國立臺灣師範大學
資訊安全及個資保護內部稽核報告

中華民國 106 年 6 月 6 日

一、 稽核目的：

藉由實地訪查，瞭解學校資訊安全及個人資料管理系統(PIMS)制度是否確實執行。

二、 稽核範圍：本校各單位。

三、 稽核執行期間：2017/5/15~2017/5/19

日　期		上午	下午
5 月 15 日	星期一	圖書館、國際與社會科學學院	秘書室、研發處、主計室
5 月 16 日	星期二	師培處、總務處	理學院、運休學院、環安衛中心
5 月 17 日	星期三	學務處、教務處	文學院、進修推廣學院
5 月 18 日	星期四	教育學院、藝術學院、科技學院	國際事務處、體育室、資訊中心
5 月 19 日	星期五	人事室、音樂學院、管理學院	僑先部、林口校區

四、 稽核執行人員：資訊中心[柯文傑、林峰立、張祖鼎、吳宗曄、林柏宏、李樹昌、陳昱甫]、外部稽核單位 NII[許嘉雯、黃金月、王彥鈞、張云蘋]。

五、 稽核方式: 依照「資訊安全及個資保護內部稽核查檢表」項目，以面談、觀察、抽樣檢查等方式進行。

六、 「資訊安全及個資保護內部稽核查檢表」內容:

一、個人管控措施	
1	禁止使用違反智慧財產權相關的軟體、資訊或文件。
2	應避免將通行密碼記錄在書面上，或張貼於個人電腦、螢幕或其它容易洩漏秘密之場所。
3	為防止未經授權之存取，人員離開前，應將敏感等級之文件(如包含身分證字號)與可攜式資訊設備存放於可上鎖之儲櫃，避免資訊外洩。
4	使用影印機、印表機、傳真機、掃描機或多功能事務機後，應立即將資料取走。
5	敏感等級（含）以上紙本文件不再使用時，應以碎紙方式銷毀。
二、個人電腦管控措施	
1	電子郵件應關閉自動下載圖片或影像功能，不隨意開啟不明信件，以避免惡意程式之攻擊。
2	電腦應設定螢幕保護程式並設密碼保護。(建議設定值為十分鐘)
3	個人電腦不得安裝 P2P 分享軟體下載未經授權之軟體。(包含非法音樂、電腦等)
4	個人電腦須安裝防毒軟體，並定期更新病毒碼，以防止病毒攻擊及擴散。
5	防毒軟體系統應設定主動掃描檢查，且定期執行掃描檢查作業。
6	電腦應定時修補作業系統及應用程式漏洞。(windows 及 office update 須設定自動更新，Adobe Reader、flash 須進行更新)
7	通行密碼的長度最少應有六碼，且應符合密碼設置原則（至少英文、數字混合），並定期更新密碼。
8	個人電腦須設定防火牆，並關閉不使用之服務。遠端桌面若不使用請關閉，需要使用時再開啟。
9	個人電腦內機密文件檔案，應以加密方式保存。若欲使用電子郵件傳輸個人機敏資料前，請先加密處理。
10	電腦設備不可任意架站或做私人、營利用途。
三、單位管控措施	

1	單位應指派專人負責資安及個資業務，並參加相關教育訓練。
2	使用軟體與資訊產品應遵守該軟體或產品之規定，例如限制於指定之機器使用、限制僅於備份時方可複製等。
3	丟棄單位資訊電子媒介前，應刪除電子媒介資訊，並徹底消磁或銷毀至無法解讀之程度。
4	單位人員須隨時注意身分不明或可疑的人員，發現不明身分人員時，應主動詢問並儘速通知權責單位處理。
5	重要儲存媒體，應上鎖或由專人管理，並且僅經授權之使用者方能使用。
6	未經授權不得將設備、軟體、儲存資訊之媒體或機敏文件攜出電腦機房及辦公環境。若有需要，須經主管人員核准，始得進行。
7	公用電腦需有專人負責管理，避免因無人管理造成資安漏洞。
8	敏感等級之文件(如包含身分證字號)應存放於可上鎖之櫥櫃，並規劃只允許授權之同仁有權限可開啟。
9	單位直接蒐集個人資料應取得當事人書面、電話、傳真或電子方式同意(法令授權免通知者除外)，並明確說明蒐集個人資料的學校名稱、目的、個資類別、期間、地區、對象、處理方式/當事人行使權利及方式/不提供之影響。
10	單位內應針對個人資料顯示(包含紙本及電子檔)進行適當的去識別化(最小化、隱碼)。
11	與其他單位(包含校內、外)交換個人資料時，應採取適當保護措施，並符合蒐集時之目的。
12	單位應針對受委託處理個資之廠商，於契約上訂有個資保護法令及學校內部個資相關規定要求，並有明確的監督要求。
四、單位網站管控措施	
1	敏感等級以上之業務資料或文件不得存放於對外開放之資訊系統中，若因特殊業務功能之需求，必須採取安全管控機制。
2	伺服器不使用時，應採用密碼保護、鎖定或登出離線等安全控制措施。
3	伺服主機應指定負責人，負責該主機之正常運作，包括應用程式之執行、資料庫之維護及相關作業系統與主機硬體資源之分配管理等。
4	網站資料及資料庫資料應定期進行備份作業。
5	公告之資訊，應經由權責主管之審查與核定，確認未含有敏感等級以上資訊、違反資訊安全管理相關資訊，以及違反智慧財產權或法令所明訂之禁止資訊。
6	非因業務需求不得將系統存取帳號提供給外部人員，若因業務需要開放帳號予外部人員，應有適當安全控管措施，該安全控管措施應考量業務需求及資訊資產之機密性，授與適當之存取權限及有效日期。
7	人員離職時，應移除其作業管理權限。
8	伺服器管理者應設有代理人，系統管理者通行碼設置至少 7 碼，且應符合通行碼設置原則。並定期更新密碼。
9	伺服器應設定防火牆，並關閉不使用之服務。若只限校內人員使用，建議限制只允許師大 IP 可讀取，校外可透過 VPN 登入使用。
10	windows 伺服器應定期進行 windows update 及安裝防毒軟體。
11	系統修改或開發時，測試資料應避免使用真實資料，避免個人資料外洩。

七、 稽核結果彙總：

【行政單位】

受稽單位	不符合項目數		受稽單位	不符合項目數	
	106 年	105 年		106 年	105 年
秘書室	0	0	資訊中心	0	0
教務處	0	1	體育室	0	3
學務處	1	2	人事室	0	0
總務處	0	0	主計室	0	0
研發處	1	1	環安衛中心	0	0
師培處	1	0	進修推廣學院	0	2
國際事務處	0	2	僑生先修部	3	3
圖書館	0	2	林口聯辦	0	1
			總計	6	17

【學術單位】

受稽單位	不符合項目數		備註
	106 年	105 年	
教育學院	0	5	抽查 2 個系所:健康促進與衛生教育學系、公民教育與活動領導學系。
文學院	1	2	抽查 1 個系所:地理學系。
理學院	0	1	抽查 2 個系所:化學系、生科系。
藝術學院	0	3	抽查 1 個系所:藝術史研究所。
科技與工程學院	0	0	抽查 1 個系所:機電工程學系。
運動與休閒學院	0	1	抽查 1 個系所:運動休閒與餐旅館理研究所。
國際與社會科學學院	0	0	抽查 2 個系所:應用華語文學系、大眾傳播研究所。
音樂學院	0	0	抽查 1 個系所:表演藝術研究所。
管理學院	1	0	抽查 1 個系所:全球經營與策略研究所。
總計	2	12	

八、 各單位內部稽核不符合事項說明(查核發現內容為稽核員現場檢測發現之問題，與當場提供之報告內容相符)：

- 學務處

項次	不符合查檢項目	查核發現
1	電腦應定時修補作業系統及應用程式漏洞。(windows 及 office update 須設定自動更新，Adobe Reader、flash 須進行更新)	發現一台公用電腦 windows update 異常，無法定期更新。

- 研發處

項次	不符合查檢項目	查核發現
1	電腦應定時修補作業系統及應用程式漏洞。(windows 及 office update 須設定自動更新，Adobe Reader、flash 須進行更新)	經查一台電腦未進行更新。

- 師培處

項次	不符合查檢項目	查核發現
1	電腦應定時修補作業系統及應用程式漏洞。(windows 及 office update 須設定自動更新，Adobe Reader、flash 須進行更新)	發現一台電腦 windows update 異常，無法定期更新。

- 僑生先修部

項次	不符合查檢項目	查核發現
1	為防止未經授權之存取，人員離開前，應將敏感等級之文件(如包含身分證字號)與可攜式資訊設備存放於可上鎖之儲櫃，避免資訊外洩。	辦公區公共區域放置個人資料，如健保卡資料及通訊錄。
2	使用影印機、印表機、傳真機、掃描機或多功能事務機後，應立即將資料取走。	二樓茶水間公用印表機無專人管控，發現列印失敗個資文件未銷毀。
3	敏感等級（含）以上紙本文件不再使用時，應以碎紙方式銷毀。	回收紙箱發現個人資料文件未銷毀。

- 文學院

項次	不符合查檢項目	查核發現
1	地理學系： 電腦應定時修補作業系統及應用程式漏洞。(windows 及 office update 須設定自動更新，Adobe Reader、flash 須進行更新)	檢查發現 2 台電腦並未定時修補漏洞。

- 管理學院

項次	不符合查檢項目	查核發現
1	全球經營與策略研究所： 為防止未經授權之存取，人員離開前，應將敏感等級之文件(如包含身分證字號)與可攜式資訊設備存放於可上鎖之儲櫃，避免資訊外洩。	重要個資文件並未放置於可上鎖之櫥櫃。

九、 各單位內部稽核不符合項目類型彙總：

類型項次	查檢項目說明	查檢不符次數
1	電腦應定時修補作業系統及應用程式漏洞。(windows 及 office update 須設定自動更新，Adobe Reader、flash 須進行更新)。	4
2	為防止未經授權之存取，人員離開前，應將敏感等級之文件(如包含身分證字號)與可攜式資訊設備存放於可上鎖之儲櫃，避免資訊外洩。	2
3	使用影印機、印表機、傳真機、掃描機或多功能事務機後，應立即將資料取走。	1
4	敏感等級（含）以上紙本文件不再使用時，應以碎紙方式銷毀。	1
		總計 8

十、 其他稽核發現：

- Office Scan 10 無法針對勒索病毒進行阻擋，建議更新 11 版或安裝卡巴。
- 小紅傘免費版只能用在個人端，學校非免費版授權使用對象，請安裝學校提供防毒軟體。
- 部分單位還在使用 winXP 系統，微軟已不更新 winXP 系統漏洞，建議進行升級。
- 少數同仁 windows update 預設為凌晨 3 時更新，建議修改為中午 12 時。
- 發現單位有不使用舊個資文件，建議清查舊個資紙本文件，若不需要，可考慮銷毀。
- 部分單位尚有舊職員通訊錄，本校教職員通訊錄為密件，若不使用，請送人事室或自行銷毀。
- 發現某單位電腦教室系統環境超過 1 年未更新，電腦教室電腦雖然有還原卡，但還是會中毒造成內部感染，建議定期進行 windows update。
- 發現重新安裝電腦未完成 windows update 即上線使用，建議必須完成 windows update 後再上線使用。
- 發現某系辦門口公共區域張貼學生照片、姓名及學號，非系上師生也可以看到。恐有違反個資規定，建議於蒐集學生資料前告知及保留同意紀錄，或將學生資料放置在系辦內部。

十一、稽核總結：

雖存在不符合事項，但仍達一定管理水準，建議應儘速完成不符合事項之矯正，以加強安全防護。

十二、各單位須針對不符合項目填寫「矯正與預防處理單」，述明不符合原因及改善措施後，將另指派稽核人員至各單位複查確認完成矯正。