

## 國立臺北科技大學 109 學年度第一學期計算機與網路發展指導委員會會議紀錄

時間：中華民國 110 年 1 月 15 日（星期五）上午 10 時 10 分

地點：行政大樓九樓國際會議廳

主席：王主任委員永鐘

紀錄：洪碧珍

出席：楊士萱教務長、張仁家學務長、陳昭榮總務長、蘇昭瑾研發長、莊賀喬國際長(李瑞元<sup>代</sup>)、黃聲東產學長(宋春樺<sup>代</sup>)、吳建文圖資長、進修部劉建浩主任、蘇程裕主任秘書(高千智<sup>代</sup>)、機電學院李春穎院長、電資學院黃育賢院長、工程學院宋裕祺院長(陳亭華<sup>代</sup>)、管理學院邱垂昱院長(林芷瑩<sup>代</sup>)、設計學院黃志弘院長(陳振誠<sup>代</sup>)、人文與社會科學學院李傑清院長(吳同鈞<sup>代</sup>)、能源系陳清祺教授、自動化所陳文輝教授、電機系吳昭正教授、電子系李文達教授、光電系鄭鈺潔教授、化工系李旻聰教授、資源所邱家吉教授、土木系林祐正教授、分子系許益瑞教授、環境所曾昭衡教授、資財系陳俊豪教授(魏鎬志<sup>代</sup>)、工設系江振維教授、建築系陳振誠教授、互動系王聖銘教授、技職所蔡佩珊教授、應英系辜炳達(黃如妍<sup>代</sup>)教授、智財所陳志遠教授、通識教育中心林建洲教授、體育室張文馨教授、學生代表陳懋晨同學、學生代表楊子萱同學及計網中心同仁(機械系許志明教授、車輛系陳柏全教授、製科所何昭慶教授、資工系劉建宏教授、材資系李文正教授、工管系張文華教授、經管系張瑋倫教授及文發系吳宇凡教授請假)

列席指導：任副校長貽均

## 壹、主席報告

今日適逢期末最後一天，感謝任副校長、各位主管及委員撥冗出席會議。以下為計網中心本學期的工作重點：

一、109 年教育部對本校進行全機關實地資通安全稽核作業，12 月 8 日及 9 日為技術檢測，12 月 23 日則是針對管理面、政策面與技術面進行檢核。在本次稽核過程中已可預知未來對於資安的要求將會越來越嚴謹，可能造成大家的不便，但由於行政院資安處及教育部資科司的要求，未來將不限只是在計網中心，而是本校全機關的資安稽核，這部分需要全校教師及同仁的協助及配合。

二、同樣是資安的議題。為避免發生資安問題時通報教育部造成各單位困擾，計網中心系統組訂定「委外資訊系統建置需求標準作業流程」，請各單位於系統採購或續約維護前先依該標準作業流程進行審視，並非要為難大家，目的是要透過該標準作業流程降低資安的風險。目前行政單位的申請案都已納入管理，教學單位如有需求，亦可填寫該標準作業流程，由本中心系統組協助審視。



三、承蒙任副校長及電資學院黃院長極力爭取教育部「優化技職校院實作環境計畫」經費，計網中心協助建置北科 AI 運算平台，日前與他校交流，管理機制大獲肯定。各位委員如果在執行計畫時需要用到繁重的運算資源，歡迎申請使用，盼此能創造出更多研究計畫與機會。NVIDIA 公司同時亦提供自駕車、醫療及工廠生產等相當完善之開發工具環境，中心將於準備完善後將其開放於平台使用，期能大幅度降低研究的門檻，促進相關計畫進行。計網中心規劃與 NVIDIA 辦理開發工具環境說明會，歡迎各位老師參加。

以上為本中心這學期的工作重點，感謝各位委員的指導、參與，在此並先向各位拜個早年，敬祝各位長官及委員大家新年快樂。

#### 貳、任副校長致詞：

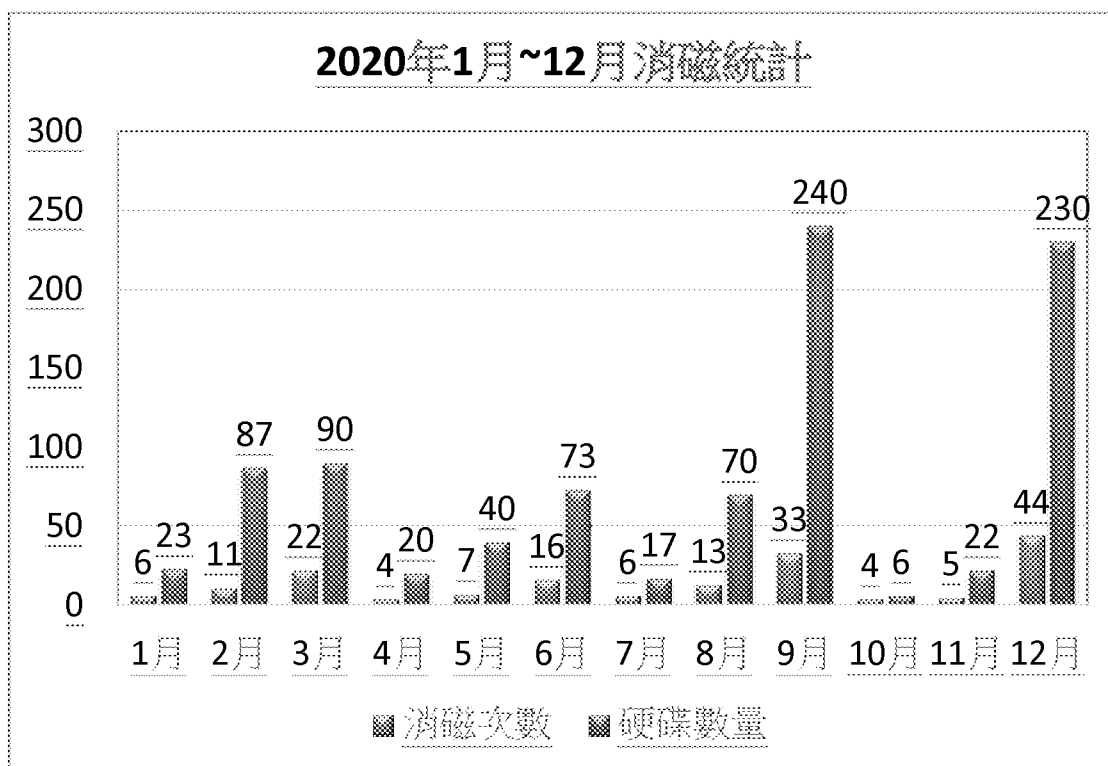
首先感謝各位委員參加會議。109 年本校接受教育部的資安稽核，整個過程都是以非常高的標準檢視本校的資安，不只是計網中心，也包含學校其他單位；會後稽核團隊提供了非常多的意見，這些意見有些是學術單位在短時間無法達到，有些是可以參考的。但無論如何這些意見都提醒學校重視資安，並指引了我們一些方向。俟本校收到教育部的資安稽核意見後，會再和各單位說明。在此呼籲各單位要重視資安這件事，未來資安的檢視將是全校性的，包含行政單位及教學單位。也感謝計網中心同仁這一年來的努力，謝謝大家！

#### 參、工作報告

※行政及諮詢組：

##### 一、已完成項目：

- (一) 配合總務處經管組電腦報廢財產點收作業，109 年 1 月至 12 月共計消磁總硬碟數 918 顆 (詳如圖一)。



圖一、109年1月至12月全校消磁統計圖

(二)本學期全校各單位申請電腦維修數量共計 249 件(詳如表一)。

表一、109年6月至12月各單位維修統計表

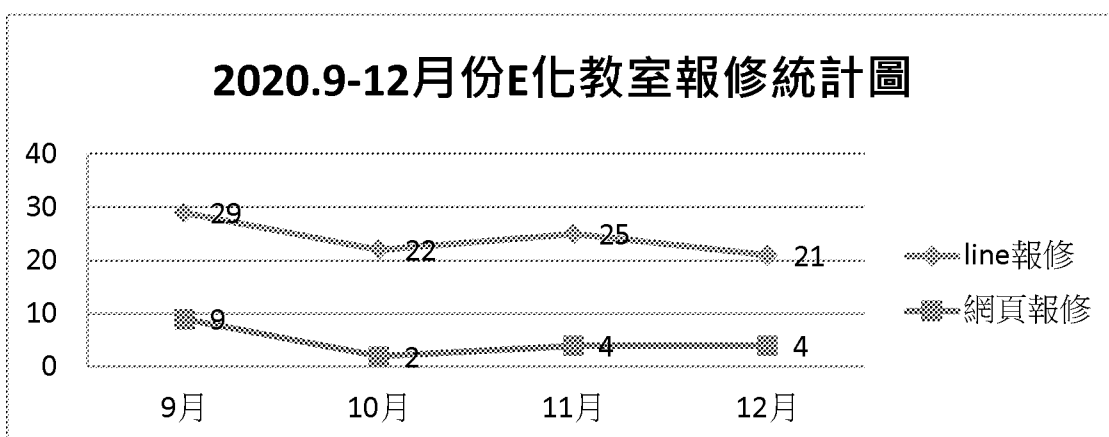
單位	件數	單位	件數	單位	件數	單位	件數
秘書室	8	國際事務處	4	機電學院	8	體育室	4
教務處	11	人事室	1	電資學院	28	其他 (未註明)	5
學務處	25	軍訓室	3	工程學院	47		
總務處	29	進修部	5	管理學院	13		
研發處	10	安環中心	4	設計學院	10		
產學處	5	計網中心	15	人文學院	14		
總計	249 件						

(三) 109年9月至12月檢測各e化教室環控設備、投影機與監視系統等報修項目，共計 116 次(詳如表二及圖二)：

表二、109年9月至12月e化教室報修統計表

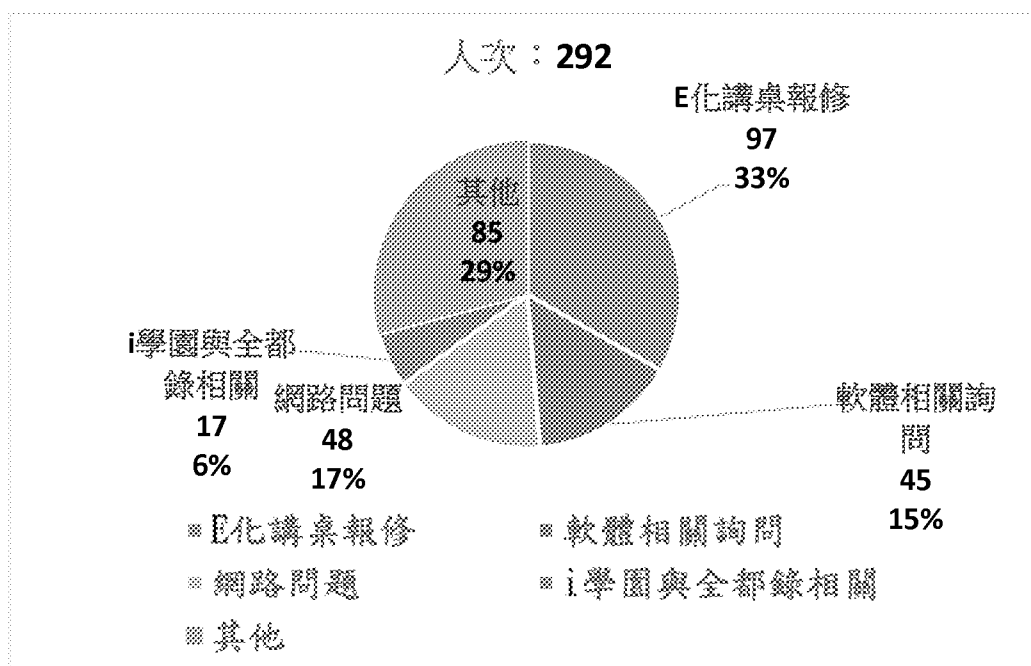
故障問題	硬體	軟體	破壞	自然	誤報	操作	其他
------	----	----	----	----	----	----	----

項目	問題	問題	盜竊	損壞		不當	原因
電腦	20	23	0	0	16	7	10
講桌本體	15	-	4	0			
單槍與銀幕	5	0	0	2			
網路攝影機	0	0	0	0			
電箱與 PCI8	3	-	0	0			
環控設備	2	0	0	0			
擴大機與麥克風	7	-	0	0			
觸控螢幕	2	0	0	0			
總計	54	23	4	2			



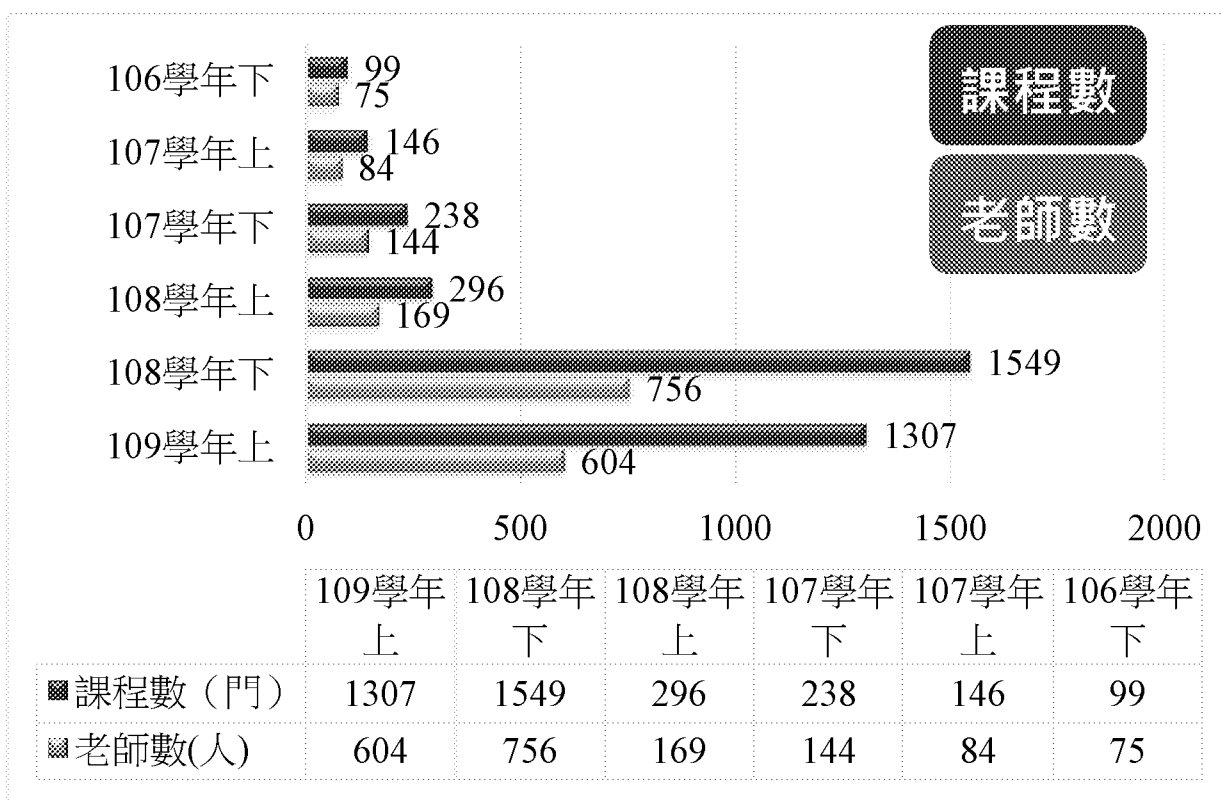
圖二、109年9月至12月E化教室報修統計圖

(四) 本中心 Line@服務於 109 年 9 月至 12 月共有 292 人次報修或詢問(詳如圖三)，其中 E 化講桌報修佔 33%，網路問題佔 17%，軟體相關詢問佔 15%，i 學園與全都錄相關詢問佔 6%，其他佔 29%(如電子郵件、校友相關、詢問其他單位問題等)。



圖三、109 年 9 月至 12 月 Line@報修及詢問統計圖

(五) 本學期計有 1307 門課及 604 位老師使用教學全都錄，106 學年至 109 學年錄影課程數與老師參與數之統計資料請參閱圖四及表三。



圖四、錄影課程數與老師人數統計圖

表三、102 學年下學期至 109 學年上學期-各學院使用全都錄錄影課程數統計表

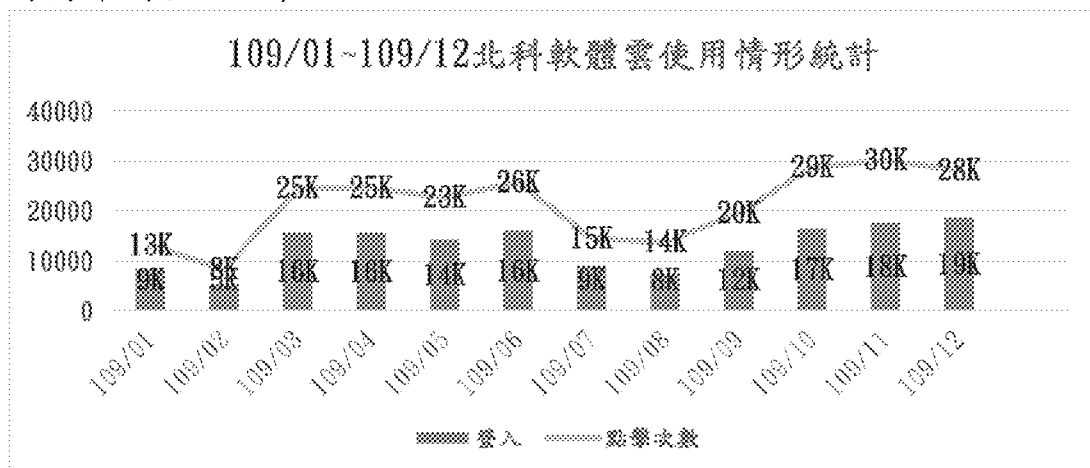
	機電	電資	工程	管理	設計	人社
109 學年上	127	206	210	89	46	92
108 學年下	163	258	216	159	70	110
108 學年上	45	69	62	51	12	57
107 學年下	39	65	56	26	4	48
107 學年上	19	46	30	16	4	31
106 學年下	15	27	24	10	2	21
106 學年上	46	40	36	13	2	31
105 學年下	33	36	43	10	3	25
105 學年上	25	23	36	13	7	30
104 學年下	15	30	31	5	8	13
104 學年上	13	24	29	3	0	22
103 學年下	12	31	28	7	0	10
103 學年上	9	31	42	3	1	14
102 學年下	9	16	15	1	2	4
各學院課程 數總計	<b>570</b>	<b>902</b>	<b>858</b>	<b>406</b>	<b>161</b>	<b>508</b>

(六) 北科 VCP-AI 雲端運算平台已於 109 年 7 月完成平台網路及儲存架構調整。109 年 9 月平台已正式上線，並將持續依使用情形進行功能調整及使用規範。

(七) 北科軟體雲相關業務：

- 1、109 年 8 月完成平台年度更新及維護。
- 2、109 年 5 月至 9 月完成：[Autodesk、Solidworks、Matlab] 等 8 項軟體更新及上架作業。
- 3、109 年 10 月完成北科軟體雲及開放電腦教室網域管理系統安全性更新。
- 4、109 年 11 月完成教育部自由軟體作業系統-EzGo 雲端桌面佈署、共同科館 111 電腦教室-精簡客戶端佈署及效能調校以及 Adobe 使用專區佈署。
- 5、109 年 12 月完成虛擬機作業系統及代理程式更新。

(八) 109 年 1 月至 12 月北科軟體雲之使用情形(詳如圖五及表四)，每月平均登入 13,151 人次。



圖五、109 年 1 月至 12 月北科軟體雲登入及點擊次數統計圖

表四、109 年 1 月至 12 月北科軟體雲登入及點擊次數統計表

月份	1	2	3	4	5	6	7	8	9	10	11	12	平均
登入	8626	5431	15806	15762	14382	16103	9151	7594	12038	16536	17698	18689	13151
點擊次數	13268	8466	24679	24742	22847	25911	14623	13904	19740	28909	30315	28281	21307

(九) 109 學年度第 1 學期北科 VCP-AI 雲端運算平台使用統計如下(詳如表五及表六)：

1. 平台專案申請總計 33 筆。

表五、專案申請統計表

系所	數量	系所	數量	系所	數量
電資學院	3	計網中心	1	光電系	2
電機系	14	製科所	3	五專自動科	2
電子系	5	自動化所	3	其他	4
資財系	5	機械系	1		
資訊系	7	工程學院	1		
合計	33				

2. 使用者 GPU 運算資源佈署，運算環境佈署共 702 次。

表六、GPU 運算環境佈署統計表

系所	GPU 總數/ 次數	系所	GPU 總數/ 次數	系所	GPU 總數/ 次數
電資四	2 / 2	資財碩二	1 / 1	職電機碩三	2 / 2
電機碩二	84 / 93	資財系	2 / 2	職電子碩三	2 / 3
電機碩三	810 / 174	資訊系	2 / 2	職自動化碩四	17 / 19
電機系	5 / 5	資工碩二	12 / 12	職自動化碩三	9 / 9
電機博四	4 / 4	資工三	1 / 1	機電碩二	6 / 6
電子碩二	69 / 74	計網中心	54 / 64	智動三	59 / 64
電子碩一	2 / 3	製科碩三	12 / 14	光電碩二	3 / 3
電子系	9 / 9	自動碩四	4 / 5	其他	124 / 131
合計	1295 / 702				

\*GPU 用量係指使用者每次使用 GPU 數量之加總(單位：張\*次)

\*次數係指使用者成功佈署環境之次數

(十) 109 年 8 月完成共同科館 412、413 電腦教室高架地板翻新與線路重整工程。

(十一) 109 年 8 月完成 NI LabVIEW 全校授權採購作業。

(十二) 109 年 9 月完成 Matlab、Apexone 與 PC-Cillin 全校授權採購作業。

(十三) 109 年 10 月完成微軟全校授權採購作業。

## 二、進行中及擬辦項目：

(一) 寒假期間將進行全教室 e 化講桌清潔，講桌電腦系統更新、防毒軟體更新，預計 110 年 2 月開學前完成。

(二) 因應北科軟體雲使用者需求增加，將進行虛擬化伺服器及儲存設備擴充，預計 110 年 8 月完成。

(三) 北科 VCP-AI 雲端運算平台相關項目：

1、持續依使用情形進行功能調整及使用規範。

2、監控及資源佈署功能擴增及修正。

3、建立使用者資料封存機制。

4、修正校園入口網站單一簽入機制，改善使用者體驗。

(四) 延續電腦教室防疫作業，自開學起每周進行計中電腦教室消毒及打掃。

## ※網路作業組：

### 一、已完成項目：



- (一) 109 年 10 月完成本校第二次社交工程演練，統計結果請參考表七至表九。已於 12 月 3 日辦理第三梯次資訊安全觀念宣導教育訓練，課程教材置於校園入口網站之雲端資料夾。
- (二) 本校 109 年第二次社交工程演練結果，寄發測試信件總數為 5,696 封(前次 5,370 封)，總測試人數為 1,424 人(前次 1,112 人)，開啟人數計 31 人(前次 57 人)，開啟率為 2.2%(前次 5.1%)；連結點閱人數計 27 人(前次 45 人)，點閱率為 1.9%(前次 4%)，詳如表八及表九。

表七、社交工程演練郵件主旨分類表

類別	郵件主旨
健康	「168 斷食法」有效？營養師實測：瘦 7 公斤
國際	美國大選最新民調出爐 台網友驚呼：押錯寶了？
娛樂	丁國琳昔遭渣男「爽玩 6 人行」未婚產女
科技	iPhone12 防摔、夜拍、售價是亮點

表八、演練結果信件開啟率 TOP10

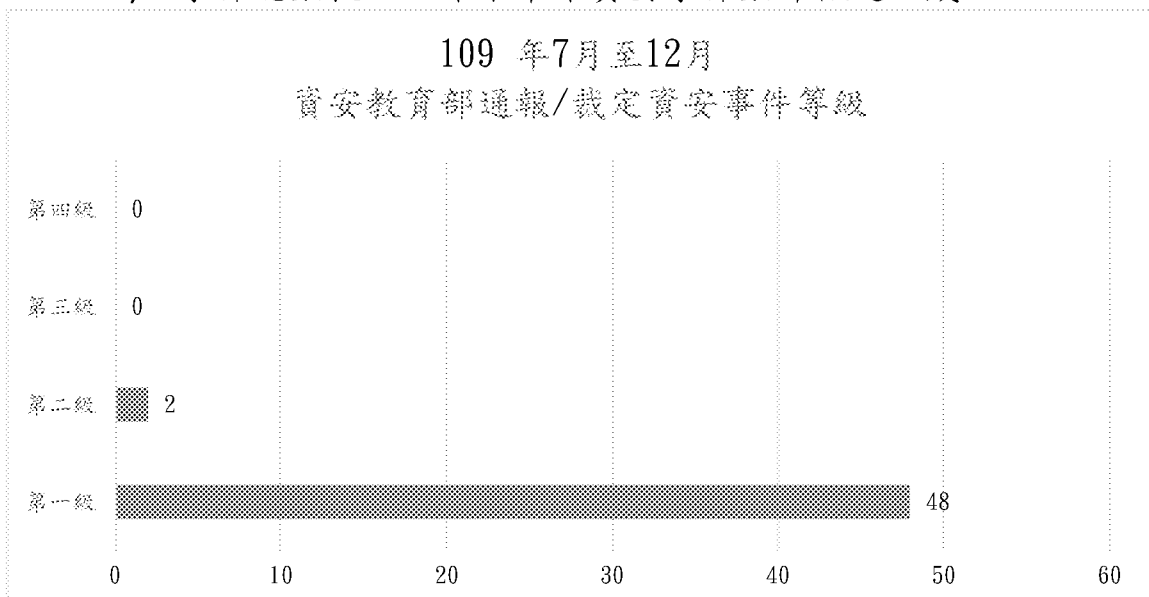
Top	單位	演練人數	開啟人數	開啟次數	開啟率 開啟人數/ 演練人數
1	木藝培育暨設計研發中心	1	1	1	100%
2	資源工程研究所	12	3	9	25%
3	安全衛生環保中心	5	1	1	20%
4	技專校院招生策進總會	7	1	2	14%
5	工程學院	15	2	20	13%
6	生化與生醫工程研究所	8	1	3	13%
7	五年制專科部 智慧自動化工程科	9	1	3	11%
8	管理學院	14	1	2	7%
9	車輛工程系	19	1	7	5%
10	土木工程系	40	2	4	5%

表九、演練結果信件點選連結率 TOP10

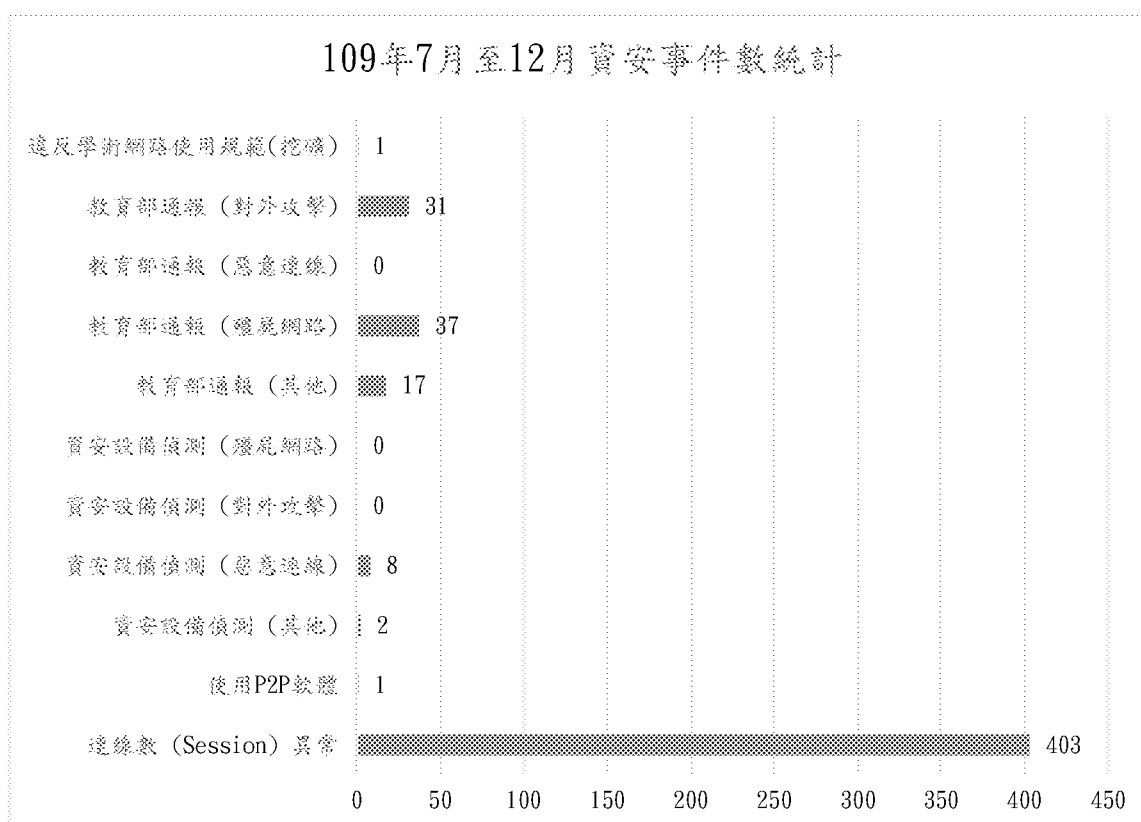
Top	單位	演練人數	連結人數	連結次數	連結率 連結人數/ 演練人數
1	安全衛生環保中心	5	1	2	20%
2	人事室	20	2	4	10%

3	軍訓室	14	1	1	7%
4	工程學院	15	1	5	7%
5	圖書資訊處	15	1	1	7%
6	技術及職業教育研究所	19	1	2	5%
7	聯合會	19	1	1	5%
8	主計室	20	1	4	5%
9	製造科技研究所	20	1	1	5%
10	學生事務處	43	2	2	5%

(三) 109 年 7 月至 12 月教育部通報與裁定資安事件等級總數為 50 件(上半年 49 件)(詳如圖六)，核心系統受到影響之二級以上資安事件 2 起。校內資安事件總數為 500 件(上半年 886 件)(詳如圖七)，事件總數較 108 年下半年資安事件數降低近五成。



圖六、教育機構資安通報平台事件統計圖

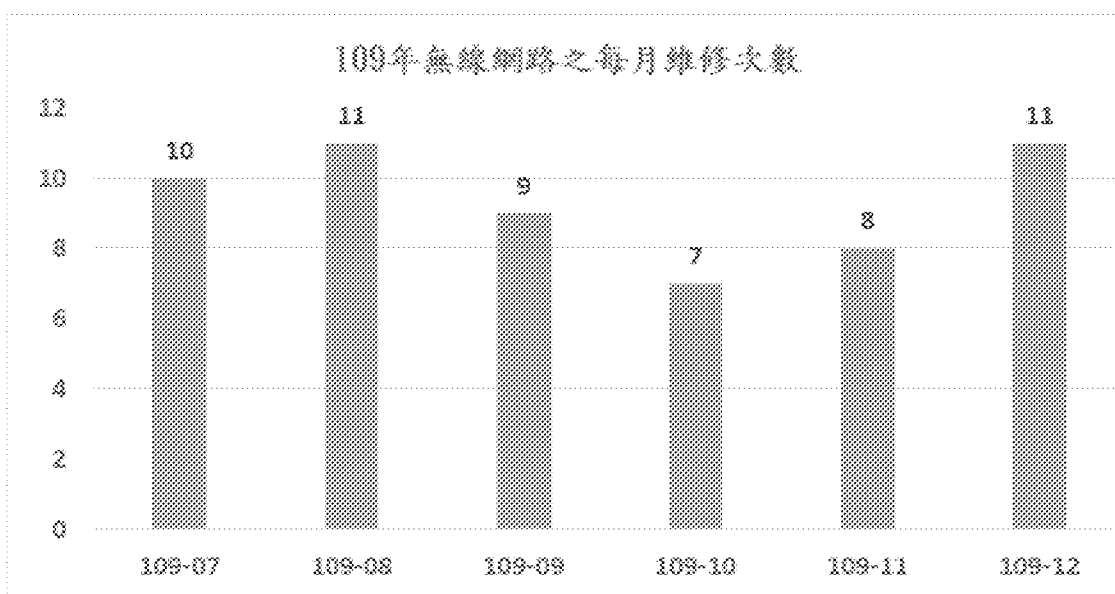


圖七、資安事件統計圖

- (四) 關於教育部函轉行政院 109 年 7 月 27 日與 109 年 12 月 18 日兩份函文提及採購限制並要求 110 年底前汰除全機關中國大陸製及中國廠商資通訊產品一案，目前正與總務處經管組、事務組討論因應措施；另於 110 年 1 月 8 日收到行政院電子郵件回覆未來將會要求源頭控管措施，教師亦在管控範圍內，計網中心將針對上述資通訊設備評估相關配套管理辦法，以避免政令衝擊。
- (五) 原 109 年配合資通安全管理法要求之教學與行政網段重新調整作業，因疫情與 109 年 12 月教育部資通安全稽核訪視作業，改為 110 年規劃進行。
- (六) 依據教育部 109 年 12 月資通安全稽核結果報告之三十餘項缺失，將協同系統組針對管理面、政策面與技術面進行矯正及預防作業，並於 110 年研擬配套後逐步施行，且依缺失改善建議進行資安控管。此外，未來各系所、單位與計劃自建之系統平台如未能遵照教育部要求之資通安全管理法規進行 ISMS 導入與 ISO27001 認證者，可依本中心相關資安規範落實資訊系統向上集中。
- (七) 為配合資通安全管理法要求之委外標準作業程序規範，109 年下半年已強制落實委外系統維運 VPN 帳號申請及防火牆開通作

業，以免不合規之廠商承攬本校資通訊產品(含軟體、硬體及服務)，減少本校教職員工暴露於可能違反資通安全管理法遭懲處之風險。

- (八) 109 年 7 月至 12 月接獲多起校內資安通報，正陸續修補校內系統資安漏洞；將依據資通安全管理法研擬本校內部資安通報漏洞規範，用以要求具有一定技術能力之教職員工生依循其規定，進行良性測試與通報作業。避免因測試系統漏洞造成資料損毀、外洩等情事，影響其他教職員工生權益，並給予通報者獎勵，藉以建立正向循環。
- (九) 109 年 7 月 完成 aruba controller 7240 及 77 台 AP 採購，對化工館及共科館無線網路基地台汰換升級。
- (十) 109 年 10 月完成無線網路骨幹頻寬管理設備採購及上線，每人每日無線網路總流量為 10GB。
- (十一) 109 年 11 月完成化學館及生技館網路重整作業。
- (十二) 109 年 11 月完成智慧型流量管理平台擴充、APT 進階持續性防護系統、個人資料洩漏防護系統及委外廠商遠端桌面連線側錄系統。
- (十三) 109 年無線網路 7-12 月各單位維護統計表(詳如圖八、表十)，以作為未來基地台汰換評估之依據。



圖八、無線網路 109 年 7 至 12 月報修次數統計圖

表十、無線網路各單位報修次數統計表

單位	件數	單位	件數	單位	件數	單位	件數

教務處	2	產學合作處	1	機電學院	1	管理學院	2
學務處	6	人事室	2	電資學院	3	設計學院	4
總務處	9	計網中心	1	工程學院	8	人文學院	12
研發處	1					其他 (未註明)	4
總計	56 件						

## 二、進行中項目：

- (一) 聯外線路負載平衡路由器汰換作業，分流及平衡多路網路線路，預計 110 年 5 月完成。
- (二) 於精勤樓建置第三座資訊節能機房，預計 110 年 5 月完成。
- (三) 綜科館無線網路基地台汰換作業，提升無線網路品質及覆蓋率，預計 110 年 7 月完成。

## ※系統組：

### 一、已完成項目：

- (一) 109 年 7 月完成二場 RPAGE 網站平台教育訓練，共計 84 人參加。
- (二) 「北科 i 學園」已於 109 年 8 月 31 日停止服務，109 年 9 月完成教務處「北科 i 學園 PLUS」版本更新，變更介接全都錄影片同步及 MP4 播放器功能。
- (三) 109 年 8 月完成國際事務處「國際生學費信用卡繳費系統」上線。
- (四) 為遵循本校資安政策，「電子公文系統」、「學校網頁系統」、「校園入口網站」於 109 年 8 月完成業務持運作演練，109 年 10 至 11 月完成使用者帳號權限清查作業。
- (五) 109 年 9 月完成「109 年校慶網站」改版，更新版面及相關資料。
- (六) 109 年 9 月及 12 月完成人事室「差勤系統」版本更新，變更漏未刷卡(不含假日)，以及修正勞基法特休計算公式、公務員特休必修天數等功能。
- (七) 109 年 7 月及 9 月完成「學校網頁系統」版本更新，擴增發佈資訊可設定起迄時間，以及帳號及密碼複雜度政策由計中統一管理等功能。
- (八) 109 年 11 月完成總務處「電子公文系統」版本更新，變更彙併辦追加檢核機制、調整公文移交介面，以及修正公告名稱問題、展期天數檢核等功能。

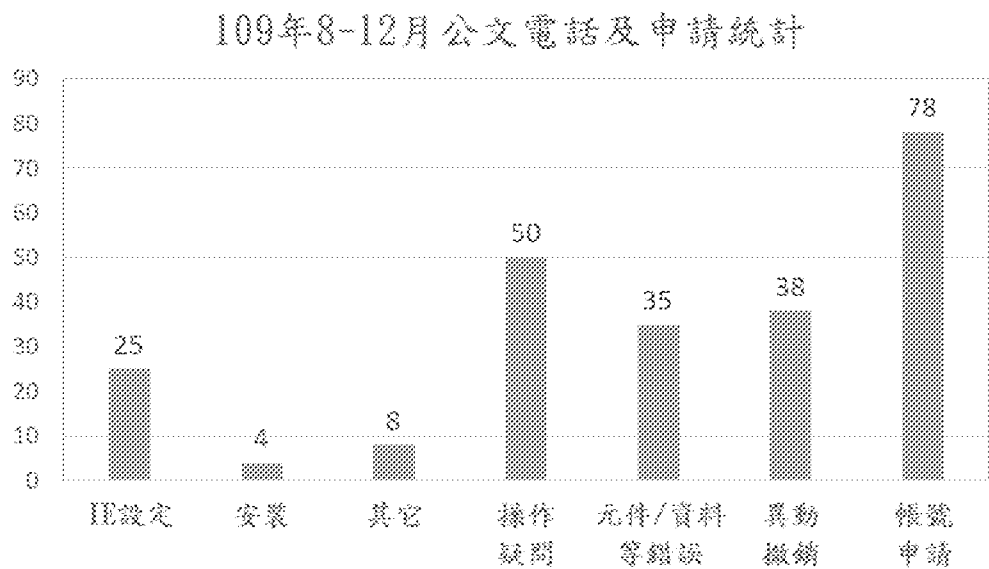
- (九)109年11月完成研發處「畢業生流向問卷調查系統」改版，擴增問卷題目以及介面優化。
- (十)109年12月完成教務處「碩士一般招生系統」改版及相關作業。
- (十一)109年12月完成「資安健診」檢測作業，針對計網中心資訊設備進行，檢測項目有：網路架構檢視、有線網路惡意活動檢視、使用者端電腦檢視、伺服器主機檢視及安全設定檢視。
- (十二)109年12月完成教育部對本校全機關進行實地資通安全稽核作業，12月8至9日主要進行技術檢測，12月23日主要進行策略面、管理面與技術面稽核。後續將針對教育所提供報告進行檢討並強化本校資安方向，有關技術檢測抽檢結果如下：
1. 使用者電腦安全檢測
    - 弱點掃描檢測 50 台使用者電腦，發現：8 個高風險弱點、104 個中風險弱點。
    - 抽查其中 5 台電腦，其中 1 台發現疑似惡意程式。
  2. 網路惡意活動檢測：依行政院技服中心於 109 年 12 月 2 日提供的惡意中繼站名單檢測，合計 477 筆資料中有 133 筆未成功阻擋，阻擋率約 72%。
  3. 核心資通系統安全檢測：核心系統有 2 項中風險及 1 項低風險弱點，2 項防護基準控制措施未符合。
  4. 網路架構檢測：共發現 1 個中風險弱點、1 個建議風險弱點。
  5. 目錄伺服器安全檢測：抽驗網域主機 2 項不符合單位規定。
  6. 物聯網設備安全檢測：抽驗 9 台印表機、1 台網路攝影機、2 台環控系統及 2 台無線網路基台進行檢核，共發現 14 個高風險。
  7. 組態設定安全檢測：抽檢 1 台使用者電腦與 2 台伺服器，共檢核 1965 項組態設定，其中 1104 項未符合政府組態要求，設定率為 44%。
- (十三)109年9至12月協助秘書室完成109年下半年度「全國技專校院校務基本資料庫」填報與修正相關作業，進行匯出資料光碟供秘書室報部。
- (十四)109年8至12月協助行政單位「委外資訊系統建置需求標準作業流程」已完成審核共計17件(詳如表十一)，尚在審核中共計8件。

表十一、委外資訊系統建置需求標準作業流程審核統計表

單位	已完成件數	單位	審核中件數
計網中心	6	總務處	3
圖資處	5	計網中心	1

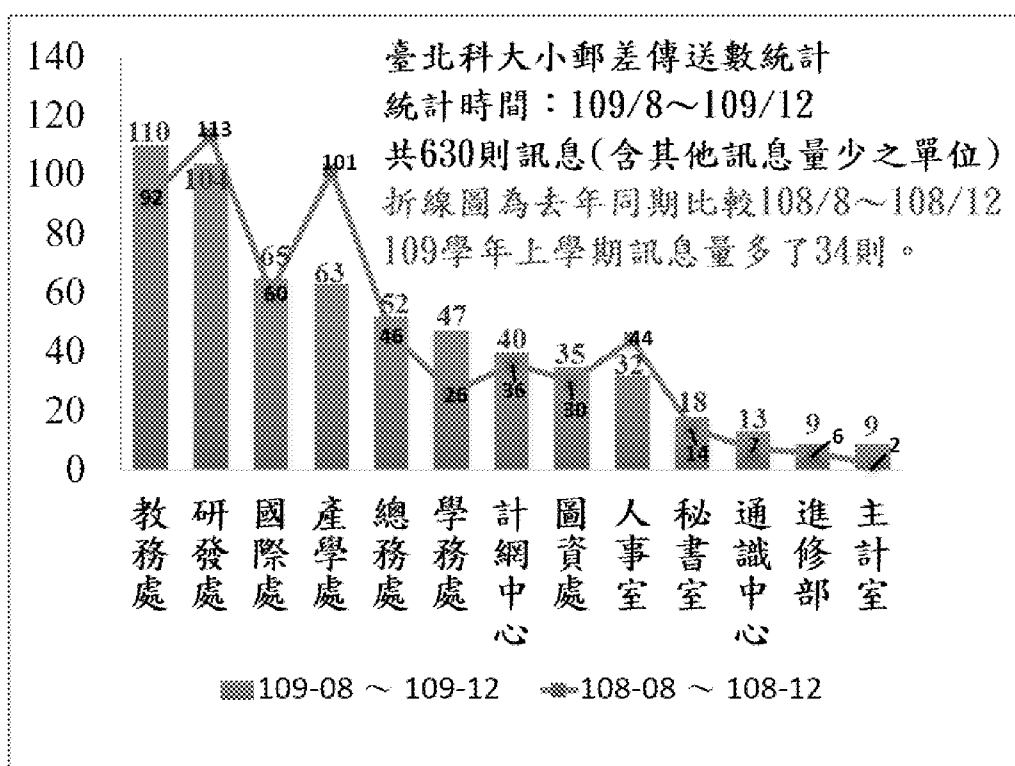
總務處	3	教務處	1
教務處	1	秘書室	1
產學處	1	主計室	1
學務處	1	人事室	1
總計	17	總計	8

(十五) 109年8至12月「電子公文系統」電話及申請處理件數 IE 設定 25 件、安裝 4 件、其它 8 件、操作疑問 50 件、元件/資料等錯誤 35 件、異動撤銷 38 件、帳號申請 78 件，共計 238 件(詳如圖九)。



圖九、公文系統處理件數統計

(十六) 109年8至12月「臺北科大小郵差」傳遞發佈訊息數共計 630 則(詳如圖十)。



圖十、單位公務訊息傳遞統計圖

## 二、進行中項目：

- (一) 為防疫需求及維護學生個資之正確性，擴增學生登入「校園入口網站」定時(每年)驗證學生行動電話功能，作為學校緊急且重要訊息通知之用途，預計 110 年 1 月 18 日上線。
- (二) 計網中心 ISO 27001「資訊安全管理制度」內部稽核已於 109 年 12 月 28 日完成，BSI 國際資安標準外部稽核預訂於 110 年 1 月 22 日辦理。
- (三) 因應 IE 瀏覽器停止運作前置作業，協助總務處「電子公文系統」新版規畫，以期改善使用者操作及配合資訊安全政策，預計 110 年 1 月底完成採購。
- (四) 協助人事室規畫差勤簽到退刷卡機制，以人事資料、卡務系統與校園 Web 門禁平台整合完成的架構為基礎，配合採購刷卡及攝影設備，已進行刷卡紀錄同步差勤資料庫介接，預計 110 年 2 月 1 日完成上線。
- (五) 為彙整校內各項活動、講演、競賽等資訊，統一於單一平台呈現「學校網頁系統」擴增校園活動報名功能，預計 110 年 3 月底完成。

## ※校務資訊組：

## 一、已完成項目：

- (一) 教務處「學籍系統」、「新生電子大頭照上傳系統」、「英文畢業門檻考試報名系統」、「網路加退選系統」、「新生資料網頁」、



- 「碩士班甄試入學招生系統」、「排課系統」、「視教中心資訊系統」、「學生查詢 RWD 系統」、「選課系統」、「線上成績單申請系統」、「開課系統」與「成績系統」功能擴增或變更，於 109.06.24~109.12.28 完成。
- (二) 教務處「教師評鑑系統」106-108 教師評鑑統計資料，於 109.11.20 完成。
- (三) 教務處「110 碩甄招生」總成績製作及 E-mail 通知，於 109.12.02 完成。
- (四) 教務處「註冊編班查詢系統」與「學籍系統」權限異動，於 109.11.23~109.12.09 完成。
- (五) 學務處「學生每日防疫日誌系統」、「學生請假系統」與「校園健康管理系統」功能擴增或變更，於 109.06.17~109.12.30 完成。
- (六) 學務處「學生請假系統」、「導師教職員查詢專區」與「校園健康管理系統」權限異動，於 109.07.07~109.12.09 完成。
- (七) 學輔中心「預約諮商系統」功能擴增，於 109.12.31 完成。
- (八) 總務處「線上繳費系統」功能擴增，於 109.12.07 完成。
- (九) 研發處「產學合作系統-專利技轉」、「產學合作系統-技術移轉」與「校外實習系統」功能擴增或變更，於 109.09.14~109.11.10 完成。
- (十) 產學合作處「產學合作系統」與「教師評鑑系統」功能擴增或變更，於 109.11.01~109.12.24 完成。
- (十一) 聯合服務中心「聯合服務中心系統」權限異動，於 109.07.16 完成。
- (十二) 人事室「教師升等作業系統」功能擴增，於 109.12.24 完成。
- (十三) 進修部「110 學年度管理學院 EMBA 專班招生報名系統」與「110 學年度碩士在職專班招生報名系統」功能變更，於 109.11.26~109.12.09 完成。
- (十四) 推廣教育中心「推廣教育系統」功能擴增，於 110.01.05 完成。
- (十五) 新北市「高中職校務行政系統」：  
「成績系統」、「學籍系統」、「重補修系統」、「學生成績查詢系統」、「班級幹部管理系統」、「出缺席系統」、「人事系統」、「配課系統」與「獎懲系統」功能擴增或變更，於 109.06.09~109.12.22 完成。
- (十六) 國教署校務行政系統「調代補課系統」新系統建置，於 109.07.14 完成。
- (十七) 國教署校務行政系統：  
「學生學習歷程系統」、「重補修系統」、「學籍系統」、「課務系統」、「出缺席系統」、「學務系統」、「調代課系統」

與「社團系統」功能擴增或變更，於 109.07.10~110.01.05 完成。

## 二、進行中項目：

- (一)教務處「畢業生離校系統」新系統建置，預計 110.02.22 完成。
- (二)教務處「網路加退選系統」功能擴增，預計 110.01.31 完成。
- (三)總務處「線上繳費系統」功能擴增，預計 110.01.31 完成。
- (四)人事室「校務人力管理系統」新系統建置，預計 110.02.22 完成。
- (五)聯合服務中心「聯合服務中心資訊系統」功能擴增，預計 110.02.01 完成。
- (六)國教署校務行政系統「自動排課系統」新系統建置，預計 110.02.22 完成。
- (七)國教署校務行政系統「成績系統」功能擴增，預計 110.02.22 完成。
- (八)逆向工程：(1)教務處「學生成績管理系統」；(2)學務處「學生獎懲及操行成績管理系統」；(3)教務處「教學評量管理系統」；(4)教務處「學生成績單自動列印系統」。

## 肆、提案討論

案由(一)	提案單位：計網中心系統組
提案主旨	本校「計算機與網路中心電腦帳號管理要點」第四點修正草案，提請討論。
說明	<p>一、依「資通安全責任等級分級辦法」第 11 條略以，各機關自行或委外開發之資通系統應依附表九所定資通系統防護需求分級原則完成資通系統分級，並依附表十所定資通系統防護基準執行控制措施。</p> <p>二、109 年 12 月教育部資通安全實地稽核報告，針對本校身分驗證管理有三項不符合資通系統防護基準控制措施。</p> <p>三、為遵循現行資訊安全規範擬修訂「計算機與網路中心電腦帳號管理要點」。</p>
討論資料	<p>一、「國立臺北科技大學計算機與網路中心電腦帳號管理要點」第四點修正草案對照表。(如附件 1)</p> <p>二、「國立臺北科技大學計算機與網路中心電腦帳號管理要點」修正草案。(如附件 2)</p> <p>三、資通系統防護基準。(如附件 3)</p>
辦法	通過後，提行政會議討論。
決議	照案通過。

伍、臨時動議

。

陸、散會。



## 國立臺北科技大學計算機與網路中心電腦帳號管理要點

### 第四點修正草案對照表

110年1月15日109學年度第1學期計算機與網路發展指導委員會議討論

修正條文	現行條文	說明
<p>四、管理規範：</p> <p>(一) 本中心對所提供之使用者帳號資料具有保密責任，任何未經正式申請及身份驗證之個人帳號查詢，本中心將不予處理。</p> <p>(二) 各單位主管基於需要瞭解與輔導使用者言論行為時，得向計算機與網路中心提出書面申請查詢使用者帳號資料，但查詢資料僅限於校園內合法使用。如查詢資料擬使用於校園外，申請書須經校長核可後交計算機與網路中心處理，並應遵守台灣學術網路連線單位相關法規。</p> <p>(三) 本中心基於維護校園網路安全，依規定得進入網路系統中監督與了解使用者的當時狀況。</p> <p>(四) 為維護電腦帳號安全，其密碼設定須符合下列規則：</p> <p>1、使用者應變更初始或預設密碼。</p> <p>2、密碼長度不可少於8個字元。</p> <p>3、密碼應具備複雜性，如大小寫英文字母、數字或符號構成。</p> <p>4、<u>密碼最長使用期限為180天，最短使用期限為1天。</u></p> <p>5、密碼不可與前3組重覆。</p> <p>6、<u>密碼驗證失敗達3次後，至少15分鐘內不允許該帳號繼續嘗試登入。</u></p>	<p>四、管理規範：</p> <p>(一) 本中心對所提供之使用者帳號資料具有保密責任，任何未經正式申請及身份驗證之個人帳號查詢，本中心將不予處理。</p> <p>(二) 各單位主管基於需要瞭解與輔導使用者言論行為時，得向計算機與網路中心提出書面申請查詢使用者帳號資料，但查詢資料僅限於校園內合法使用。如查詢資料擬使用於校園外，申請書須經校長核可後交計算機與網路中心處理，並應遵守台灣學術網路連線單位相關法規。</p> <p>(三) 本中心基於維護校園網路安全，依規定得進入網路系統中監督與了解使用者的當時狀況。</p> <p>(四) 為維護電腦帳號安全，其密碼設定須符合下列規則：</p> <p>1、使用者應變更初始或預設密碼。</p> <p>2、密碼長度不可少於8個字元。</p> <p>3、密碼應具備複雜性，如大小寫英文字母、數字或符號構成。</p> <p>4、應至少每180天變更乙次。</p> <p>5、密碼不可與前1組重覆。</p>	<p>一、依資通系統防護基準控制措施，身分驗證管理基於密碼之鑑別資通系統應強制最低密碼複雜度；強制密碼最短及最長之效期限制，故修正第(四)項第4點內容。</p> <p>二、依資通系統防護基準控制措施，身分驗證管理使用者更換密碼時，至少不可以與前三次使用過之密碼相同，故修正第(四)項第5點內容。</p> <p>三、依資通系統防護基準控制措施，身分驗證管理具備帳戶鎖定機制，帳號登入進行身分驗證失敗達3次後，至少15分鐘內不允許該帳號繼續嘗試登入或使用機關自建之失敗驗證機制，故新增第(四)項第6點內容。</p>



附件2

## 國立臺北科技大學計算機與網路中心電腦帳號管理要點 修正草案

86年11月19日計算機發展指導委員會會議通過  
86年12月2日行政會議通過  
88年12月28日計算機發展指導委員會會議修正通過  
89年1月11日行政會議修正通過  
89年1月8日計算機發展指導委員會會議修正通過  
90年4月30日行政會議修正通過  
93年3月2日行政會議修正通過  
96年7月3日行政會議修正通過  
98年2月10日行政會議修正通過  
98年8月4日行政會議修正通過  
100年2月22日擴大行政會議修正通過  
105年7月12日行政會議修正通過

### 一、目的：

計算機與網路中心(以下簡稱本中心)為提昇其正常使用功能及有效管理本校教職員工及學生之電腦帳號，特訂定電腦帳號管理要點(以下簡稱本要點)。

### 二、電腦帳號申請：

- (一)凡在本校當學年度註冊之學生(含復學生)，本中心將主動為之開設電子郵件及資訊系統帳號，合稱電腦帳號。
- (二)現職教職員工，皆可向本中心提出申請電腦帳號。
- (三)單位及社團電腦帳號申請比照教職員工，以建置網頁及校內信箱為主要用途，而帳號密碼由單位主管及社團負責人保管，並於卸任時隨職務交接。
- (四)專任教職員工得向本中心申請 Google 之「@mail.ntut.edu.tw」額外電子郵件帳號。
- (五)學生得向本中心申請 Google 之「@ntut.org.tw」額外電子郵件帳號。

### 三、密碼重設：

- (一)學生可持學生證、教職員工可持識別證至本中心，經電腦認證後自行重設密碼，或經由入口網站更改密碼。
- (二)無識別證之員工、主管公務帳號及社團帳號等，可填申請表交本中心重設密碼。
- (三)於本校退休之專任教職員工須持身分證明文件至本中心申請重設密碼。

### 四、管理規範：

- (一)本中心對所提供之使用者帳號資料具有保密責任，任何未經正式申請及身份驗證之個人帳號查詢，本中心將不予處理。
- (二)各單位主管基於需要瞭解與輔導使用者言論行為時，得向計算機與網路中心提出書面申請查詢使用者帳號資料，但查詢資料僅限於校園內合法使用。如查詢資料擬使用於校園外，申請書須經校長核可後交計算機與網路中心處理，並應遵守台灣學術網路連線單位相關法規。
- (三)本中心基於維護校園網路安全，依規定得進入網路系統中監督與了解使用者的當時狀況。
- (四)為維護電腦帳號安全，其密碼設定須符合下列規則：
  1. 使用者應變更初始或預設密碼。
  2. 密碼長度不可少於 8 個字元。
  3. 密碼應具備複雜性，如大小寫英文字母、數字或符號構成。
  4. 密碼最長使用期限為 180 天，最短使用期限為 1 天。
  5. 密碼不可與前 3 組重覆。
  6. 密碼驗證失敗達 3 次後，至少 15 分鐘內不允許該帳號繼續嘗試登入。

#### 五、使用規範：

- (一)使用者所公開發表之文章內容不得汙衊同仁、師長或同學，並應尊重他人權益及隱私，委婉用詞，避免造成誤解及糾紛。
- (二)禁止將個人帳號轉借他人使用或盜用他人之帳號。
- (三)禁止使用帳號散佈電腦病毒、嘗試侵入未經授權之電腦系統、干擾網路上其它使用者、破壞網路節點之軟硬體系統或其它類似之情形。
- (四)禁止使用帳號傳送具威脅性、猥褻性、攻擊性或商業性的文字、圖片或影音；禁止上述不當內容放置於個人帳號或任何伺服器上供他人瀏覽或擷取。
- (五)尊重智慧財產權，禁止複製或使用未經授權的軟體。

#### 六、罰則：

- (一)違反使用規範者，本中心立即暫停該帳號之使用權，並視情節輕重給予停權一星期至一學期。情節重大者，除停權外，在學學生部份，送請學生事務處議處；現職教職員工部份，送請考績委員會或教師評審委員會處理；畢業學生及退休專任教職員工部份，本中心得立即停止該帳號之使用權。
- (二)違反使用規範或其他未載明之規定而觸犯法律者，須自負法

律責任。

- (三)違反使用規範而受停權處分者，如對處分不服，得於受停權處分有效日起二星期內向本中心提出書面申訴，逾期未提出申訴者，視為對處分結果無異議。申訴以一次為限。

#### 七、使用期限：

- (一)學生退學，本中心得依教務資料逕行停用資訊系統帳號和校內電子郵件帳號；學生畢業、休學，得保留至次學期(6月30日或12月31日)後停用資訊系統帳號，並保留校內電子郵件帳號三年。
- (二)職員工離職，本中心得依人事資料逕行停用資訊系統帳號，並保留校內及 Google 電子郵件帳號三個月。
- (三)專任教師離職，本中心得依人事資料逕行停用資訊系統帳號，並保留校內及 Google 電子郵件帳號三年。
- (四)兼任教師逾二年未續聘，本中心得逕行停用資訊系統帳號，並保留校內及 Google 電子郵件帳號一年。
- (五)教職員工退休，本中心得逕行停用資訊系統帳號，永久保留電子郵件帳號，本中心於教職員工退休後三年，每年寄送一次電子郵件帳號續用意願調查函給退休教職員工，凡未於兩個月內回覆者，本中心得逕行停止該帳號之使用權。

#### 八、單位伺服器電腦帳號：

各單位經本中心核可之 DNS 伺服器得為本校教職員工生開設電腦帳號，其相關管理與使用規範亦應參照本要點辦理。

#### 九、本要點經計算機發展指導委員會及行政會議通過後實施，修正時亦同。



附表十 資通系統防護基準

系統防護需求 分級		高	中	普
控制措施				
構面	措施內容			
存取控制	帳號管理	一、逾越機關所定預期閒置時間或可使用期限時，系統應自動將使用者登出。 二、應依機關規定之情況及條件，使用資通系統。 三、監控資通系統帳號，如發現帳號違常使用時回報管理者。 四、等級「中」之所有控制措施。	一、已逾期之臨時或緊急帳號應刪除或禁用。 二、資通系統閒置帳號應禁用。 三、定期審核資通系統帳號之建立、修改、啟用、禁用及刪除。 四、等級「普」之所有控制措施。	建立帳號管理機制，包含帳號之申請、開通、停用及刪除之程序。
	最小權限	採最小權限原則，僅允許使用者（或代表使用者行為之程序）依機關任務及業務功能，完成指派任務所需之授權存取。		無要求。
	遠端存取	一、應監控資通系統遠端連線。 二、資通系統應採用加密機制。 三、資通系統遠端存取之來源應為機關已預先定義及管理之存取控制點。 四、等級「普」之所有控制措施。		對於每一種允許之遠端存取類型，均應先取得授權，建立使用限制、組態需求、連線需求及文件化，使用者之權限檢查作業應於伺服器端完成。
稽核與可歸責性	稽核事件	一、應定期審查稽核事件。 二、等級「普」之所有控制措施。		一、依規定時間週期及紀錄留存政策，保留稽核紀錄。 二、確保資通系統有稽核特定事件之功能，並決定應稽核之特定資通系統事件。 三、應稽核資通系統管理者帳號所執行之各項功能。
	稽核紀錄內容	一、資通系統產生之稽核紀錄，應依需求納入其他相關資訊。 二、等級「普」之所有控制措施。		資通系統產生之稽核紀錄應包含事件類型、發生時間、發生位置及任何與事件相關之使用者身分





			識別等資訊，並採用單一日誌紀錄機制，確保輸出格式之一致性。	
稽核儲存容量	依據稽核紀錄儲存需求，配置稽核紀錄所需之儲存容量。			
稽核處理失效之回應	一、機關規定需要即時通報之稽核失效事件發生時，資通系統應於機關規定之時效內，對特定人員提出警告。 二、等級「中」及「普」之所有控制措施。	資通系統於稽核處理失效時，應採取適當之行動。		
時戳及校時	一、系統內部時鐘應依機關規定之時間週期與基準時間源進行同步。 二、等級「普」之所有控制措施。	資通系統應使用系統內部時鐘產生稽核紀錄所需時戳，並可以對應到世界協調時間(UTC)或格林威治標準時間(GMT)。		
稽核資訊之保護	一、定期備份稽核紀錄至與原稽核系統不同之實體系統。 二、等級「中」之所有控制措施。	一、應運用雜湊或其他適當方式之完整性確保機制。 二、等級「普」之所有控制措施。	對稽核紀錄之存取管理，僅限於有權限之使用者。	
營運持續計畫	系統備份	一、應將備份還原，作為營運持續計畫測試之一部分。 二、應在與運作系統不同處之獨立設施或防火櫃中，儲存重要資通系統軟體與其他安全相關資訊之備份。 三、等級「中」之所有控制措施。	一、應定期測試備份資訊，以驗證備份媒體之可靠性及資訊之完整性。 二、等級「普」之所有控制措施。	一、訂定系統可容忍資料損失之時間要求。 二、執行系統源碼與資料備份。
	系統備援	一、訂定資通系統從中斷後至重新恢復服務之可容忍時間要求。 二、原服務中斷時，於可容忍時間內，由備援設備取代提供服務。	無要求。	
識別與鑑別	內部使用者之識別與鑑別	一、對帳號之網路或本機存取採取多重認證技術。 二、等級「中」及「普」之所有控制措施。	資通系統應具備唯一識別及鑑別機關使用者(或代表機關使用者行為之程序)之功能，禁止使用共用帳號。	

	身分驗證管理	<p>一、身分驗證機制應防範自動化程式之登入或密碼更換嘗試。</p> <p>二、密碼重設機制對使用者重新身分確認後，發送一次性及具有時效性符記。</p> <p>三、等級「普」之所有控制措施。</p>	<p>一、使用預設密碼登入系統時，應於登入後要求立即變更。</p> <p>二、身分驗證相關資訊不以明文傳輸。</p> <p>三、具備帳戶鎖定機制，帳號登入進行身分驗證失敗達三次後，至少十五分鐘內不允許該帳號繼續嘗試登入或使用機關自建之失敗驗證機制。</p> <p>四、基於密碼之鑑別資通系統應強制最低密碼複雜度；強制密碼最短及最長之效期限制。</p> <p>五、使用者更換密碼時，至少不可以與前三次使用過之密碼相同。</p> <p>六、第四點及第五點所定措施，對非內部使用者，可依機關自行規範辦理。</p>
	鑑別資訊回饋	資通系統應遮蔽鑑別過程中之資訊。	
	加密模組鑑別	資通系統如以密碼進行鑑別時，該密碼應加密或經雜湊處理後儲存。	無要求。
	非內部使用者之識別與鑑別	資通系統應識別及鑑別非機關使用者(或代表機關使用者行為之程序)。	
系統與服務獲得	系統發展生命週期需求階段	針對系統安全需求(含機密性、可用性、完整性)，以檢核表方式進行確認。	
	系統發展生命週期設計階段	<p>一、根據系統功能與要求，識別可能影響系統之威脅，進行風險分析及評估。</p> <p>二、將風險評估結果回饋需求階段之檢核項目，並提出安全需求修正。</p>	無要求。

	系統發展生命週期開發階段	<ul style="list-style-type: none"> <li>一、執行「源碼掃描」安全檢測。</li> <li>二、具備系統嚴重錯誤之通知機制。</li> <li>三、等級「中」及「普」之所有控制措施。</li> </ul>	<ul style="list-style-type: none"> <li>一、應針對安全需求實作必要控制措施。</li> <li>二、應注意避免軟體常見漏洞及實作必要控制措施。</li> <li>三、發生錯誤時，使用者頁面僅顯示簡短錯誤訊息及代碼，不包含詳細之錯誤訊息。</li> </ul>	
	系統發展生命週期測試階段	<ul style="list-style-type: none"> <li>一、執行「滲透測試」安全檢測。</li> <li>二、等級「中」及「普」之所有控制措施。</li> </ul>	執行「弱點掃描」安全檢測。	
	系統發展生命週期部署與維運階段	<ul style="list-style-type: none"> <li>一、於系統發展生命週期之維運階段，須注意版本控制與變更管理。</li> <li>二、等級「普」之所有控制措施。</li> </ul>	<ul style="list-style-type: none"> <li>一、於部署環境中應針對相關資通安全威脅，進行更新與修補，並關閉不必要服務及埠口。</li> <li>二、資通系統相關軟體，不使用預設密碼。</li> </ul>	
	系統發展生命週期委外階段	資通系統開發如委外辦理，應將系統發展生命週期各階段依等級將安全需求（含機密性、可用性、完整性）納入委外契約。		
	獲得程序	開發、測試及正式作業環境應為區隔。	無要求。	
	系統文件	應儲存與管理系統發展生命週期之相關文件。		
系統與通訊保護	傳輸之機密性與完整性	<ul style="list-style-type: none"> <li>一、資通系統應採用加密機制，以防止未授權之資訊揭露或偵測資訊之變更。但傳輸過程中有替代之實體保護措施者，不在此限。</li> <li>二、使用公開、國際機構驗證且未遭破解之演算法。</li> <li>三、支援演算法最大長度金鑰。</li> <li>四、加密金鑰或憑證週期性更換。</li> <li>五、伺服器端之金鑰保管應訂定管理規範及實施應有之安全防护措施。</li> </ul>	無要求。	無要求。

	資料儲存之安全	靜置資訊及相關具保護需求之機密資訊應加密儲存。	無要求。	無要求。
系統與資訊完整性	漏洞修復	一、定期確認資通系統相關漏洞修復之狀態。 二、等級「普」之所有控制措施。		系統之漏洞修復應測試有效性及潛在影響，並定期更新。
	資通系統監控	一、資通系統應採用自動化工具監控進出之通信流量，並於發現不尋常或未授權之活動時，針對該事件進行分析。 二、等級「中」之所有控制措施。	一、監控資通系統，以偵測攻擊與未授權之連線，並識別資通系統之未授權使用。 二、等級「普」之所有控制措施。	發現資通系統有被入侵跡象時，應通報機關特定人員。
	軟體及資訊完整性	一、應定期執行軟體與資訊完整性檢查。 二、等級「中」之所有控制措施。	一、使用完整性驗證工具，以偵測未授權變更特定軟體及資訊。 二、使用者輸入資料合法性檢查應置放於應用系統伺服器端。 三、發現違反完整性時，資通系統應實施機關指定之安全保護措施。	無要求。

備註：

- 一、靜置資訊，指資訊位於資通系統特定元件，例如儲存設備上之狀態，或與系統相關需要保護之資訊，例如設定防火牆、閘道器、入侵偵測、防禦系統、過濾式路由器及鑑別符內容等資訊。
- 二、特定非公務機關之中央目的事業主管機關得視實際需求，於符合本辦法規定之範圍內，另行訂定其所管特定非公務機關之系統防護基準。

