臺北市立大學 113 學年度第一學期

「資訊安全暨個人資料保護推動執行委員會」會議紀錄

時　間：113 年 10 月 18 日(星期五)上午 11 時 00 分

地　點：本校博愛校區行政大樓 T201 會議室

主　席：曾國維副校長

出 席 者:如簽到表

壹、主席報告：

貳、報告事項：

一、宣讀上次會議決議：

案由一：配合加速與深化全校導入資訊安全管理制度（ISMS），請各單位定期更新「資訊安全暨個人資料保護窗口」，提請討論。

決　議：照案通過。

案由二：為有效進行網頁管理，請各單位定期更新「網頁管理窗口」，提請討論。

決　議：照案通過。

案由三：為維護全校網路安全，擬重新盤點本校各單位分配之 IP 位址，提請討論。

決　議：照案通過。

案由四：本校物聯網（IoT）設備管理，提請討論。

決　議：照案通過。請各單位配合進行列管設備填報及密碼管理。

案由五：有關本校落實推動辦理「校內電腦使用者每人每年需接受三小時以上之一般資通安全教育訓練」作法，提請討論，提請討論。

決　議：照案通過。

案由六：本年度辦理個人資料管理規範驗證（PIMS）追查稽核作法，提請討論。

決　議：照案通過。

二、工作報告：

(一)通過認證

1. 本校於 111 年 10 月 24 日通過教育體系資通安全暨個人資料管理規範(PIMS)驗證審查，效期為 3 年，並於 112 年 11 月 16 日完成第一次追查稽核。
2. 本校於 113 年 9 月 30 日進行 ISO 27001:2022 外部稽核(受驗範圍為本校計中)，目前進行補件說明，依稽核結果預計可取得核可證書。

(二)稽核及演練

1. 個人資料保護內部稽核(PIMS)
   (1) 準備 113 年度教育體系資通安全暨個人資料管理規範追查稽核相關事宜。
   (2) 本校於 113 年 8 月 30 日完成本年度個人資料保護內部稽核。
   (3) 外部稽核日期預計為 113 年 11 月 7 日。
2. 資安管理系統及擴大導入稽核(ISMS)
   (1) 本中心及機房業於 113 年 9 月 19 日及 9 月 30 日分別完成內外部稽核。
   (2) 本年度 ISMS 擴大導入自 113 年 8 月起輔導學務處、總務處、國際事務處、進修推廣處及圖書館等單位。擴大導入單位內部稽核預計於 113 年 11 月 18 日及 19 日辦理。

(三)重申依資通安全管理法子法-資通安全責任等級分級辦法規定：「校內電腦使用者每人每年需接受三小時以上之一般資通安全教育訓練。」，已於年初商請人事室通知全校各單位同仁抽空參訊，並協助通知及下載上課人員名單。請再次轉達各單位未上課同仁盡速利用台北 E 大接受免費教育訓練。

(四)依據「臺北市政府各機關網站服務管理作業原則」規定，本校網站內容倘涉及機密性、敏感性及個人隱私資料與文件不宜公布，建議除取得當事人同意外，應將姓名等個人資訊進行遮罩後再行公布。

參、討論事項：

提案一：有關落實本校同仁禁止遠端桌面連線軟體一案，提請討論。

提案單位：計算機與網路中心

說　　明：

（一）依「臺北市政府資通訊業務委外作業指引」第 7 條第 1 項規範，行政單位嚴禁採用遠端連線軟體連入校內網路，本校業於 112 年度建置 VPN 系統供外部廠商遠端連入本校維護伺服器。

（二）考量遠端連線軟體可能因版本為更新等原因成為資安漏洞，本中心擬禁止全校教職員生直接進行遠端連線。

（三）倘真有相關需求者，請改採 VPN 方式處理，相關帳號請向本中心申請。

決　　議：照案通過。

提案二：有關本中心盤點全校 IP 使用，並回收不當使用 IP 一案，提請討論。

提案單位：計算機與網路中心

說　　明：

（一）因本校網路使用者眾多且用途多樣，致本校多數資安事件係因使用者自行安裝網路設備問題所致。

（二）現行因應作法

1. 倘本中心觀察或獲知資安通報發現某 IP 出現異常使用情形，為防止資安漏洞產生，擬將該 IP 對外網路中斷，並連繫該 IP 使用者使用情形，俟障礙排除後再重新開通連線。
2. 為避免本校網路流量遭不當利用，影響其餘師生網路使用權益，本校於本(113)年度採購 GSI 網路流量管理系統，觀察校內各 IP 使用情形。

（三）配合教育部資安強化專章後續規範 ，並為確認各 IP 現行使用設備及位置，擬重新盤點與清查全校 IP 使用情況，並回收不當使用 IP，以利於降低潛藏風險及發生資安事件後續排除作業。

決　　議：照案通過。

提案三：有關「非大陸廠牌資通訊產品品牌白名單」，提請討論。

提案單位：計算機與網路中心

說　　明：

（一）依臺北市政府教育局 109 年 12 月 30 日北市教資字第 1093118386 號函，為避免公務及機敏資料遭不當竊取，

全校各單位不得採購及使用大陸廠牌資通訊產品(含軟體、硬體及外包服務使用之設備)，如附件 1。

（二）為將非大陸廠牌資通訊產品品牌明確化，避免全校各單位採購及使用大陸廠牌資通訊產品，本中心參考共契及本校近三年採購品牌，針對非大陸廠牌資通訊產品品牌提供白名單，如附件 2 。

（三）後續採購如列於白名單者，將不再進行審核，惟未屬表列者，將請請購單位提供相關佐證。

（四）白名單預計配合共契資訊和本校採購，於每年提供更新版本，並置於計中網頁，供本校同仁有相關採購需求時參考。

決　　議：照案通過。

提案四：有關 113 年度個人資料保護驗證機制(PIMS)內部稽核各單位風險評鑑報告，提請討論。

提案單位：計算機與網路中心

說　　明：

（一）113 年度各受稽核單位風險評件報告如下附表，計盤點 164 項，其中列入高風險 0 項、中風險 20 項、低風險 144 項。

（二）依據個人資料風險評鑑與處理管理程序第 6.3.4(如圖 1)個資風險等級判定，風險等級 3 須列入不可接收風險，須立即控制改善。

（三）113 年度個人資料管理內部稽核報告如附件 3，已分別製作矯正預防單請各單位改善後結案。

6.3.4. 個資風險等級判定

6.3.4.1. 決定可接受風險值

6.3.4.1.1. 以下列出可接受及不可接受之風險等級，作為本校位後續風險處理之依據。

風險值(R)	風險等級	風險判別與處理	
6—10	1	可接受風險	接受
11—24	2	可接受風險	持續監視
26—54	3	不可接受風險	立即控制

圖 1：個人資料風險評鑑與處理管理程序

表 1：113 年度個人資料保護驗證單位風險評鑑統計表

臺北市立大學

113年度個人資料保護驗證單位風險評鑑統計表

統計日期：113年10月7日

單位名稱	風險等級(低)	風險等級(中)	風險等級(高)	合計
教務處	30	6	0	36
學生事務處	20	11	0	31
人事室	58	2	0	60
計算機與網路中心	36	1	0	37
合計	144	20	0	164

擬　　辦：

(一) 本年度無高風險等級個資盤點項目，擬接受各單位訂定之風險評鑑等級。

(二) 擬將上開盤點結構提供 PIMS 外部稽核做為稽核佐證。

決　　議：照案通過。

提案五：鼓勵本校同仁參加 PIMS 個資相關教育訓練一案，提請討論。

提案單位：計算機與網路中心

說　　明：

（一）截至 113 年度，本校導入 PIMS 單位共 8 個。

（二）為強化各單位個資相關知識，並為導入 ISMS 及 PIMS 預做準備，本中心於 113 年 10 月 22 日開設線上教育訓練，授課對象涵蓋全校各單位。

（三）課程網址後續將採便箋及電子郵件提供，並於課後提供線上表單進行簽到作業。

（四）本訓練課程不強制各單位派員參與，但完成教育訓練者，可視為完成年度三小時資安訓練。

決　　議：照案通過。

肆、臨時動議：無

伍、散　　會：上午 11 時 00 分