臺北市立大學112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」會議記錄

時　間：112年 10月 25日(星期三)上午 11時 17分

地　點：本校博愛校區行政大樓201會議室

主　席：張曉生副校長

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：擬推動辦理「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」，請轉達所有同仁務必參加資通安全教育訓練。

決　議：照案通過。

案由二：112 年度辦理個人資料管理規範驗證(PIMS)追查稽核作法乙案。

決　議：照案通過。

二、工作報告：

(一)　通過認證

本校於111 年9 月29 日通過資訊安全管理制度(ISMS)驗證審查，效期為3 年，並於112 年9 月4 日完成本年度複評驗證。

(二)　稽核及演練

1. 個人資料保護內部稽核(PIMS)

(1)　準備 112 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112 年9 月25 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112年11月16日(星期四)。

2. 內部資通安全稽核(ISMS)

(1)　依「資通安全責任等級 C 級之公務機關應辦事項修正規定」，內部資通安全稽核應每二年辦理一次。前次全校資訊安全稽核於110 年11 月4 日

(星期四)辦理完成，針對全校行政及教學單位抽查承辦人員是否符合資訊安全規定，並於稽核後協助使用者更新完成。

(2) 112 年度配合辦理「資訊安全管理制度(ISMS)擴大導入輔助專案」，擬於 112 年 11 月針對輔導單位進行資訊安全內部稽核。

3. 惡意電子郵件社交工程演練

(1) 轉知教育部 112 年 3 月 24 日函(附件 1)，針對受測人員寄送 5 封社交工程演練郵件。111 年第 2 次防範惡意電子郵件社交工程演練結果(附件 2) 。

(2) 本校代碼為 B86，受測人數 49 人

(3) 演練信件開啟人數 0 人，演練信件開啟率 0%:合格。

(4) 演練信件點閱(連結、附件)人數 0 人，比率 0%:合格。

(三) 填報作業

依 112 年 5 月 24 日臺北市政府教育局函，填報行政院國家資通安全會報資通安全作業管考系統，於 5 月 26 日完成。

(四) 宣導事項

1. 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，煩請再次轉達各單位同仁利用台北 E 大接受免費教育訓練，課程建議如下：

(1) 個資侵害事故之民刑事訴訟實務

(2) 個資資安事故之緊急應變

(3) 個資資安事故之調查與因應

(4) 個資內部稽核方法與實務

(5) 個資外部稽核方法與實務

(6) 資安意識及基本技能培訓課程：資安政策法規遵循教育訓練

(7) 資安意識及基本技能培訓課程-資安事件處理與應變

(8) 資安事件應變管理&建立資安威脅風險意識

(9) 資通安全新創觀點&最新資安威脅報告解析

(10) 資安意識及基本技能培訓課程-資通安全系統防護

基準稽核與履約管理

2. 臺北市政府112年8月11日府授資安字第1123008279號公告「臺北市政府所屬人員資通安全事項獎懲基準」(附件3、附件4)。依據規定，業務單位業務上因資安意識不足造成資通安全事件發生，獎懲基準羅列如下：

(1) 主動發現新型態之資通安全弱點或入侵威脅，並進行資通安全情資分享，防止資通安全事件之發生或降低其損害，予以記功。

(2) 違反本法及其授權訂定之法規或本府規範，致生一級或二級資通安全事件，予以申誡。

(3) 違反本法及其授權訂定之法規或本府規範，致生三級以上資通安全事件，予以記過。

(4) 聘用人員、約僱人員或其他與本府所屬機關具有僱傭關係者，其獎勵及懲處情形應納入續聘之參考。

3. 教育局112年6月13日來函通知本校未符合市府遠端連線規範，本校立即停止全校委外廠商遠端連線，並建置「VPN+一人一帳號+雙因子認證，且僅能連線至受託單位管理主機」連線機制，以利符合「臺北市政府資通訊業務委外作業指引」之要求，並於6月20日公告調查各單位連線需求後報請市府審查，7月24日教育局同意備查後，於7月31日起重新開放各單位遠端連線服務。爾後如有申請需求，請至計網中心網站下載與申請。

參、討論事項：

提　案　一：有關 112 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）112 年度各受稽核單位風險評件報告如下附表，計盤點 229 項，其中列入高風險 0 項、中風險 42 項、低風險 187 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。

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 1：112 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 112年度個人資料保護驗證單位風險評鑑統計表				
				統計日期: 112年9月26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	59	8	0	67
學生事務處	47	14	0	61
人事室	63	2	0	65
計算機與網路中心	18	18	0	36
合計	187	42	0	229

（三）擬辦：

1. 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。

2. 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，同意將上開盤點結構提供 PIMS 外部稽核做為稽核佐證。

提 案 二：為提升本校同仁參與資訊安全或個人資料保護相關訓練受訓人數比例，擬公告線上影片課程，並設計測驗題目做為受訓之依據，提請討論。

提案單位：計算機與網路中心

說　　明：

(一)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。」

(二)另依本校個人資料教育訓練管理程序，本校一般同仁，每年應至少參加 3 小時以上（含）之資訊安全或個人資料保護相關訓練。

(三)為落實上開要求，本校於 111 學年度第二學期「資訊安全暨個人資料保護推動執行委員會」決議，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」。

(四)人事室已於 112 年 3 月 3 日發送全校通知「公務人員需研習業務相關學習時數 20 小時」，台北 E 大提供相關免費教育訓練課程，提供 10 門資通安全教育訓練建議清單。然而此課程僅能提供職員受訓（不包含一二級主管或約用人員、助理人員等）。為有效提升受訓人數與成效，擬以線上影片課程公告周知，並設計相關具鑑別度之測驗題目做為受訓之依據。

決　　議：照案通過。

提 案 三：有關深化全校導入資訊安全管理制度(ISMS)，請各單位指派「資訊安全暨個人資料保護窗口」，提請討論。

提案單位：計算機與網路中心

說　　明：

(一)依「112 年高教深耕計畫資安專章共通性審查意見」建議：「(四)大部分學校資安工作推動或執行小組僅由資

訊中心成員擔任，建議應「跨單位」組成如盤點、稽核及教育訓練等。」

(二)本中心 112 年度配合辦理「資訊安全管理制度(ISMS)擴大導入輔助專案」，112 年度針對教務處、人事室先行導入。

(三)依本次導入經驗，本中心擬進行公告調查，請各單位預先指派「資訊安全暨個人資料保護窗口」，以利陸續強化全校各單位之資訊安全與個人資料保護相關業務。

決　　議：照案通過。

肆、臨時動議:無。

伍、散　　會： 11 時 30 分

附件1

檔　　號:
保存年限:

教育部 函

地址：100217 臺北市中正區中山南路5號
承辦人：宋伯謙
電話：(02)7712-9078
電子信箱：a230222@mail.moe.gov.tw

受文者：臺北市立大學

發文日期：中華民國112年3月24日
發文字號：臺教資(四)字第1122701002號
速別：普通件
密等及解密條件或保密期限：
附件：附件1-111年第2次防範惡意電子郵件社交工程演練結果概要(TANet)、附件2_演練成績說明_11102 (A09000000E_1122701002_senddoc7_Attach1.pdf、A09000000E_1122701002_senddoc7_Attach2.pdf)

裝

主旨：檢送本部所屬公務機關及臺灣學術網路111年第2次防範惡意電子郵件社交工程演練結果概要與成績說明（如附件1、2），請查照。

說明：

訂

一、依資通安全事件通報及應變辦法第8條規定及本部「111年度教育部、所屬公務機關及臺灣學術網路防範惡意電子郵件社交工程演練計畫」（以下稱演練計畫）辦理。

二、依演練計畫目標，演練對象之社交工程郵件開啟率、點閱（連結、附件）率應分別低於10%(含)及6%(含)。

線

三、請貴機關配合辦理下列事項：

(一)針對社交工程演練遭誘騙之所屬人員，加強教育訓練，督促其落實公務信件處理安全。

(二)屬演練成績不良之機關，擬定改善措施自行列管並落實執行。如111年度2次成績皆屬不良，須擬定改善計畫回復本部備查。

(三)請加強宣導所屬人員研判信件真偽，針對仿公務類型社

交工程信件提高警覺，不開啟來路不明或可疑之電子郵件及附加檔案，不連結及登入未經確認之網站。

四、本案聯繫窗口：

(一)旨揭演練結果摘要報告之演練對象名稱已代碼化。機關代碼及人員詳細名單，請洽本部楊小姐（電話：02-77129088，電子郵件：cjyang@mail.moe.gov.tw)。

(二)本案其他問題，請洽本部宋先生（電話：02-77129078，電子郵件：a230222@mail.moe.gov.tw)。

正本：部屬機關(構)及國家運動訓練中心、各公私立大專校院、各直轄市及縣市教育網路中心、國立臺灣大學醫學院附設醫院、國立臺灣大學醫學院附設醫院雲林分院、國立臺灣大學醫學院附設醫院北護分院、國立臺灣大學醫學院附設醫院金山分院、國立臺灣大學醫學院附設醫院新竹臺大分院、國立臺灣大學醫學院附設醫院癌醫中心分院、國立成功大學醫學院附設醫院、國立成功大學醫學院附設醫院斗六分院、國立陽明交通大學附設醫院、國立臺灣大學生物資源暨農學院實驗林管理處

副本：本部各單位(資訊及科技教育司除外)、臺灣學術網路區域網路中心、各直轄市政府教育局及各縣市政府(均含附件) 電子公文交換章 2023/03/24 15:05:47

111 年第二次演練結果彙整表_臺北市立大學

代碼	受測 人數	演練信件 開啟人數	演練信件 開啟率	開啟率超過目標值？
B86	49	0	0.00%	N

演練信件連結點選人數	演練信件連結點選比例	演練信件附件點選人數	演練信件附件點選比例
0	0.00%	0	0.00%

演練信件點閱(連結、附件)人數	演練信件點閱(連結、附件)率	點閱率超過目標值？	本次未符合目標值	格式(csv)
0	0.00%	N	N	Y

編碼(UTF-8-BOM)	欄位數(7)	人員類別描述(主管人員/一般人員)	回復資料包含演練人員名單、自我檢核表	自我檢核表已完成檢查及主管核章
Y	Y	Y	Y	Y

未刻意阻擾演練作業寄信主機來源	配合演練信件寄送測試之回復確認作業	本次寄信失敗率	回復資料格式正確性(6%)	回復資料內容完整性(6%)
N	N		6	6

作業配合狀況(8%)	社交工程郵件開啟率(40%)	社交工程郵件點閱率(40%)	分數
0	40	40	92.0

附件3

檔　　號:
保存年限:

臺北市政府　函

地址：110204臺北市信義區市府路1號10樓
承辦人：黃俊瑋
電話：02-27208889#51502
電子信箱：am5043@gov.taipei

受文者：臺北市立大學

發文日期：中華民國112年8月11日
發文字號：府授資安字第1123008279號
速別：普通件
密等及解密條件或保密期限：
附件：臺北市政府所屬人員資通安全事項獎懲基準、臺北市政府所屬人員資通安全事項獎懲基準總說明、臺北市政府所屬人員資通安全事項獎懲基準逐點說明(27066635_1123008279_1_ATTACH1.odt、27066635_1123008279_1_ATTACH2.odt、27066635_1123008279_1_ATTACH3.odt)

主旨：檢送「臺北市政府所屬人員資通安全事項獎懲基準」、總說明及逐點說明各1份，自即日生效，請查照

說明：本案業完成臺北市政府法律事務管理系統線上填報作業，系統流水號為1123400J00169，請法務局刊登臺北市法規查詢系統。

正本：臺北市政府各機關學校(臺北市政府資訊局除外)
副本：臺北市議會（含附件） 電子公文交換章 2023/08/11 10:33:33

市立大學 1120811

VWAA1126023020

臺北市政府所屬人員資通安全事項獎懲基準

中華民國112年8月11日臺北市政府資訊局(112)府授資安字第1123008279號函訂定全文十一點，自函頒日生效

一、本基準依公務機關所屬人員資通安全事項獎懲辦法第二條規定訂定之。

二、本基準所稱臺北市政府（以下簡稱本府）所屬機關，係指依臺北市政府組織自治條例第六條至第八條規定設置之局、處、委員會、區公所，及該等機關所轄機關、機構、學校。

三、本基準所稱本府所屬人員，指下列人員：
（一）本府所屬機關職員。
（二）本府所屬機關聘用人員、約僱人員。
（三）本府所屬機關臨時人員。
（四）本府所屬機關技工、工友及其他與本府所屬機關有僱傭關係之人員。

四、本府所屬人員有下列情形之一者，予以嘉獎：
（一）依資通安全管理法（以下簡稱本法）及其授權訂定之法規或本府規範，訂定、修正及實施資通安全維護計畫，績效優良。
（二）配合上級或監督機關（不含本法主管機關及本府）資通安全維護計畫實施情形之稽核或資通安全演練作業，經評定績效優良。
（三）稽核所屬或監督機關之資通安全維護計畫實施情形或辦理資通安全演練作業，績效優良。
（四）本府資通安全維護計畫實施情形稽核之稽核員，績效優良。
（五）其他有關資通安全事項之優良行為或事蹟，足資獎勵者。

五、本府所屬人員有下列情形之一者，予以記功：
（一）配合本法主管機關及本府資通安全維護計畫實施情形之稽核或資通安全演練作業，經評定績效優良。
（二）辦理本府資通安全維護計畫實施情形之稽核或資通安全演練作業，績效優良。
（三）主動發現新型態之資通安全弱點或入侵威脅，並進行資通安全情資分享，防止資通安全事件之發生或降低其損害。
（四）積極查察資通安全維護之異狀，即時發現重大資通安全事件，並辦理通報及應變，防止其損害擴大。
（五）對資通安全業務提出具體建議或革新方案，並經採行。

（六）辦理資通安全人才培育事務，有具體貢獻。
（七）辦理資通安全科技之研發、整合、應用、產學合作或產業發展事務，有具體貢獻。
（八）辦理資通安全軟硬體技術規範、相關服務及審驗機制發展等事務，有具體貢獻。
（九）辦理資通安全政策、法制研析或國際合作事務，有具體貢獻。
前項第一款記功人員以機關資通安全長及主要辦理人員一至三人為限。

六、本府所屬人員有下列情形之一者，予以申誡：
（一）未依本法及其授權訂定之法規或本府規範辦理下列事項，情節重大：
1. 資通安全情資分享作業。
2. 訂定、修正及實施資通安全維護計畫。
3. 提出資通安全維護計畫實施情形。
4. 辦理資通安全維護計畫實施情形之稽核。
5. 配合上級或監督機關資通安全維護計畫實施情形稽核結果，提出改善報告。
6. 訂定資通安全事件通報及應變機制。
7. 資通安全事件之通報或應變作業。
8. 提出資通安全事件調查、處理及改善報告。
（二）違反本法及其授權訂定之法規或本府規範，致生一級或二級資通安全事件。
（三）對業務督導不力，致其屬員、所屬或所監督機關之人員有前二款情形之一。

七、本府所屬人員有下列情形之一者，予以記過：
（一）違反本法及其授權訂定之法規或本府規範，致生三級以上資通安全事件。
（二）本府所屬人員辦理資通安全業務經本法主管機關、上級或監督機關、本府資通安全主管機關評定績效不良或發現作業缺失，經疏導無效，情節重大。
（三）對業務督導不力，致其屬員、所屬或所監督機關之人員有前二款情形之一。

八、本基準所列嘉獎、記功、申誡、記過之規定，得視事實發生之原因、動機及影響程度等因素，核予一次或二次之獎懲。

九、聘用人員、約僱人員或其他與本府所屬機關具有僱傭關係者，其獎勵及懲處情形應納入續聘之參考。

十、臺北市依自治條例設置之行政法人，就其所屬人員辦理業務涉及資通安全事項之獎懲，得參考本基準之規定自行訂定獎懲基準。

十一、本府所屬人員之獎懲程序，循各類人員相關作業流程處理。