISMS 及 PIMS 的業務承辦單位，祕書室為本校對口單位，待申請通過後，應正式告知祕書室。

- (4) B1 電腦教室規畫如圖。

電腦教室搬遷規畫



- 電腦檢修區
- 電腦教室
- 會議室
- 密集書架



I. 密集書架區因考慮漏水問題，將往右移動。

讀者服務組婉佳組長：

1. 密集書架區往右移動後，走道將變小，需考量是否利於書車行動。

圖資長裁示：請有物與健彥協同廠商丈量密集書架區移動應保留多少空間或和何移動書架區，以利書車及人員移動。

2. B1 增設電腦教室後將成為開放空間，其密集書架區中的期刊合訂本需改採閉架式，將造成 1F 圖書館櫃檯管理人員工作負擔，當有讀者需取用期刊合訂本時，櫃檯人員需兩邊來回服務讀者，工作負擔將加重。

圖資長裁示：

1. 電腦教室工讀生服務台設於演講廳前，如有單位在上課時間借用演講廳辦理活動，其報名簽到處將與服務台位置有所衝突，規劃時應一併考慮。

2. 多功能會議室空間大小規劃時應考慮是否能容納常用單位人數。

3. B1 電腦教室規劃涉及讀者服務組業務（密集書區位置調整），請網路與資訊系統管理組與讀者服務組討論可行方案後，再提請會議討論。

4. 為降低學生使用電腦教室之影響，執行期程以暑假期間為主要考量。

(5) 國立彰化師範大學資訊安全管理要點修訂。

（參閱附件一）

(6) 電腦教室學生遺失物品在電腦教室服務櫃台關閉時可否移置於一樓失物招領區，提請討論。

補充：今年 6/7 晚上 10 時 40 分，資管系學生打電話向同仁反應其摩托車鑰匙遺漏在電腦教室，無法騎摩托車返家。當下時間已超過電腦教室工讀時間，工讀生皆已離開，且教室皆已關閉上鎖。

建議：因圖書值班至凌晨 12 時，未來是否在五樓工讀生下班時，一併將同學遺落於電腦教室物品移交給圖書館櫃台失物招領區，以利同學領取。

圖資長裁示：

請讀服組協助處理，但需請工讀生建立失物清冊，屆時清冊連同失物於下班時移交給圖書館櫃檯值班人員供學生招領。至上班日若尚有未領取之失物，則將失物與清冊移交電腦教室工讀生點收。

五、 系統開發組

- (1) 研發處「專兼任助理系統」新增需求訪談已完成，原考慮在舊系統架構上修改，但因需求大幅變更，考慮程式撰寫的方便性，經評估後有可能會重新改寫。
- (2) 研發處擬建置「研究管理系統」，預計將教師學術歷程系統(ET)的研究資料移至新系統共用，增加資料審核及教師申請研究成果獎勵功能。
- (3) 教務處「離校申請系統」各單位之標準作業流程均已收齊，下一步將於暑假開始後進行個別訪談。

圖資長裁示：

I. 進修學院相當重視此系統。

II. 需求訪談需確認系統是否真能減輕作業人員的負擔，莫為了資訊化而大費周章寫成系統，卻又沒有減輕作業人員的 loading。

- (4) App 新增教師輸入成績功能。
- (5) 開放文件教育訓練預計於 6/22(三)、6/23(四)下午各舉辦一場。近日文書組來文，請本處填寫相關調查資料，會與文書組再溝通，本處僅支援教育訓練部份。

圖資長裁示：

ODF 推廣及問卷調查為業務單位進行，本處僅支援教育訓練部份。此相關會議決議記錄再請文書組提供，並公告予圖資處同仁知曉。

參、列管事項執行進度：

一、 綜合業務組

- (1) 本棟建築物外牆名稱字樣形式、大小，請廠商提供相關字樣形式及大小，進行評估與討論。
- (2) B1 二手書區樓梯漏水處會請總務處，偕同專業技師進行會勘，由專業人員提供解決方案後，再行討論。
- (3) 請電梯維護廠商將超載警示音音量調大
- (4) 因電梯建置年份已久，且其使用量大，務必與營繕組及維護廠商確認是否有安全疑慮？應如何調校。
- (5) 本期台銀標結束在即，請確認電腦教室更換設備的執行期程。
- (6) 確認新增對外線路執行期程。
- (7) 請概算明年度工讀金費用，並確認相關經費。

二、 網路與資訊系統管理組

- (1) B1 電腦教室規劃涉及讀者服務組業務（密集書區位置調整），請網路與資訊系統管理組與讀者服務組討論可行方案

三、 系統開發組

- (1) 請仁德組長評估目前系統開發維護人力是否足夠或不足。

肆、討論事項：

- 一、 七月八月適逢學校暑假期間，主管會議暫不召開，俟開學前再行召開，召開日期暫訂 2016/9/8。
- 二、 因目前二手書交換區位於圖書館 B1，容易因滲水問題導致書籍受損，未來預計參考中山大學規劃二手書交換平台，可方便讀者直接透過網路查詢有何二手書籍可供索取或交換。
- 三、 圖資處對於同仁受訓計劃採取支持立場，冀望同仁受訓完畢後，亦可對本處提供新觀念，讓圖資處可保持一直進步的動力。

伍、臨時動議：無。

陸、散會(下午 15：20)

附件一、

修正規定	現行規定	說明
<p>三、資訊安全政策（三）本要點應適時評估，以順應技術、業務等相關環境之趨勢，確保實務作業之有效性。</p>	<p>三、資訊安全政策（三）本要點應定期評估，以順應技術、業務等相關環境之趨勢，確保實務作業之有效性。</p>	<p>配合現況做文字修訂。</p>
<p>四、資訊安全組織及權責（一）為統籌、協調、研議本校各項資訊安全之政策、計畫及資源調度，並考量實務推行效率與組織簡化，由本校各單位 IP 管理者或指定專責人員負責各單位資通安全事件通報、協助執行安全預防、危機處理及緊急應變等工作之職掌。（二）各項電腦軟硬體設備、應用系統、網路通訊之安全計畫、緊急應變計畫及技術規範之研議、訂定、建置及評估等，由所屬資訊或管理單位負責辦理。</p>	<p>四、資訊安全組織及權責（一）為統籌、協調、研議本校各項資訊安全之政策、計畫及資源調度，並考量實務推行效率與組織簡化，由本校網路委員會委員附加負責各單位資通安全事件通報、協助執行安全預防、危機處理及緊急應變等工作之職掌，以組成本校資通安全小組。（二）由本校各單位網路委員兼辦各項資料之安全需求研議、使用管理與保護等事項。（三）各項電腦軟硬體設備、應用系統、網路通訊之安全計畫、緊急應變計畫及技術規範之研議、訂定、建置及評估等，由所屬資訊或管理單位負責辦理。</p>	<p>1.配合現況做文字修訂並刪除（二）條文。 2.點次遞移。</p>

修正規定	現行規定	說明
<p>五、資產分類與控管各單位對於重要的資產(含資訊、軟體、實體等)均指定專人負責，並建置資產清冊且隨時更新。</p>	<p>五、資產分類與控管各單位對於重要的資產(含資訊、軟體、實體)均指定專人負責，並建置資產清冊且隨時更新。</p>	<p>加列文字。</p>
<p>六、人員安全管理及教育訓練 (五) 各單位資訊安全人力或經驗如有不足，得洽請學者專家、專業機關 (構) 或本校圖書與資訊處提供顧問諮詢服務。</p>	<p>六、人員安全管理及教育訓練 (五) 各單位資訊安全人力或經驗如有不足，得洽請學者專家、專業機關 (構) 或本校電子計算機中心提供顧問諮詢服務。</p>	<p>單位名稱修訂。</p>
<p>七、電腦系統實體及環境安全管理 (五) 本校各單位電腦系統安全管理 1. 校內使用者端電腦系統對校外網路之存取，僅限於使用服務，禁止對外提供商業相關網路服務。 2. 伺服器應使用合法授權之軟體，並經常修補安全漏洞。 3.資料備份：(1) 執行必要的資料及軟體備份，以便發生災害或是儲存媒體失效時，可迅速回復正常作業。(2) 應定期測試備份資料，以確保備份資料之可用性及時效性。</p>	<p>七、電腦系統實體及環境安全管理 (五) 本校各單位電腦系統安全管理 1. 校內使用者端電腦系統對校外網路之存取，僅限於使用服務，禁止對外提供網路相關服務。 2.本校各類電腦伺服器建置必須事先向電子計算機中心提出申請，並由電子計算機中心資訊系統組及通訊網路組負責監督。 3.伺服器應使用合法授權之軟體，並經常修補安全漏洞。</p>	<p>1.配合現況做文字修訂並刪除 2.條文。 2.點次遞移。 3.加列條文。</p>

修正規定	現行規定	說明
<p>七、電腦系統實體及環境安全管理（八）公務用電腦： 1.應啟用螢幕保護程式，設定螢幕保護密碼，並將螢幕保護啟動時間設定為十分鐘以內。 2.應安裝防毒軟體，定期更新病毒碼。 3.在不影響系統正常運作下，應定期更新修正程式，修補系統漏洞。 4.應遵守智慧財產權，使用合法授權軟體。</p>		<p>加列條文強化公務用電腦之資訊安全防護。</p>
<p>八、網路、通訊與操作管理（一）各單位利用公眾網路傳送資訊或進行交易處理，應遵守「台灣學術網路管理規範」；（九）本校圖書與資訊處應配合教育部定期檢測網路運作環境之安全漏洞、公告有關網路安全之事項、定期檢討網路安全控管事項之執行。（十）本校圖書與資訊處應公告有關電腦作業系統及應用軟體安全之事項。</p>	<p>八、網路、通訊與操作管理（一）各單位利用公眾網路傳送資訊或進行交易處理，應遵守「台灣學術網路使用規範」；（九）本校由電子計算機中心通訊網路組應配合行政院資通安全小組定期檢測網路運作環境之安全漏洞、公告有關網路安全之事項、定期檢討網路安全控管事項之執行。（十）本校由電子計算機中心資訊系統組應公告有關電腦作業系統</p>	<p>1.規範名稱修訂。 2.配合現況做單位名稱及文字修訂。 3.加列條文。</p>

修正規定	現行規定	說明
<p>(十一) 關於個人資料的蒐集、處理、利用及相關的申請登記、損害賠償、處罰等事宜應依個人資料保護法等相關法令規定辦理。</p>	<p>及應用軟體安全之事項。</p>	
<p>九、系統存取控制(四) 各單位離職、解聘、不續聘或停聘人員，應限期內停止使用校內各項資訊資源之所有權限，並列入人員離職必辦之手續。各單位人員職務異動，應依系統存取授權規定，限期調整其權限。</p>	<p>九、系統存取控制(四) 各單位離職、解聘、不續聘或停聘人員，應立即停止使用校內各項資訊資源之所有權限，並列入人員離職必辦之手續。各單位人員職務異動，應依系統存取授權規定，限期調整其權限。</p>	<p>配合現況做文字修訂。</p>
<p>十、系統開發與維護 (七) 為避免影響系統正常運作，各單位於系統開發與維護階段應建立系統測試環境，完成系統測試後上線運作。(八) 本校校務行政系統與資料之資訊安全管理與維護，應由系統管理單位負責，其資訊安全規定如下：</p>	<p>十、系統開發與維護 (七) 本校校務行政系統與資料之資訊安全管理與維護，均由本校電子計算機中心軟體工程組與相關使用單位負責，電子計算機中心主任負責督導，其資訊安全規定如下：</p>	<p>1.加列條文。 2.配合現況做文字修訂。 3.點次遞移。</p>
<p>十一、永續經營管理 (二) 本校電腦、網路及校務行政等系統之業務永續運作計畫 2.本校校務行政系</p>	<p>十一、永續經營管理 (二) 本校電腦、網路及校務行政等系統之業務永續運作計畫 2.本校校務行政系</p>	<p>配合現況做文字修訂。</p>

修正規定	現行規定	說明
<p>統、主幹網路系統之永續運作計畫及緊急應變與回復作業程序之訂定、管理與維運，應由本校業務主管單位負責。（三）各單位應建立資訊安全事件緊急處理機制，在發生資訊安全事件時，應依處理程序，通知系統管理人員，並立即向本校資通安全通報窗口通報，於採取反應措施後，陳報本校資訊安全長，必要時向上級或國家資通安全會報通報，或由本校聯繫檢警調機關偵查。</p>	<p>統、主幹網路系統之永續運作計畫及緊急應變與回復作業程序之訂定、管理與維運，均由本校電子計算機中心負責，電子計算機中心主任負責督導。</p> <p>（三）各單位應建立資訊安全事件緊急處理機制，在發生資訊安全事件時，應依處理程序，通知單位網管人員或單位資安負責人員，並立即向本校電子計算機中心資通安全通報窗口通報，於採取反應措施後，陳報電子計算機中心主任，必要時向上級或國家資通安全會報通報，或由本校聯繫檢警調機關偵查。</p>	
<p>十二、本要點經行政會議討論通過，陳請校長核定後施行，修正時亦同。</p>	<p>十二、本要點經行政會議討論通過，陳請校長核定後實施，修正時亦同。</p>	<p>文字修訂。</p>

國立彰化師範大學資訊安全管理要

點（修正後條文）

94年 9月 14日行政會議通過待
提 105年 x月 x日行政會議

一、目的為強化本校各單位暨所屬單位資訊安全管理，確保資料、系統、設備及網路安全，保障教職員工生權益，依據行政院所屬各機關資訊安全管理要點及相關規定，訂定國立彰化師範大學資訊安全管理要點（以下簡稱本要點）。

二、通則

本要點適用對象為本校各單位（含宿舍）暨附屬單位。三、資訊安全政策（一）資訊安全之範圍分列如下：

1.管理制度， 2.作業流程， 3.人員， 4.軟體， 5.應用系統， 6.電腦作業系統， 7.硬體， 8.通訊設備，9.資料、文件、媒體的儲存及 10.實體設施等。

（二）資訊安全管理之範圍分列如下：

1. 資訊安全組織及權責。
2. 資產分類與控管。
3. 人員安全管理及教育訓練。
4. 電腦系統實體及環境安全管理。
5. 網路、通訊與操作管理。
6. 系統存取控制。
7. 系統開發與維護。

8.永續經營管理。（三）本要點應適時評估，以順應技術、業務等相關環境之趨勢，確保實務作業之有效性。（四）本要點應以書面、電子郵件或其他方式告知全體教職員工生、連線作業之公私機構及提

供資訊服務之廠商共同遵行。（五）本要點實施時如有必要，各單位應訂定說明文件，如管理規範、作業程序、資訊安全控

管文件等。（六）資訊安全應定期或不定期進行稽核。四、資訊安全組織及權責（一）為統籌、協調、研議本校各項資訊安全之政策、計畫及資源調度，並考量實務推行效率

與組織簡化，由本校各單位 IP管理者或指定專責人員負責各單位資通安全事件通報、協助執行安全預防、危機處理及緊急應變等工作之職掌。（二）各項電腦軟硬體設備、應用系統、網路通訊之安全計畫、緊急應變計畫及技術規範之研

議、訂定、建置及評估等，由所屬資訊或管理單位負責辦理。（三）各項資料之安全需求、使用管理及保護等事項，由業務承辦單位負責辦理。（四）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。（五）附屬單位必須指派資訊或適當單位負責資訊安全管理，並依本校規定辦理。（六）委外與第三方[協力廠商]依據合約內容配合，負責委外或協力部份之資訊安全運作。

五、資產分類與控管

各單位對於重要的資產(含資訊、軟體、實體等)均指定專人負責，並建置資產清冊且隨時更新。六、人員安全管理及教育訓練 (一) 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，並進行必要的考核。(二) 各單位對可存取機密性與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。(三) 各單位應針對管理、業務及資訊等不同工作類別之需求，定期辦理資訊安全教育訓練或
宣導，建立員工資訊安全認知，提升單位資訊安全水準。(四) 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。(五) 各單位資訊安全人力或經驗如有不足，得洽請學者專家、專業機關(構)或本校圖書與
資訊處提供顧問諮詢服務。(六) 各單位負責重要系統之管理、維護、設計及操作之人員，應妥
適分散權責，並視需要建
立制衡機制，實施人員輪調，建立人力備援制度。(七) 各單位主管應負責督導所屬員工之資訊
安全作業，防範不法及不當行為。七、電腦系統實體及環境安全管理 (一) 設置電腦機房及重要
地區之單位，對於進出人員必須由管理人員作必要之限制及監督其

活動、各項安全設備必須定期檢查，並訂定電腦機房安全管理規定，員工必須施予適當
的安全設備使用訓練。(二) 各單位設置有機密性工作站或伺服器者必須由專人管理。(三) 各
單位應依著作權等相關法規或契約規定，複製及使用軟體，並應依據「政府所屬各級

行政機關電腦軟體管理作業要點」，建立軟體使用管理制度。(四) 各單位設備之維護必須由授
權之維護人員執行，應採行必要的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。(五) 本
校各單位電腦系統安全管理

- 1 校內使用者端電腦系統對校外網路之存取，僅限於使用服務，禁止對外提供商業相關網路服務。

- 2 伺服器應使用合法授權之軟體，並經常修補安全漏洞。

- 3 資料備份：

- (1) 執行必要的資料及軟體備份，以便發生災害或是儲存媒體失效時，可迅速回復正常作業。

- (2) 應定期測試備份資料，以確保備份資料之可用性及時效性。(六) 各單位對於重要之攜帶型的電腦設備須有嚴謹的保護措施(如設通行碼、檔案加密、專人看管)並落實執行。(七) 具敏感性或機密性資料之單位其資訊財產攜出辦公處所，必須訂有安全之攜出管理規

則。(八) 公務用電

腦：

1. 應啟用螢幕保護程式，設定螢幕保護密碼，並將螢幕保護啟動時間設定為十分鐘以內。

- 2.應安裝防毒軟體，定期更新病毒碼。
 - 3.應定期或即時(real time)掃瞄電腦系統及資料儲存媒體。
 - 4.在不影響系統正常運作下，應定期更新修正程式，修補系統漏洞。
- 5.應遵守智慧財產權，使用合法授權軟體。八、網路、通訊與操作管理（一）各單位利用公眾網路傳送資訊或進行交易處理，應遵守「台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。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。

（二）各單位與外界網路連接之網點，必要時得以防火牆或其他安全設施，控管外界與單位內部網路之資料傳輸及資源存取。

（三）各單位開放外界連線作業之資訊系統，必要時得視資料及系統之重要性及價值，採用資料加密、身分鑑別、電子簽章、防火牆及安全漏洞偵測等不同安全等級之技術或措施，防止資料及系統被侵入破壞、竊改、刪除及未經授權之存取。

（四）各單位開放外界連線作業之資訊系統，必要時得以代理伺服器等方式提供外界存取資料，避免外界直接進入資訊系統或資料庫存取資料。

（五）各單位利用網際網路及全球資訊網公布及流通資訊，應實施資料安全等級評估，機密性、敏感性及未經當事人同意之個人隱私資料及文件，不得上網公布。單位網站存有個人資料及檔案者，應加強安全保護措施，防止個人隱私資料遭違法或不當之竊取使用。

（六）本校建置有郵件伺服器之單位應訂定電子郵件使用規定，機密性資料及文件，不得以電子郵件或其他電子方式傳送。機密性資料以外之敏感性資料及文件，如有電子傳送之需要，本校應視需要以適當之加密或電子簽章等安全技術處理。單位業務性質特殊，須利用電子郵件或其他電子方式傳送機密性資料及文件者，得採用權責主管機關認可之加密或電子簽章等安全技術處理。

（七）各單位採購資訊軟硬體設施，應依國家標準或權責主管機關訂定之政府資訊安全規範，研提資訊安全需求，並列入採購規格。各單位發展及應用加密技術，應採用權責主管機關認可之密碼模組產品。各單位採購外國產製之密碼模組產品，應請廠商提出輸出許可或相關授權文件，確保密碼模組之安全性，並避免採購金鑰代管或金鑰回復功能之產品。

（八）各單位應視需求建置防火牆、防毒軟體及入侵偵防系統，重要伺服主機應單獨外掛硬體防火牆、防毒軟體及入侵偵防系統。

（九）本校圖書與資訊處應配合教育部定期檢測網路運作環境之安全漏洞、公告有關網路安全之事項、定期檢討網路安全控管事項之執行。

（十）本校圖書與資訊處應公告有關電腦作業系統及應用軟體安全之事項。

（十一）關於個人資料的蒐集、處理、利用及相關的申請登記、損害賠償、處罰等事宜應依個人資料保護法等相關法令規定辦理。

九、系統存取控制

（一）凡建置多人使用之應用系統之單位應訂定系統存取政策及授權制度，對電腦資料庫及檔案應建立分級(機密及安全等級)管理制度，並以書面、電子或其他方式告知教職員工生及使用者之相關權限及責任。

(二) 各項正式作業之電腦系統操作及資料處理，由各權責單位指定專人負責建檔、核對、更新、審查及維護電腦資料之正確性。資訊系統發展人員非經核准不得操作使用或更改已正式作業之系統檔案與資料。

(三) 電腦資料庫及檔案，應按不同業務範圍及使用權限，分別設定目錄、識別保護碼；重要或具機密性資料在建檔或提供使用時，應加設通行密碼、使用權限碼，以確保資料安全，且通行密碼應經常更新。

(四) 各單位離職、解聘、不續聘或停聘人員，應限期內停止使用校內各項資訊資源之所有權限，並列入人員離職必辦之手續。各單位人員職務異動，應依系統存取授權規定，限期調整其權限。

(五) 各單位應建立教職員工生及使用者註冊管理制度，加強通行密碼管理，並要求定期更新；其通行密碼之更新週期，由各單位視作業系統及安全管理需求決定。對單位內外擁有系統存取特別權限之人員，應建立使用人員名冊，加強安全控管，並縮短密碼更新週期。

(六) 各單位若開放外界連線作業，應事前簽訂契約或協定，明定其應遵守之資訊安全規定、標準、程序及應負之責任。(七) 需由系統服務廠商以遠端登入方式進行系統維護之單位，應加強安全控管，並建立人員名冊，課其相關安全保密責任。(八) 各單位資料或系統需委外建檔者，不論在單位內外執行，均應採取適當及必要之安全管制措施，防止資料被竊取、竄改、販售、洩漏及不當備份等情形發生。(九) 凡建置多人使用之應用系統之單位應確立系統稽核項目，建立資訊安全稽核制度，定期

或不定期進行資訊安全稽核作業；系統中之稽核紀錄檔案，應禁止任意刪除及修改。十、系統開發與維護(一) 自行開發或委外發展系統之單位，應在系統生命週期之初始階段，即將資訊安全需求納

入考量；系統之維護、更新、上線執行及版本異動等作業，應予安全管制，避免不當軟體、暗門及電腦病毒危害系統安全。(二) 辦理資訊業務委外作業之單位，應於事前研提資訊安全需求，明定廠商之資訊安全責任及保密規定，並列入契約，要求廠商遵守並定期考核。

(三) 各單位對廠商之軟硬體系統建置及維護人員，應規範及限制其可接觸之系統與資料範圍，並嚴禁核發長期性之系統辨識碼及通行密碼。各單位基於實際作業需要，得核發短期性及臨時性之系統辨識及通行密碼供廠商使用。但使用完畢後應立即取消其使用權限。

(四) 各單位委託廠商建置及維護重要軟硬體設施時，應在單位相關人員監督及陪同下始得為之。(五) 各單位自行開發或委外發展系統之變更作業，應建立控管制度，並建立紀錄，以備查考。(六) 各單位於系統開發與維護階段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。(七) 為避免影響系統正常運作，各單位於系統開發與維護階段應建立系統測試環境，完成系統測試後上線運作。(八) 本校校務行政系統與資料之資訊安全管理與維護，應由系統管理單位負責，其資訊安全規定如下：

- 1.校務行政網路應適度與宿網、教學研究網路系統隔離，若使用網際網路必須使用合適之隔離或加密措施。

2.所有校務行政電腦資料應具備異動紀錄，紀錄異動時間與異動者等資料。

3.所有校務行政電腦資料必須有復原計畫，復原計畫所需時間與正確性必須符合業務所需，且每年至少確實執行一次。

十一、永續經營管理

(一)各單位應評估各種人為及天然災害對單位正常業務運作之影響，視需要訂定業務永續運作計畫、緊急應變與回復作業程序及相關人員之權責，並定期演練及調整更新計畫。(二)本校電腦、網路及校務行政等系統之業務永續運作計畫

1.本校校務行政系統、各類伺服器(含電子郵件等)、網路系統與電腦系統中資料庫、應用程式與資料，必須備份分開存放並且提供備援運轉服務，以便當設備發生運轉問題，備援設備可以立即接手取代繼續運轉，以提供本校師生更完善的電腦網路環境，達到支援教學、研究不間斷。

2.本校校務行政系統、主幹網路系統之永續運作計畫及緊急應變與回復作業程序之訂定、管理與維運，應由本校業務主管單位負責。

(三)各單位應建立資訊安全事件緊急處理機制，在發生資訊安全事件時，應依處理程序，通知系統管理人員，並立即向本校資通安全通報窗口通報，於採取反應措施後，陳報本校資訊安全長，必要時向上級或國家資通安全會報通報，或由本校聯繫檢警調機關偵查。

十二、本要點經行政會議討論通過，陳請校長核定後施行，修正時亦同。

國立彰化師範大學資訊安全管理要

點（現行條文）

94年 9月 14日行政會議討論通過

一、目的為強化本校各單位暨所屬單位資訊安全管理，確保資料、系統、設備及網路安全，保障教職員工生權益，依據行政院所屬各機關資訊安全管理要點及相關規定，訂定國立彰化師範大學資訊安全管理要點（以下簡稱本要點）。

二、通則本要點適用對象為本校各單位（含宿舍）暨附屬單位。

三、資訊安全政策（一）資訊安全之範圍分列如下：

1.管理制度， 2.作業流程， 3.人員， 4.軟體， 5.應用系統， 6.電腦作業系統， 7.硬體， 8.通訊設備，9.資料、文件、媒體的儲存及 10.實體設施等。

（二）資訊安全管理之範圍分列如下：

- 一. 資訊安全組織及權責。
- 一. 資產分類與控管。
- 一. 人員安全管理及教育訓練。
- 一. 電腦系統實體及環境安全管理。
- 一. 網路、通訊與操作管理。
- 一. 系統存取控制。
- 一. 系統開發與維護。

8.永續經營管理。（三）本要點應定期評估，以順應技術、業務等相關環境之趨勢，確保實務作業之有效性。（四）本要點應以書面、電子郵件或其他方式告知全體教職員工生、連線作業之公私機構

及提供資訊服務之廠商共同遵行。（五）本要點實施時如有必要，各單位應訂定說明文件，如管理規範、作業程序、資訊安全控管文件等。（六）資訊安全應定期或不定期進行稽核。四、資訊安全組織及權責

（一）為統籌、協調、研議本校各項資訊安全之政策、計畫及資源調度，並考量實務推行效率與組織簡化，由本校網路委員會委員附加負責各單位資通安全事件通報、協助執行安全預防、危機處理及緊急應變等工作之職掌，以組成本校資通安全小組。

（二）由本校各單位網路委員兼辦各項資料之安全需求研議、使用管理與保護等事項。

（三）各項電腦軟硬體設備、應用系統、網路通訊之安全計畫、緊急應變計畫及技術規範之研議、訂定、建置及評估等，由所屬資訊或管理單位負責辦理。（四）各項資料之安全需求、使用管理及保護等事項，由業務承辦單位負責辦理。（五）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。（六）附屬單位必須指派資訊或適當單位負責資訊安全管理，並依本校規定辦理。（七）委外與第三方[協力廠商]依據合約內容配合，負責委外或協力部份之資訊安全運作。

五、資產分類與控管各單位對於重要的資產(含資訊、軟體、實體)均指定專人負責，並建置資產清冊且隨時更新。

六、人員安全管理及教育訓練 (一) 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，並進行必要的考核。(二) 各單位對可存取機密性與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。(三) 各單位應針對管理、業務及資訊等不同工作類別之需求，定期辦理資訊安全教育訓練或宣導，建立員工資訊安全認知，提升單位資訊安全水準。(四) 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。(五) 各單位資訊安全人力或經驗如有不足，得洽請學者專家、專業機關(構)或本校電子計算機中心提供顧問諮詢服務。(六) 各單位負責重要系統之管理、維護、設計及操作之人員，應妥適分散權責，並視需要建立制衡機制，實施人員輪調，建立人力備援制度。(七) 各單位主管應負責督導所屬員工之資訊安全作業，防範不法及不當行為。

七、電腦系統實體及環境安全管理 (一) 設置電腦機房及重要地區之單位，對於進出人員必須由管理人員作必要之限制及監督其活動、各項安全設備必須定期檢查，並訂定電腦機房安全管理規定，員工必須施予適當的安全設備使用訓練。(二) 各單位設置有機密性工作站或伺服器者必須由專人管理。(三) 各單位應依著作權等相關法規或契約規定，複製及使用軟體，並應依據「政府所屬各級行政機關電腦軟體管理作業要點」，建立軟體使用管理制度。(四) 各單位設備之維護必須由授權之維護人員執行，應採行必要的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。(五) 本校各單位電腦系統安全管理

1. 校內使用者端電腦系統對校外網路之存取，僅限於使用服務，禁止對外提供網路相關服務。

2. 本校各類電腦伺服器建置必須事先向電子計算機中心提出申請，並由電子計算機中心資訊系統組及通訊網路組負責監督。

3. 伺服器應使用合法授權之軟體，並經常修補安全漏洞。(六) 各單位對於重要之攜帶型的電腦設備須有嚴謹的保護措施(如設通行碼、檔案加密、專人看管)並落實執行。(七) 具敏感性或機密性資料之單位其資訊財產攜出辦公處所，必須訂有安全之攜出管理規則。八、網路、通訊與操作管理

(一) 各單位利用公眾網路傳送資訊或進行交易處理，應遵守「台灣學術網路使用規範」；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。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。

(二) 各單位與外界網路連接之網點，必要時得以防火牆或其他安全設施，控管外界與單位內部網路之資料傳輸及資源存取。

(三) 各單位開放外界連線作業之資訊系統，必要時得視資料及系統之重要性及價值，採用資料加密、身分鑑別、電子簽章、防火牆及安全漏洞偵測等不同安全等級之技術或措施，防止資料及系統被侵入破壞、竄改、刪除及未經授權之存取。

(四) 各單位開放外界連線作業之資訊系統，必要時得以代理伺服器等方式提供外界存取資料，避免外界直接進入資訊系統或資料庫存取資料。

(五) 各單位利用網際網路及全球資訊網公布及流通資訊，應實施資料安全等級評估，機密性、敏感性及未經當事人同意之個人隱私資料及文件，不得上網公布。單位網站存有個人資料及檔案者，應加強安全保護措施，防止個人隱私資料遭違法或不當之竊取使用。

(六) 本校建置有郵件伺服器之單位應訂定電子郵件使用規定，機密性資料及文件，不得以電子郵件或其他電子方式傳送。機密性資料以外之敏感性資料及文件，如有電子傳送之需要，本校應視需要以適當之加密或電子簽章等安全技術處理。單位業務性質特殊，須利用電子郵件或其他電子方式傳送機密性資料及文件者，得採用權責主管機關認可之加密或電子簽章等安全技術處理。

(七) 各單位採購資訊軟硬體設施，應依國家標準或權責主管機關訂定之政府資訊安全規範，研提資訊安全需求，並列入採購規格。各單位發展及應用加密技術，應採用權責主管機關認可之密碼模組產品。各單位採購外國產製之密碼模組產品，應請廠商提出輸出許可或相關授權文件，確保密碼模組之安全性，並避免採購金鑰代管或金鑰回復功能之產品。

(八) 各單位應視需求建置防火牆、防毒軟體及入侵偵防系統，重要伺服器主機應單獨外掛硬體防火牆、防毒軟體及入侵偵防系統。。(九) 本校由電子計算機中心通訊網路組應配合行政院資通安全小組定期檢測網路運作環境之安全漏洞、公告有關網路安全之事項、定期檢討網路安全控管事項之執行。(十) 本校由電子計算機中心資訊系統組應公告有關電腦作業系統及應用軟體安全之事項。九、系統存取控制

(一) 凡建置多人使用之應用系統之單位應訂定系統存取政策及授權制度，對電腦資料庫及檔案應建立分級(機密及安全等級)管理制度，並以書面、電子或其他方式告知教職員工生及使用者之相關權限及責任。

(二) 各項正式作業之電腦系統操作及資料處理，由各權責單位指定專人負責建檔、核對、更新、審查及維護電腦資料之正確性。資訊系統發展人員非經核准不得操作使用或更改已正式作業之系統檔案與資料。

(三) 電腦資料庫及檔案，應按不同業務範圍及使用權限，分別設定目錄、識別保護碼；重要或具機密性資料在建檔或提供使用時，應加設通行密碼、使用權限碼，以確保資料安全，且通行密碼應經常更新。

(四) 各單位離職、解聘、不續聘或停聘人員，應立即停止使用校內各項資訊資源之所有權限，並列入人員離職必辦之手續。各單位人員職務異動，應依系統存取授權規定，限期調整其權限。

(五)各單位應建立教職員工生及使用者註冊管理制度,加強通行密碼管理,並要求定期更新;其通行密碼之更新週期,由各單位視作業系統及安全管理需求決定。對單位內外擁有系統存取特別權限之人員,應建立使用人員名冊,加強安全控管,並縮短密碼更新週期。

(六)各單位若開放外界連線作業,應事前簽訂契約或協定,明定其應遵守之資訊安全規定、標準、程序及應負之責任。(七)需由系統服務廠商以遠端登入方式進行系統維護之單位,應加強安全控管,並建立人員名冊,課其相關安全保密責任。(八)各單位資料或系統需委外建檔者,不論在單位內外執行,均應採取適當及必要之安全管制措施,防止資料被竊取、竄改、販售、洩漏及不當備份等情形發生。

(九)凡建置多人使用之應用系統之單位應確立系統稽核項目,建立資訊安全稽核制度,定期或不定期進行資訊安全稽核作業;系統中之稽核紀錄檔案,應禁止任意刪除及修改。

十、系統開發與維護(一)自行開發或委外發展系統之單位,應在系統生命週期之初始階段,即將資訊安全需求納入考量;系統之維護、更新、上線執行及版本異動等作業,應予安全管制,避免不當軟體、暗門及電腦病毒危害系統安全。(二)辦理資訊業務委外作業之單位,應於事前研提資訊安全需求,明定廠商之資訊安全責任及保密規定,並列入契約,要求廠商遵守並定期考核。(三)各單位對廠商之軟硬體系統建置及維護人員,應規範及限制其可接觸之系統與資料範圍,並嚴禁核發長期性之系統辨識碼及通行密碼。各單位基於實際作業需要,得核發短期性及臨時性之系統辨識及通行密碼供廠商使用。但使用完畢後應立即取消其使用權限。(四)各單位委託廠商建置及維護重要軟硬體設施時,應在單位相關人員監督及陪同下始得為之。(五)各單位自行開發或委外發展系統之變更作業,應建立控管制度,並建立紀錄,以備查考。(六)各單位於系統開發與維護階段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。(七)本校校務行政系統與資料之資訊安全管理與維護,均由本校電子計算機中心軟體工程組與相關使用單位負責,電子計算機中心主任負責督導,其資訊安全規定如下:

1. 校務行政網路應適度與宿網、教學研究網路系統隔離,若使用網際網路必須使用合適之隔離或加密措施。
2. 所有校務行政電腦資料應具備異動紀錄,紀錄異動時間與異動者等資料。

3.所有校務行政電腦資料必須有復原計畫,復原計畫所需時間與正確性必須符合業務所需,且每年至少確實執行一次。十一、永續經營管理

(一)各單位應評估各種人為及天然災害對單位正常業務運作之影響,視需要訂定業務永續運作計畫、緊急應變與回復作業程序及相關人員之權責,並定期演練及調整更新計畫。

(二) 本校電腦、網路及校務行政等系統之業務永續運作計畫

1. 本校校務行政系統、各類伺服器(含電子郵件等)、網路系統與電腦系統中資料庫、應用程式與資料，必須備份分開存放並且提供備援運轉服務，以便當設備發生運轉問題，備援設備可以立即接手取代繼續運轉，以提供本校師生更完善的電腦網路環境，達到支援教學、研究不間斷。
2. 本校校務行政系統、主幹網路系統之永續運作計畫及緊急應變與回復作業程序之訂定、管理與維運，均由本校電子計算機中心負責，電子計算機中心主任負責督導。

(三) 各單位應建立資訊安全事件緊急處理機制，在發生資訊安全事件時，應依處理程序，通知單位網管人員或單位資安負責人員，並立即向本校電子計算機中心資通安全通報窗口通報，於採取反應措施後，陳報電子計算機中心主任，必要時向上級或國家資通安全會報通報，或由本校聯繫檢警調機關偵查。

十二、本要點經行政會議討論通過，陳請校長核定後實施，修正時亦同。