國立臺北大學 114 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：黃蕙琳

時間：114 年12 月30 日(二)下午 1 時30 分

地點：本校三峽校區行政大樓 6 樓簡報室

主席：張玉山副校長

出席人員：胡龍騰主任秘書、汪志堅主任、陳婉琪教務長、胡中宜學務長(陳三義組長代)、王佳惠總務長(高仁川副總務長代)、陳裕賢研發長(舒昌榮專門委員代)、韋岱思國際長(林予安組長代)、洪健榮館長(賴郁蕙秘書代)、蔡佳靜代理主任、李慧強主任、薛敏正部主任(請假)、吳慧卿主任、郭大維院長、黃啟瑞院長(鄭博耕院秘書代)、陳明燦院長、林昭吟院長(范捷然執行秘書代)、朱孟庭院長、楊棧雲代理院長(鄒欣宜院助理代)、詹佳縈院長、法律學系高仁川副教授

列席人員：資訊中心周冠吉助教、林金霖程式設計師
秘書室黃蕙琳助理

壹、主席致詞(略)

貳、工作報告

主席裁示：

一、自114-2學期開始，管審會每學期召開一次。

二、有關【資】附件一中提及教育訓練時數未達標之量測項目，請資訊中心通知未達成教育訓練時數之同仁及其所屬主管知悉，以達成每年度人員教育訓練時數之規定。

【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

編號	關注訊息來源	關注訊息內容	備註
1	公文	有關行政院來函說明盤點大陸廠牌資通訊產品及委外營運公眾場域契約事宜，及進行資安宣導，請查照並轉知所屬。	教育部 114年 1月14 日臺教資通字第1130136777 號函
2	公文	檢送「學校使用資通系統或服務蒐集及使用個人資料注意事項」及「校園使用生物特徵辨識技術個人資料保護指引」各 1 份，並自即日生效，請查照並轉知所屬學校。	教育部 114 年 2 月 4 日臺教資通字第1132705044 號函

<table>
<tr><td>3</td><td>公文</td><td>檢送本部 114 年度對所屬公務機關及所管特定非公務機關資通安全稽核計畫，請查照辦理。</td><td>教育部 114 年 3 月 4 日臺教資通字第 1142700536 號函</td></tr>
<tr><td rowspan="2">4</td><td>公文</td><td>檢送 114 年度本部、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，請查照。
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。</td><td>教育部 114 年 3 月 6 日臺教資通字第 1142700703 號函</td></tr>
<tr><td>演練結果</td><td colspan="3"><table>
<tr><th>受測人數</th><th>演練信件開啟率</th><th>演練信件連結點選比例</th><th>演練信件附件點選比例</th><th>演練信件點閱(連結、附件)率</th><th>回復資料包含演練人員名單、自我檢核表</th><th>未刻意阻擾演練作業寄信主機來源</th><th>配合演練信件寄送測試之回復確認作業</th><th>分數</th></tr>
<tr><td>100</td><td>0.00%</td><td>0.00%</td><td>0.00%</td><td>0.00%</td><td>Y</td><td>Y</td><td>Y</td><td>100</td></tr>
</table></td></tr>
<tr><td>5</td><td>公文</td><td>有關 114 年本部對國立臺北大學資通安全稽核，受機機關配合事項，請查照。</td><td>教育部 114 年 3 月 14 日臺教資通字第 1142700806A 號函</td></tr>
<tr><td>6</td><td>公文</td><td>函轉數位發展部函有關 113 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，請查照並轉知所屬。</td><td>教育部 114 年 4 月 1 日臺教資通字第 1140029433 號函</td></tr>
<tr><td>7</td><td>公文</td><td>為因應新型態數位服務延伸之新興資安風險，請各機關遵循「危害國家資通安全產品限制使用原則」，並依規定辦理，請查照。</td><td>教育部 114 年 4 月 11 日臺教資通字第 1140036031 號函</td></tr>
<tr><td>8</td><td>公文</td><td>函轉行政院資通安全稽核計畫及稽核作業說明簡報，請預為準備，請查 照。</td><td>教育部 114 年 4 月 11 日臺教資通字第 1140037871 號函</td></tr>
<tr><td>9</td><td>公文</td><td>檢送修正「資通安全稽核項目檢核表」及修正對照表，請查照。</td><td>教育部 114 年 4 月 25 日臺教資通字第 1142701351 號函</td></tr>
<tr><td>10</td><td>公文</td><td>「教育部補助資通安全及網路先導應用服務建置要點」，業經本部於中華民國 114 年 5 月 2 日以臺教資通字第1142700833A 號令修正發布，茲檢送發布令影本及行政規則修正規定各 1份，請查照。</td><td>教育部 114 年 5 月 2 日臺教資通字第 1142700833B 號函</td></tr>
</table>

11	公文	函轉數位發展部檢送「113 年度資通安全稽核共同發現事項及建議」1 份，請查照並轉知所屬。	教育部 114 年 5 月 21 日臺教資通字第 1140053829 號函
12	公文	函轉數位發展部訂定「公務機關資通安全業務績效評核獎勵金支給表」，並自中華民國一百十四年一月一日生效，請查照並轉知所屬。	教育部 114 年 6 月 4 日臺教資通字第 1140058298 號函
13	公文	為每二年提交本部所屬或監督之公務機關及所管之特定非公務機關之資通安全責任等級，請於 114 年 6 月 19 日前依式函復調查表，請查照。	教育部 114 年 6 月 6 日臺教資通字第 1140056137A 號函
14	公文	有關 Penoval 品牌觸控筆涉資通安全風險案，請各機關依規定檢視使用情 形，請查照。	教育部 114 年 7 月 8 日臺教資通字第 1140068637 號函
15	公文	函轉經濟部標準檢驗局勘誤CNS 27001「資訊安全、網宇安全及隱私保護-資訊安全管理系統-要求事項」等 5 種國家標準，請查照。	教育部 114 年 8 月 27 日臺教資通字第 1140089272 號函
16	公文	函轉國家資通安全研究院自即日起提供線上訂閱資通週報服務，請查照並轉知所屬。	教育部 114 年 11 月 24 日臺教資通字第 1140120309 號函
17	公文	函轉行政院有關本部 114 年所屬大專校院及其附設機關(構)之資通安全責任等級業經核定，請查照。	教育部 114 年 11 月 27 日臺教資通字第 1142703749A 號函

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. 數位發展部：
   提供資安週報線上訂閱服務，妥善參酌資安週報，運用於資通安全管理相關工作。
4. 學術區域網路中心(TANet)：
   本校已調整上層連網組織架構，原由中央研究院改介接至台北區網中心維運管理，且每年須參加區網會議，遵循區域網路規定辦理並取得資安情資資源。
5. 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。
6. 固網業者：配合本校連外光纜線路調整介接地點，並維護網路光纜線路正常維運。
7. 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。
8. 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)、BS10012(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 114 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： 114 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 114 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	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」

3.本校「資通安全維運計畫」經今(114)年 7 月教育部部屬機關實地資通安全稽核作業，稽核委員指導本校核心業務「校園網路維運系統」非資通系統，建議可刪除。故調整「資通安全維運計畫」。

4.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) 114 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 114 年經統計共有 81 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

114 年已完成作業系統弱點掃描，共 5 次(校務資訊系統、郵件系統mail 與 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 114 年 7 月至 9 月間由「教育體系資安攻防演練平台(CODE)」進行 114 年安全檢測(依規定每年定期檢測至少 1 次)。

經檢測後，本校共被告知有 5 個系統有安全弱點，分別是「GamePlatform .git leak」、「企業管理學報學報投審稿系統」、「土地與環境規劃研究中心網頁系統」、「公行系中英文網站」與「永續創新國際學院網頁」。

目前上述安全弱點問題，除「土地與環境規劃研究中心網頁系統」限制校內連線外，其餘皆經各單位管理者通知系統維護人員處理並改善完成。

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： 114 年 11 月 26 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

本校一級單位(含所屬二級單位)，包含秘書室、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、法律學院與公共事務學院等。

5. 查核結果：資訊安全項目缺失有 35 項不符合事項，請詳<【資】附件五>。

十、預防與矯正措施之狀況

【說明】

1. 教育部資安技術檢測

教育部於 114 年 6 月 16-17 日進行本校資安技術檢核作業，經檢核結果共發現 96 個須改善事項，截至今日尚有 18 個待改善事項尚未改善完成，未改善完成項目請詳<【資】附件六>。

2. 教育部資通安全二方實地稽核作業

教育部定期每 2 年進行公務機關資通安全實地稽核作業，本年度已於 114 年 7 月 22 日進行查核作業，經檢核共發現 18 待改善事項以及 15 個建議事項，改善情形請詳<【資】附件七>。截至今日尚有 8 個缺失尚未改善完成。

3. 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 114 年 11 月 26 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 35項(詳<【資】附件五>)，目前尚再追蹤各單位缺失矯正處理情形。

4. 其他改善追蹤事項

統計民國 113 年 12 月至民國 114 年 12 月間矯正處理單共有 5 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。檢核報告請詳<【資】附件八> 。

【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：國際事務處(含國合組、國發組)、永續辦公室、學務處生輔組、學務處軍訓室、體育室、經濟系、資訊中心作業組，皆於 114 年 12 月 29 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：教務處、總務處、研究發展處、秘書室、商學院、公共事務學院、法律學院及高教深耕辦公室，已於 114 年 11 月 26 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：無。

六、個人資料盤點作業與風險評鑑結果：

(一)本校於 114 年度執行盤整個人資料檔案作業，總計 1,127 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，114 年度共計 9 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 114 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。

肆、討論事項：

案由一：有關本校 115 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 115 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 9 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 11 月至 12 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：修正通過，自115學年度開始，請調整盤點作業及教育訓練於暑假期間辦理，模擬演練及內部稽核作業於寒假期間辦理。

案由二：今(114)年教育部資通安全稽核技術檢核團隊提出「本校行政、教師和學生資訊系統於密碼變更時，至少不可以與前三次使用過之密碼相同」之缺失，相關預計改善措施提請審議。[矯正處理表請詳<【資】附件九>]

說　明：

一、由於啟用使用者在修改密碼時，無法使用與至少前 3 次相同的密碼，後續會衍生使用者修改密碼的不便，例如：使用者忘記密碼，要重新設定密碼時，就無法立即使用先前慣用的密碼。

二、預計會在明(115)年 8 月 1 日正式於行政、教師和學生資訊系統實施「密碼變更時，至少不可以與前三次使用過之密碼相同」，並於開始實施前公告調整原因與更新說明使用方式，降低對行政人員、教師和學生的影響。

決　議：照案通過。

伍、臨時動議(**無**)

陸、散會(14:35)