國立臺北大學113學年度個人資料暨資通安全保護管理委員會管理階層審查會議紀錄

紀錄：黃薏琳

時間：113年12月27日(五)上午10時

地點：本校三峽校區行政大樓6樓簡報室

主席：陳俊強副校長

出席人員：陳宥杉主任秘書、林伯星主任、張仁俊教務長(陳志昌副教務長代)、胡中宜學務長(黃鈺婷秘書代)、葉大綱總務長(姜炳俊副總務長代)、魏希聖研發長(舒昌榮專門委員代)、韋岱思國際長(張筱瑩秘書代)、張文俊館長(孫翠莉組長代)、易秀娟主任、李孔文主任(請假)、陳國華部主任、陳達新主任(請假)、李靜雯主任、侯岳宏院長(請假)、黃啟瑞院長(鄭博耕院祕書代)、陳明燦院長、張恒豪院長(郭文忠副院長代)、朱孟庭院長、張玉山院長(沈瑞欽院祕書代)、衛萬明院長(邱淑宜主任代)、法律學系高仁川副教授

列席人員：周冠吉、黃政欽、黃薏琳

壹、主席致詞(略)

貳、工作報告

【資通安全保護管理】

一、第三方團體的建議回饋

【說明】

1. 教育部

(1) 教育部來函(發文文號：臺教資通字第1132701100號)

教育部檢送「資通安全實地稽核項目檢核表」及修正對照表，請各機關更新資通安全稽核計畫之檢核項目，以備實地稽核作業。

(2) 教育部來函(發文文號：臺教資通字第1132700495號)

教育部檢送本校「112年度教育體系資安攻防演練」演練結果及後續改善。

本校資安攻防演練結果，共有27個網頁有安全漏洞風險，資訊

中心已通知網頁各相關單位協請加強措施、修補漏洞及改善處理，並於 112 年 12 月底前改善完成並回復改善結果至資安攻防演練檢核平台。

(3) 數位發展部資通安全署發布之各機關對危害國家資通安全產品限制使用原則(數授資綜字第 1111000056 號函)：
若因業務需求且無其他替代方案需採購或使用中國產品時，應具體敘明理由，經機關資通安全長及其上級機關資安長逐級核可，函報本法主管機關核定後，以專案分式購置，並列冊管理。

(4) 教育部來函(發文文號：臺教資通字第 1130034193 號)
教育部轉知數位發展部有關 112 年「資通安全維護計畫實施情形」及「大陸廠牌資通訊產品盤點」提報作業事宜。

(5) 教育部來函(發文字號：臺教秘(二)字第 1130065428 號)
行政院公共工程委員會檢送數位發展部修正「政府資訊服務採購作業指引」之「使用者體驗」常用資訊服務等級協議(SLA)參考項目。

(6)教育部來函(發文字號：臺教資通字第 1132703538 號)
教育部所屬公務機關及台灣學術網路 113 年第 1 次防範惡意電子郵件社交工程演練結果報告
演練標準：惡意郵件開啟率低於 10%以下，惡意連結(或檔案)點擊率低於 6%以下。

對象	參演人數	開啟郵件		點閱連結		開啟附件		任一行為	
		人數	比率(%)	人數	比率(%)	人數	比率(%)	人數	比率(%)
大專院校及其附設機構	16948	552	3.28%	216	1.27%	240	1.42%	840	4.96%
國立臺北大學	100	0	0.00%	0	0.00%	0	0.00%	0	0.00%

2. 高教深耕計畫資安專章：
   - 落實管理危害國家資通安全產品
     為落實宣導及採購審查機制，從採購源頭做起，請採購單位及審查單位皆須依標準程序審視是否**非大陸廠牌資通訊產品**，以

避免使用單位誤用危害國家資通安全的產品。

- 辦理年度「資訊系統分級與資通安全防護作業」，調查各單位「資訊系統安全等級評估表」，向各單位宣導資訊系統應符合相應安全等級資通安全責任等級分級辦法「附表十 資通系統防護基準」之要求。教育部每年定期會辦理資安攻防演練作業，各單位應依安全基準要求加強資安維護作業。

3. 學術區域網路中心(TANet)：規劃並調整本校連外光纜線路由中央研究院改介接至台北區網中心。
4. 臺灣學術網路危機處理中心：
   不定期轉發並分享「國家資安資訊分享與分析中心」資安訊息警訊，以進行校園資安防護安全。
5. 固網業者：配合本校連外光纜線路調整介接地點。
6. 資訊設備維護商：
   不定期分享資安設備漏洞更新之資安訊息或警訊，以進行校園資通設備防護安全。
7. 校內單位、師生與同仁：無

二、有效性量測(KPI)評量狀況

【說明】量測目標

1.重要系統執行正常運作率一年達 98%。且不可中斷 12 次以上（可用性）。

2.不得發生機密資料外洩情形(機密性)。

3.因惡意程式錯誤造成業務中斷不得發生（完整性）。

4.資訊安全措施或規範符合政策與現行法令之要求(適法性)。

5.定期實施資訊安全教育。

量測結果，請參閱<【資】附件一>。

三、統計資訊安全專業證照與職能證照狀況

【說明】

1. 資訊安全專業證照數量： ISO 27001:2022(10 張)、ISO 27701(2 張)、BS 10012(2 張)
2. 資訊安全職能證照數量：資通安全概論(2 張)、電子郵件安全(1 張)

四、資訊資產與資通系統盤點狀況

【說明】

1. 資訊資產盤點：

(1)已於 113 年 10 月完成資訊資產盤點，並建立資產清冊。

(2)大陸廠牌盤點情形：113 年盤點無大陸廠牌資通訊設備。

2. 資訊系統盤點：

(1)全校資訊系統盤點已於 113 年 4 月完成清查並造冊列管。

(2)資訊系統清單請詳<【資】附件二>。

五、資訊安全管理系統風險評鑑結果

【說明】

依「資訊資產風險評鑑作業辦法(NTPU-ISMS-C-005)」之風險值方法論評估。

風險評估標準：

- 資訊資產價值：將機密性評價、完整性評價與可用性評價相比後取最大值。
- 風險值=資訊資產價值*威脅發生可能性*弱點利用難易度

執行小組建議風險值評估為 16(含)以下，為可接受風險等級。

目前依各單位風險評估之風險值確認，本年度無須進行風險改善。

六、可能影響資訊安全管理系統之內外部事件

【說明】

變更項目	變更內容	因應作為
營運需求變更	無	無
安全需求變更	無	無
業務程序變更	無	無
管理或法規需求變更	規劃修訂本校資通安全管理規範程序書，以符合 ISO 27001:2022 要求。	ISMS 規範與程序更新
契約要求變更	• 禁用大陸品牌之資通訊設備 • 租賃場域禁止使用危害資通系統的產品或設施	加強盤查資產與宣導
可接受風險等級評估標準變更	可接受風險值為16(含)以下之風險	無

七、檢核本校「資訊安全政策」與「資通安全維運計畫」，是否進行變更作業。

【說明】

1. 依據教育部「教育體系資通安全暨個人資料管理規範」與本校「資通安全維運計畫」規定，每年應審查管理制度規範及業務執行狀況。
2. 目前本校無重大組織架構異動或調整，故建議不調整「資訊安全政策」與「資通安全維運計畫」。
3. 本校「資訊安全政策」與「資通安全維運計畫」，請詳<【資】附件三>與<【資】附件四>。

八、資通系統安全檢測執行情形

【說明】

1. 網頁服務弱點掃描作業
   (1) 113 年完成核心資通系統「學生資訊系統、教師資訊系統及行政資訊系統」與「電子郵件系統」之弱點掃描作業，無高風險弱點。
   (2)各單位進行網頁請購與核銷作業時，資訊中心會針對各網頁服務進行弱點掃描，目前 113 年經統計共有 92 個網頁(含重複網頁)已有進行弱點掃瞄作業，並將風險報告轉知各網頁系統管理者知悉。
2. 作業系統弱點掃描作業
   113 年已完成作業系統弱點掃描，共 4 次(校務資訊系統、全球資訊網、郵件系統 mail&webmail)，無高風險。
3. 「教育體系資安攻防演練平台(CODE)」安全檢測
   本校各資通系統(含各單位網頁、服務主機..等)於民國 113 年 7 月至 9 月間由「教育體系資安攻防演練平台(CODE)」進行 113 年安全檢測(每年定期檢測至少 1 次)。經檢測後，本校共被告知有 7 個系統有安全弱點，分別是資訊工程學系網頁與系友通訊錄管理系統、校務資訊系統(學生)、推廣教育組網頁、GPS 水氣資料共享平台、歷史學系網頁、回聲計畫客製化文字轉語音系統測試頁面…等。
   目前上述安全弱點問題，皆經各單位管理者通知系統維護廠商處理並改善完成。

九、安全檢核控制措施之內部稽核執行狀況

【說明】

1. 本校內部稽核規劃與執行，依公文文號第 1139500118 號辦理， 採 3 年一循環進行各單位稽核作業安排，並邀請各單位個資與資安窗口於民國 113 年 6 月進行各年度的稽核單位抽籤作業完成。經抽籤結果，說明如下(以下為抽籤序排列)：

- 民國 113 年：資訊中心、國際事務處、人事室、主計室、進修暨推廣部、校友中心、體育室與永續辦公室。
- 民國 114 年：秘書室、教務處、總務處、研究發展處、高等教育深耕計畫辦公室、商學院、法律學院、公共事務學院。
- 民國 115 年：資訊中心、學生事務處、圖書館、社會科學學院、人文學院、電機資訊學院、永續創新國際學院、通識教育中心　。

2.本次內部稽核執行日期： 113 年 11 月 11 日

3.內部稽核實施內容

依「內部稽核及矯正預防管理程序」與「校園資通安全維護計畫」實施，並偕同個資保護管理制度推動作業共同辦理。

4.稽核範圍

本校核心資通系統、資訊機房維運管理，以及本校一級單位(含所屬二級單位)，包含資訊中心、國際事務處、人事室、主計室、進修暨推廣部、校友中心、體育室與永續辦公室等。

5.查核結果：資訊安全項目缺失有 14 項不符合事項以及 1 項建議事項，請詳<【資】附件五>。

十、預防與矯正措施之狀況

【說明】

1. 內部資訊安全稽核不符合事項矯正預防

由稽核小組委請外聘專家學者於 113 年 11 月 11 日進行本校個資暨資安內部稽核作業，關於資安項目之缺失提出不符合事項共 14 項及 1 項建議事項，目前尚再追蹤各單位缺失矯正處理情形。

2. 其他改善追蹤事項

統計民國 112 年 12 月至民國 113 年 12 月間矯正處理單共有 14 件需改善處理(其中包含教育體系資安攻防演練平台 CODE 的安全檢測安全弱點項目)，經查目前皆已矯正改善完成。

【個人資料保護管理】

一、個資管理變更要求： 無。

二、個資保護管理目標與指標量測執行結果：

(一)依據本校 NTPU-PIMS-A-001 個人資料保護管理政策，總計 5 項管理目標如下：

1.依「個人資料保護法」、「個人資料保護法施行細則」、「教育體系資通安全

暨個人資料管理規範」要求，保護個人資料蒐集、處理、利用、儲存、傳輸、銷毀之過程。

2. 為保護本校業務相關個人資料之安全，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。

3. 提升對個人資料之保護與管理能力，降低營運風險，並創造可信賴之個人資料保護及隱私環境。

4. 為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。

5. 定期識別作業流程之個人資料檔案並執行風險評估，鑑別可接受之風險等級與風險處理作業。

(二)依本年度內部稽核執行結果，5 項個人資料保護管理之目標均有效執行，請參閱「個人資料保護管理制度有效性量測表」(詳見【個】附件 1)。

三、個人資料侵害事件緊急應變模擬演練：全球變遷與永續科學研究中心、歷史系、財政系、環境組、課務組、大數據與智慧城市研究中心，皆於 113 年 12 月 16 日完成模擬演練作業，相關個人資料侵害事件緊急應變計畫、通報與紀錄表(詳見【個】附件 2)。

四、內部稽核作業：資訊中心、國際事務處、人事室、主計室、進修暨推廣部、校友中心、體育室與永續辦公室，已於 113 年 11 月 11 日完成內部稽核作業，內部稽核計畫及稽核報告書(詳見【個】附件 3)，將持續追蹤矯正進度。

五、資安事故與不符合項目之矯正情形：本校 113 年有 1 件個資通報事件，惟經調查後並無個資洩漏之情事，通報與紀錄表 (詳見【個】附件 4)。

六、個人資料盤點作業與風險評鑑結果：

(一)本校於 113 年度執行盤整個人資料檔案作業，總計 1,089 項個人資料在案，檔案風險值落於 2-9 之間，沒有須進行風險處理之個人資料檔案。

(二)依據 107 年教育體系資通安全暨個人資料管理規範所制訂之本校個人資料保護管理制度文件，113 年度共計 11 個單位修改個人資料檔案相關資料(如個人資料檔案清冊、風險評估表及公開項目彙整表等)，前揭檔案均已建立個人資料安全控管程序及相關文件。

參、前次會議執行情形：

案 由 一：有關本校 113 年度個人資料保護管理制度盤點作業及教育訓練時程，提請討論。

決　　議：照案通過。

執行情形：照案執行。

案 由 二：為了解本校各單位因執行業務向當事人蒐集個人資料時， 是否依循相關規定辦理，擬進行現況調查作業，提請討論。

決　　議：照案通過。

執行情形：照案執行。

案 由 三：校園資通安全(個資與資安)內部稽核作業時程規劃、稽核人員選任方式與經費來源，提請討論。

決　　議：照案通過。

執行情形：照案執行。

肆、討論事項：

案由一：有關本校 114 年度個人資料暨資通安全保護管理制度盤點作業及教育訓練時程，提請討論。

說　明：

一、為強化校內同仁之個人資料保護與資訊安全素養及觀念，規劃於 114 年度辦理全校性個資與資安管理教育訓練至少 4 場，請各單位派員參與訓練。

二、規劃於 6 月至 8 月進行各單位個人資料檔案與資訊資產盤點作業，請各單位依業務流程清查所屬單位所業管之個人資料檔案清冊、公開項目彙整表、風險評估表、資訊資產清單及威脅及弱點評估表。

三、規劃於 10 月至 11 月辦理個資侵害事件緊急應變模擬演練，以及個資暨資安內部稽核作業。

決　議：**照案通過。**

伍、臨時動議

【建議事項】

■ 高仁川委員：考量師生的人身安全和個資保障的重要性，提議強化校園個資隱私保護設施的設置，如：監視錄影器的設置。透過盤點校園內現有監視錄影器的數量、設置現況，作為追加預算或列為優先執行預算的參考。

■ 陳俊強主席：

一、以校內監視器安裝現況，管理單位分別有：總務處、部分學院系所；依法規及公共需求必須設置的監視器由總務處管理，教學單位則依單位需求自行加裝監視器。

二、總務處已著手規劃校內監視器的新增及汰換，惟考量設備購置與維運皆花費甚鉅，目前請總務處研議與監視器廠商簽訂租賃契約方式的可行性與效益。

陸、散會(上午 11:07)