國立宜蘭大學 107 學年

個人資料保護推動委員會度第二次會議暨第一次管理審查會議紀錄

日期：民國 107 年 11 月 28 日(星期三)下午 3 點

地點：行政大樓五樓第二會議室

主席：周副校長瑞仁　　紀錄：游佳欣

出席：賴軍維委員(須文宏副學務長代理)、吳寂絹委員(范文南組長代理)、游竹委員(王秀娟副研發長代理)、張介仁委員、江茂欽委員、程安邦委員(湯雅雯組長代理)、陳威戎委員

列席：朱達勇主任、游佳欣、康銘仁

請假：吳中峻委員(請假)、郭芳璋委員(請假)、藍輝榮委員(請假)、黃美嘉委員(請假)、江漢全委員(請假)、林豐政委員(請假)、陶金旺委員(請假)、陳凱俐委員(請假)、黃于飛委員(請假)

壹、主席致詞(略)

貳、報告事項

一、過往管理審查之議案的處理狀態

本校於 107 年導入「個人資料管理制度」，本會議為第一次會議，因此無過往的議案

二、資通訊安全或個資管理要求的變更

日期	利害關係者	主題/內容	備註
107.11.09	教育部（外部）	教育體系資通安全暨個人資料管理規範改版－主要是參考 BS10012:2017 改版讓教版個資規範更為周延，也參考 ISO29151:2017 調整教版資安規範增列個資保護補充指引，規範預定於 2019 年公告適用，讓 2016 年起採用新版規範驗證的受稽單位可於明年順利銜接採用。	今年度申請 106 年版驗證，明年度申請可考慮是否以新版申請驗証。 預訂於明年 8 月公告實施。
	全校師生（內部）	重視個資觀念等原因 ，過去僅用校內內控管理制度管理，今年開始導入個人資料管理制度。	今年五月向中興大學申請並通過個資管理制度導入輔導一案。

三、管理目標與指標量測結果

編號	目標項目	目標	評量方法	評量頻率
目標 1	促進個人資料之合理利用及最小化使用：依我國「個資法」、「個資法施行細則」要求，規範個人資料之蒐集、處理及利用，以避免人格權受侵害，並保護個人資料蒐集、處理、利用、儲存、傳輸、銷毀及國際傳輸之過程			
項目 1	個人資料蒐集、處理、利用程序	檢視個資盤點是否有漏盤情況	每單位個人資料檔案清冊是否有漏盤超過 2 件。	每年
項目 2	個人資料儲存與銷毀	檢視超過保存期限資料銷毀情況	每單位保存的個人資料檔案是否依銷毀期限進行銷毀並留存刪除紀錄。	每年
目標 2	保護本校業務相關之個人資料安全：免於因外在威脅，或內部人員不當之管理與使用，致遭受竊取、竄改、毀損、滅失、或洩漏等風險。			
項目 1	存取控制	檢視個人電腦密碼設定情況及螢幕保護程式設定	每單位抽至少 1 位同仁，檢視個人電腦設定 (1)密碼長度超過 8 碼，半年更新。 (2)螢幕保護程式是否設定。	每年

項目 2	檔案傳輸管理	抽查個人資料進行傳輸過程中是否具備安全控管	每單位抽至少 1 位同仁，檢視其 E-mail 傳送(例加密)情形	每年
目標 3	提升個人資料之保護與管理能力，降低營運風險：創造可信賴之個人資料保護及隱私環境。			
項目 1	管理組織	管理制度是否運行	每年至少召開一次管審會議，審議管理制度及相關議題	每年
項目 2	個人資料事故管理	發生個資外洩之事件	檢核是否發生個資安全事件申訴與通報事件。	每年
目標 4	提升同仁個人資料保護安全意識：每年定期辦理個人資料保護宣導教育訓練，定期針對個人資料流程進行風險評鑑，鑑別可承受風險等級。			
項目 1	教育訓練	檢查個人資料保護宣導或教育訓練次數	每年針對全員辦理一場次個人資料保護相關議題教育訓練。	每年
項目 2	風險評鑑	檢查個人資料風險評鑑，鑑別可承受風險等級。	檢核： (1)每單位每年至少執行一次風險評估 (2)檢核超過可接受風險值單位之風險處理計畫	每年

- 上述為目標量測項目是否合宜，呈請長官核示。
- 目前設定管理目標與指標量測方式，將於 12 月 4 日於受驗證單位進行量測。

四、 內外部稽核結果

於11月7日(星期三)進行個人資料管理制度內部稽核,稽核結果統計:

- 不符合事項：2 項。
- 其他建議：7 項。

五、 個資事故與不符合項目之矯正情形

- 個資事故目前尚無。
- 11 月 7 日內稽核不符合事項之矯正情形：

項次	標準條文/稽核項目	稽核發現	稽正措施
1	B4.1.1	抽查發現個資清冊漏列或蒐集、處理及利用之描述有誤，建議單位檢視業務職掌，重新確認其清冊之正確性與完整性。如： - 校園活動資訊及報名系統-報名名單(電子檔)漏列(圖書資訊館數位學習資源中心)教務行政資訊系統，蒐集階段誤植(教務處註冊課務組) - 工讀生進用表及履歷，保有依據、保存期限誤植(教務處註冊課務組) - 校務資料庫，數量再行評估；備份資料，保有依據、保存期限誤植(圖書資訊館系統設計組) - 保存期限宜再行評估合宜性(學務處學生諮商組、圖書資訊館資訊網路組)	1. 經查核發現部分個人檔案清冊宜強化內容正確性及一致性，請同仁重新檢視業務職掌，確認單位業務作業流程之個人資料流向，更新個資清冊。 2. 同仁為首次進行個資盤點作業，尚未熟悉盤點方式導致，辦理相關教育訓練及宣導作業。
2	B5.2.1	部分單位蒐集當事人個資未有宣告、告知或簽署同意書，如： - 新生入學(教務處註冊課務組) - 磨課師徵件申請(圖書資訊館數位學習資源中心) - 校外人士民眾借書證申請表(圖書資訊館圖資服務組)	1. 至「校務公開專區」/「個人資料保護業務公開專區」,下載「個人資料提供同意書」，依單位內相關業務調整適用之同意書。 2. 辦理相關教育訓練及宣導作業。

- 其他建議及後續改善方式：

項次	其他建議事項	後續改善方式
1	建議單位確認屆滿個資檔案銷毀作業之規劃，或應依本校個資管理程序規定，留存銷毀紀錄。	1. 請各單位確認保存期限已屆滿個人資料檔案，規劃銷毀行程，並依行程進行銷毀作業。 2. 並留存銷毀紀錄。 3. 如無法銷毀者，因依管理程序規定填寫「超過保存期限之個人資料檔案清冊」，並請依設定預定銷毀期限進行銷毀。
2	建議評估目標有效性量測之評量方法之合宜性，如：每單位至少抽查 3 位同仁執行履行個資告知業務。	1. 設定本校個人資料保護管理之目標的評量方式，且評量方式適合本校，且可以量測。 2. 設定評量方式後，提請委員同意。
3	建議組織宜考量強化個人電腦安全性管控措施，如安裝 Winrar、7-Zip 版本問題、螢幕保護程式設定、密碼長度及強度、離職人員帳號管理等部分。	1. 制作軟體安裝或設定文件供同仁使用。 2. 將螢幕保護程式、密碼長度及強度設定…等設定至目標量測方式，並檢核各單位執行情況。
4	宜考量委外管理契約條款項目加強監督管理機制。(契約內無個資要求條款或保密切結書完整度不足)	1. 新設置管理文件「委外專案個人資料保護條款」，新購置系統因要求廠商簽訂並提供保密切結書。 2. 舊購置系統於維護合約簽定時，因要求廠商簽訂「委外專案個人資料保護條款」並提供保密切結書
5	請重新檢視個資告知聲明之內容，如個資蒐集目的；利用期間、對象誤植(圖書資訊館圖資服務組臨時閱覽證申請)	1. 檢視各單位個資告知聲明內容，並修改之。
6	宜再確認風險評鑑作業之適切性，如風險評估表項目評不適用。(圖書資訊館系統設計組-安全防護不足、調閱個資時申請)	1. 請各單位重新檢視個資資產的風險評鑑是否適切。 2. 未來辦理相關教育訓練時，因針對檢核的內容進行更詳細的說明。
7	建議敏感性個人資料宜強化加密保護機制。(教務處註冊課務組-新生入學資料電子檔)	1. 設定為目標量測方式，並檢核各單位執行情況。 2. 制作檔案加密相關設定文件供同仁使用。

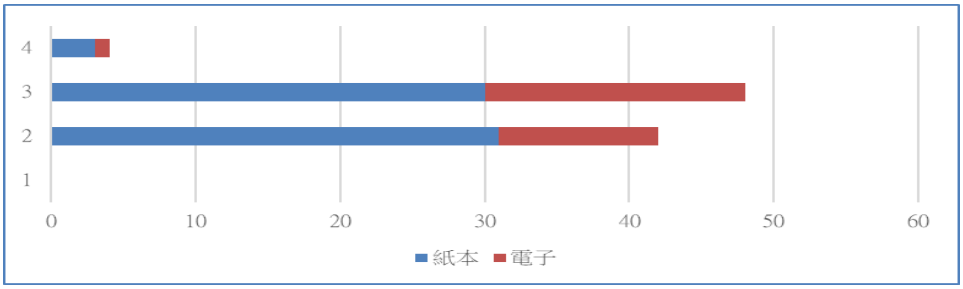
六、 風險評鑑結果及風險處理計畫執行進度

- 今年度風險評鑑結果

  受稽核驗證單位依據「國立宜蘭大學個人資料風險評鑑評估表」執行個人資料檔案清查，共辨識出 94 項個資資產，並由個人資料保護推動委員會審核。

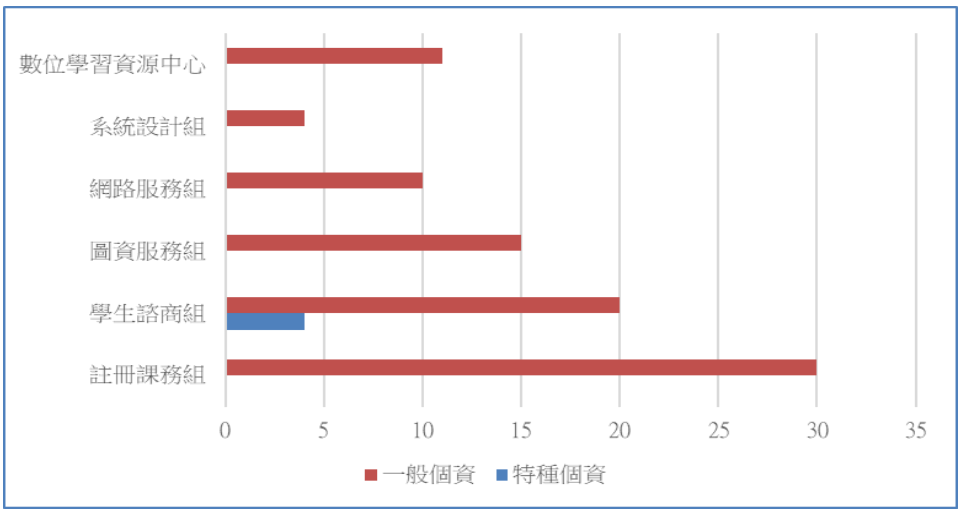
  - 個資資產辨識與價值評估結果

    依據各項資產類型及資產價值評估(個資範圍評估值，由低至高依序為 1 至 4 分)，統計結果如下：



  - 個資資產與特種個資評估結果

    依各單位是否擁有特種個資評估，統計結果如下：



- 個資資產風險分布

  依據各組個資資產之風險值由低至高分布情況如下：

單位/風險值	4	6	8	9	10	12	15	16	18	20	21	總計
註冊課務組	0	6	5	6	3	5	4	0	1	0	0	30
學生諮商組	2	4	3	0	3	2	5	1	2	1	1	24
圖資服務組	0	0	1	0	4	2	6	0	0	0	2	15
網路服務組	4	6	0	0	0	0	0	0	0	0	0	10
系統設計組	0	0	0	0	0	0	1	0	3	0	0	4
數位學習資源中心	0	0	5	0	0	5	0	0	1	0	0	11
總計	6	16	14	6	10	14	16	1	7	1	3	94
百分比	6%	17%	15%	6%	11%	15%	17%	1%	8%	1%	3%	100%

- 可接受風險值說明
  - 本校於 107 年導入「個人資料保護管理制度」，考量本校個資資產特色、業務屬性及人力配置等因素，依據 80/20 分配法則，將資源投入在高度風險的資產。
  - 依據計算本次資產項目共 94 個，最大風險值為「21」，依據 80/20 法則，計算出可接受風險值為「16.8」。超過 16.8 即界定為「高度風險」；對於風險值 16.8(含)以下的項目，視為「可接受之風險」，將依所訂定程序控管。
  - 依建議之可接受風險值 16.8，高於可接受風險值，鑑別出註冊課務組 1 項、學生諮商組 4 項、圖資服務組 2 項、系統設計組 3 項及數位學習資源中心 1 項，共 11 項，需規劃風險處理計畫，降低或接受風險值。
- 可接受風險值是否同意，呈請長官核示。
- 經會議討論可接受風險值為「16.8」，後續將通知各單位進行風險改善計畫。

七、持續改善之機會

- 辦理個資管理制度教育訓練：本校於 107 年度導入「個人資料保護管理制度」，新設置管理制度文件，需增加單位負責窗口了解本校個人資料保護管理制度運作，以符合本校個人資料管理規範。
- 擴大個人資料管理制度導入範圍：為保障校內個人資料受適當管

控，除現行已導入範圍外，考量108年個資管理制度經費減少，新增受驗證單位以4個為上限，提請委員討論。

- 辦理全體教育訓練：每年度進行全體教育訓練，宣導個人資料保護概念，以降底個資外洩的風險，提升同仁對於個資管理及法令之要求。

參、提案討論

案由一：本校個人資料保護管理目標之評量方式，提請討論。

說明：

一、今年度導入個人資料管理制度所設置目標，需規畫評量方式，以確認管理制度落實及運作。

二、擬定「國立宜蘭大學個人資料管理制度有效性量測表」請參考附件一(P.3~4頁)。

擬辦：經會議通過後，依相關規定辦理受驗証單位量測。

決議：修訂通過，將於12月4日至受驗證單位進行量測。

案由二：可接受風險值設定，提請討論。

說明：

一、本校於107年導入「個人資料保護管理制度」，因本校學生資料多，部分單位(如學生諮商組)有特種個資，且管理人力有限；其中資料量多(衝擊影響大)及特種個資(資產價值高)皆屬於高度風險，故擬將資源投入在高度風險的個資資產管理中，並依據80/20分配法則設定可接受風險值。

二、經計算本年度個資資產項目共94個(附件二，P.5)，最大風險值為「21」，依據80/20分配法則，可接受風險值為「16.8」。擬將風險值超過16.8界定為「高度風險」；對於風險值16.8(含)以下的項目，視為「可接受之風險」，並依訂定程序進行控管作業。

擬辦：

一、風險值設定擬依據80/20分配法則。

二、今年度可接受風險值為「16.8」，高於可接受風險值單位包括：註冊課務組1項、學生諮商組4項、圖資服務組2項、系統設計組3項及數位學習資源中心1項，共5個單位，11項個資資產，後續將請各單位進行風險改善計畫。

決議：

一、決議通過。

二、決議通過，超於風險值「16.8」的11項個資資產，請各單位規劃並進行風險改善計畫。

案由三：108年度導入個資管理制度之單位建議如下，提請討論。

說明：

一、為保障校內個人資料受適當管控，除107年度已接受驗證之6個單位外，擬擴大個人資料管理制度導入範圍，以保障個人資料安全。

二、因應明年度個資管理制度經費減少，新增受驗證單位以4個為上限，擬請委員推薦適合單位。

三、建議新增單位及推薦理由請參考附件三(P.6)。

擬辦：經通過後，受推薦單位及107年度受驗證單位均應參與108年個資管理制度導入計畫，並指派一名成員擔任負責窗口。

決議：

一、108年度個資管理制度新導入單位：秘書室校友服務中心、教務處綜合業務組、教務處進修推廣組、人事室。

二、下年度舉辦個資管理制度教育訓練，除導入個資管理制度單位及各單位個資保護聯絡窗口參加外，也需開放校內同仁參與。

肆、臨時動議

伍、散會