國立宜蘭大學 108 學年度

個人資料保護推動委員會第一次會議暨第一次管理審查會議議程

日期：民國 108 年 12 月 25 日(星期三)上午 10 點

地點：行政大樓五樓第一會議室

主席：陳副校長凱俐　　紀錄：游佳欣

出席：吳中峻委員、王進發委員、吳寂絹委員(邱鳳仙秘書代理)、游竹委員、張介仁委員、江茂欽委員(楊屹沛組長代理)、林連雄委員、江美芳委員、邱聰祥委員、江漢全委員、陳威戎委員、林豐政委員(裘家寧執行秘書代理)、鐘鴻銘委員、黃于飛委員、鄭麗寬委員

列席：朱達勇主任、游佳欣、蔡岱樺

請假：游依琳委員(請假)、陶金旺委員(請假)、楊秋萍委員(請假)、劉文琴委員(請假)

壹、 主席致詞

貳、 業務報告(簡報)

一、 過往管理審查之議案的處理狀態

序號	上次會議提案及決議	執行情形
1	案由一：本校個人資料保護管理目標之評量方式，提請討論。 決議：修正通過。	於 12 月 4 日至受驗證單位進行量測，量測結果都符合。
2	案由二：可接受風險值設定，提請討論。決議：照案通過。	依規定，請各單位進行風險改善計畫。
3	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。 決議：照案通過。	於 108 年安排新導入單位，由顧問進行個資盤點等相關事宜。並於 108 年 10、11 月辦理 2 場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外，也開放校內同仁參與。

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。	1. 去年度申請106年版驗證，預計於 110 年申請新版驗證 2. 預訂於明年2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，於 107 年開始導入個人資料管理制度。	

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。				
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
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。				

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
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。				
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
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。				
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
2	風險評鑑	檢查個人資料風險評鑑，鑑別可承受風險等級。	檢核每單位風評估表及風險處理計畫。	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，將於稽核驗證前至受驗證單位進行量測。

四、 內外部稽核結果

於 12 月 13、14 日(星期四、五)進行個人資料管理制度外部稽核，稽核結果統計：

主要缺失：0 項

次要缺失：2 項

觀察事項：10 項

五、 個資事故與不符合項目之矯正情形

(一)個資事故：

於 108 年 10 月 2 日接獲個資事故通報，通報處理結果於提案二說明。

(二)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	個人資料盤點作業應再加強，包括：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) ■ 人員保密切結書(數位學習資源中心) ■ 教室借用管理、個資數量、保存期限、銷毀時限、保有依據。(教務處註冊課務組) ■ Log 紀錄、CCTV、機房進出紀錄、工讀生申請資料保存期限。(圖書資訊館資訊網路組) ■ 工讀生保密切結、CCTV(圖資服務組、學生諮商組)	1. 尚未熟悉盤點方式之狀況，將辦理相關教育訓練及宣導作業。 2. 請同仁重新檢視業務職掌，確認單位業務作業流程中相關之個人資料流向，並更新各單位之個資清冊。 3. 於內部稽核時加強查核前述項目是否符合。
2	B.10.1.1	資訊系統之安全管控措施應依循程序要求予以落實，包含：諮商 e 化系統、悠遊學生卡製卡主機(資源回收桶、防毒軟體、F 槽)、註冊課務組個人電腦螢幕保護設定、雲端即時反饋系統 Web API 管控、校務資料庫(備份)主機密碼更換、資訊網路組 office365 系統帳號審查等。	1. 請同仁重新檢視業務職掌，依各單位之項目進行處理，例：系統完成帳號清查並留下記錄，業務使用之電腦應完成螢幕保護程式設定，系統定期更換密碼並留下記錄…等。 2. 於教育訓練時宣導相關資訊，並請各單位派員參與「個人資料保護宣導及教育訓練」，未參加者應利用存放於數位園區的影音課程與測驗自我學習。 3. 將「ISMS 管控程序」及相關注意事項製作為說明文件與檢核清單，供同仁使用。 4. 於內部稽核時加強查核上述措施。

六、 風險評鑑結果及風險處理計畫執行進度

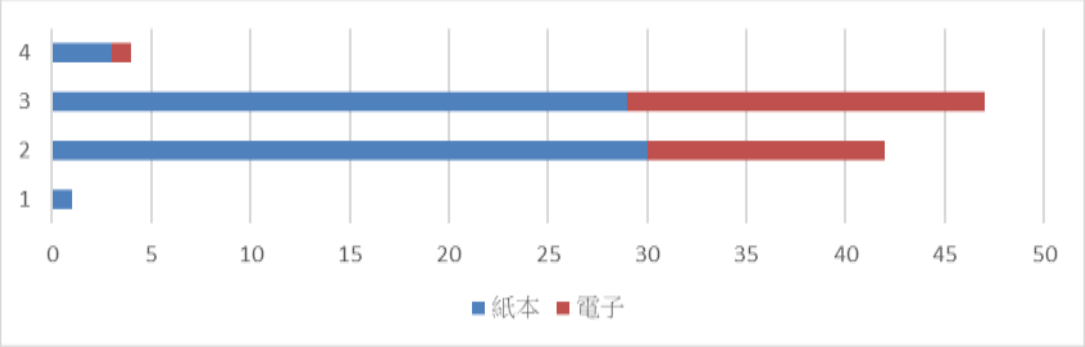
(一)今年度風險評鑑結果

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。

1. 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：

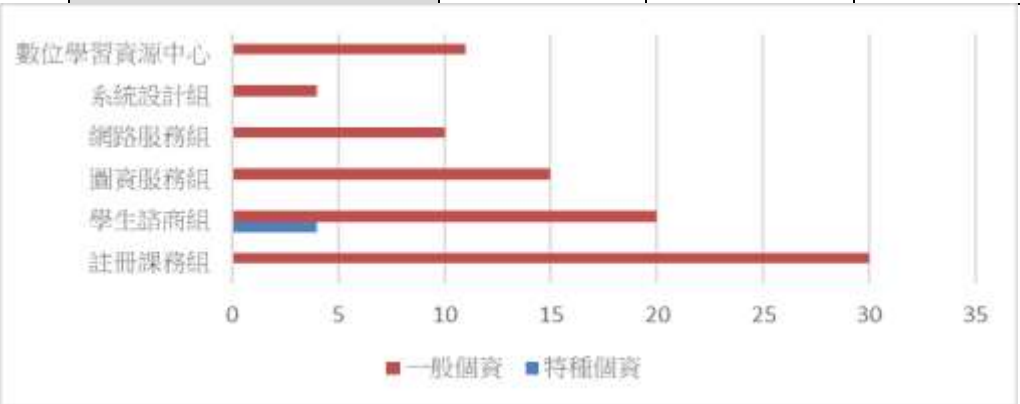
類型/個資範圍評估值	1	2	3	4	總計
紙本	1	30	29	3	63
電子	0	12	18	1	31
總計	1	42	47	4	94



2. 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：

	特種個資	一般個資	總計
註冊課務組	0	30	30
學生諮商組	4	20	24
圖資服務組	0	15	15
資訊網路組	0	9	9
系統設計組	0	4	4
數位學習資源中心	0	12	12
總計	4	90	94



3. 個資資產風險分布

依據各單位個資資產之風險值由低至高分布情況如下：

單位/風險值	2	4	6	8	9	10	12	15	18	總計
註冊課務組		8	10	1	4		6	1		30
學生諮商組		3	8	4	5		3	1		24
圖資服務組							14	1		15

資訊網路組	1	3	4		1					9
系統設計組								1	3	4
數位學習資源中心			3	3	1	1	4			12
總計	1	14	25	8	11	1	27	4	3	94
百分比	1%	15%	27%	9%	12%	1%	29%	4%	3%	

4.可接受風險值說明

- 本校於107年開始導入「個人資料保護管理制度」，考量本校個人資料資產特色、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個資資產，當時依據80/20法則計算出可接受風險值為「16.8」。
- 經107年個資驗證稽核委員建議，此方式雖可表現本校積極配合改善個資資產風險值，但也會造成未來需改善風險個資資產項目增加，以致無法全面落實改善，需列為可接受風險的個資資產項目增多。
- 依據計算本次資產項目共94個，最大風險值為「18」，且經導入後資產風險值明顯下降，排建議與去年計算設定相同可接受風險值設定為「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，鑑別出系統設計組3項，共3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後，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。
- 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：本校受驗證單位的個資資產項目可接受風險值設定，提請討論。

說明：

一、個資驗證稽核委員建議本校原定可接受風險值設定以「80/20」法則設定，雖可表現本校積極配合改善個資資產風險值，但也會造成未來需改善風險個資資產項目增加，以至無法全面落實改善，需列為可接受風險。

二、經計算本年度個資資產項目共有94個，與去年相同風險值多落在18-15區間，及去年計算設定可接受風險值「16.8」，故建議可接受風險值設定在「16.8」。

擬辦：

一、 可接受風險值設定為「16.8」。

二、 今年度可接受風險值為「16.8」，高於可接受風險值單位後續進行風險改善計畫。

決議：

一、 可接受風險值設定為「16」。

二、 今年度可接受風險值為「16」，高於可接受風險值單位後續進行風險改善計畫。

案由二：複核1081002個資事故是否處理得當，提請討論。

說明：

一、108 年 10 月 2 日校窗口接獲通報，本校協辦 PVQC 承辦助理因故疏忽，將全部考生資料已 E-MAIL 方式寄給全部考生，造成個資外洩事故。

二、於當日通報所屬單位及負責老師，了解發生情況及討論處理方式，由承辦老師寄送 EMAIL 方式，道歉及說明原因，並透過課堂及測驗期間，說明事情發生原因，並請學生將信件刪除。

三、於 10 月 16 日加開個資事故應變小組會議，並邀請負責老師與會說明，會議決議，此案處理得當，並請負責老師上簽自請處份以示負責。

四、後續宣導作業：於導師會議時，宣導此類事件處理方式，並於 11 月辦理相關研習向老師及學生宣導個資處理需注意事項。

擬辦：

一、請會議討論並判定本案分級方式與應變是否得當。

二、擬將申訴案件暫時歸檔，110 年 10 月 3 日，民事告訴期限已過再正式歸檔。

決議：

一、 決議通過，本案處理方式得當。

二、 本案件暫時歸檔，待 110 年 10 月 3 日，民事告訴期限已過再正式歸檔。

肆、 臨時動議

伍、 散會