110年度網管暨資通安全教育訓練及系統向上集中說明會

計網中心
主講人 網路作業組 陳志豪技術員
委外SOP主講人 系統組 林建成技術員
110/03/05 1400

議程1-資訊安全相關政策宣導與說明

- 公務機關使用資通訊產品(含軟體、硬體及服務)相關原則
- 總務處全校性IoT設備IP調整說明
- 委外廠商管理說明
- 委外SOP管理說明
- 委外廠商VPN連線說明
- 中國大陸廠商或生產之設備、服務採購(配套)說明
- 個資洩漏問題(協助秘書室宣導)
- 社交工程電子郵件
- 防火牆相關C3-1/C3-2表格說明

議程2-學術單位行政體系IP調整說明

- IP分配政策調整預告
- 學術單位IP調整說明

議程3-資訊系統向上集中說明

- 資安稽核結果說明
- 資訊系統向上集中原則
- 資訊系統向上集中方式
- 資訊系統向上集中管理方式
- 資訊系統自行管理原則

議程4-防火牆防護提升說明

- 外對內防火牆防護措施提升
- 校內網段間納入資安防護措施

本次會議重點

- 為配合資通安全管理法相關措施，
  要求範圍為「全機關」
- 相關政策將會向教育部及行政院確認並討論配套措施因應施行
- 因本校承辦大量獎補助及行政委託計畫，
  相關政策將盡可能與教育部同步，減少重複性作業、保有一致性使行政作業盡可能減免
- 為保護本校教職員工避免遭到法規稽核缺失導致違法事實遭懲處
- 避免事件發生後主管機關列管追查或檢調單位查扣相關設備影響業務運作

相關措施之依據

- 資通安全管理法
- 「109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」缺失、要求及建議
- 教育部針對本校承辦之”教育部核心系統”及”資訊系統安全等級”中級以上稽核之要求改善與建議措施

議程1：資訊安全相關政策宣導與說明

公務機關使用資通訊產品(含軟體、硬體及服務)相關原則

- (一)公務用之資通設備不得使用中國大陸廠牌，且不得安裝非公務用軟體。
- (二)個人資通設備不得處理公務事務，亦不得與公務環境介接。
- (三)各機關應就已使用或採購之中國大陸廠牌資通訊設備列冊管理，且不得與公務環境介接，並於110年底汰換。
- 請務必留意避免觸法。

總務處全校性IoT設備IP調整說明

- 配合法令法規要求有效管理IoT設備
- 避免全校性設備占用系所IP，增加系所可用IP數量。
- 各系所IoT設備仍為各系所自行管理
- 有關IoT設備(如印表機、監視器、門禁...等)，該設備綁定之IP或要綁定電子郵件等帳號，請綁定設備管理人員，不得使用公(共)用帳號。

- IoT定義：非個人電腦、筆電或伺服器等具有聯網功能之設備

委外廠商管理說明

- 為避免教職員工承擔違反法規風險，相關法律責任與風險應轉嫁於廠商。
- 配合法令法規要求，
  購置資通電訊產品(軟體、硬體與服務)
  應依據本中心(委外資訊系統建置需求標準作業流程)
- 委外廠商未申請前無法以遠端管理通訊協定(如RDP、SSH等)相關協定連入本校。

委外SOP管理說明

- 適用單位：
  - 行政單位、教學單位行政體系(強制要求)
  - 教學單位(政府獎補助或委託之計畫)(預計強制要求)
  - 教學單位(可參考項目評估要求廠商)

- 適用範圍：
  - 全校委外資通電訊產品(軟體、硬體與服務)

委外SOP管理說明-流程說明

- 有關SOP流程詳細說明可參閱 https://cnc.ntut.edu.tw/p/404-1004-106974.php?Lang=zh-tw

委外SOP審查說明

- 委外SOP審查方式
  - 系統組(針對ISMS管理程序相關條文進行審查)
  - 校務資訊組(針對系統開發相關管理程序進行審查)
  - 行政組(針對授權軟體有關事項進行審查)
  - 網路組(針對資通安全防護與網路管理進行審查)
- 為確保委外合約能遵循法規而降低資安風險，第一次審核，單位請以計中審核結果之建議要求廠商改善合約內容。第二次審核，若仍有未符合之檢核重點，將視為單位願意負責承擔未符合法規之風險，以最後審核結果列印紙本，請承辦人及主管核章送計網中心核章確認結案。

委外廠商遠端連線說明

- 依據教育部稽核與ISO27001稽核委員建議，委外廠商應有操作稽核軌跡。
- 預計110年第一季全面導入遠端廠商連線控管機制。
- 系統將會側錄監控封包行為、資料流、螢幕操作與鍵盤輸入等。

- 委外系統維運人員VPN帳號申請/清查

中國大陸廠商或生產之設備、服務採購(配套)說明

- 依據教育部轉行政院函
  公務機關涉及個資或業務機敏感資料不得使用或採購中國廠牌及中國製造資通電訊產品。
- 現有設備除有具體風險或遭主管機關查核確認有風險者則先不汰換。
- 新購置之設備則依據規範不得採購。
- 中國廠牌之製品請於110年底前完成報廢程序

- 有關本校採購或使用資通訊產品(軟體、硬體及服務)為中國大陸品牌或製品注意事項

個資洩漏問題(協助秘書室宣導)

- 109年發生單位個資外洩事件
  - 某單位誤將成績單資料放置官網公告卻未將無關之身分證等個資刪除。
  - 某單位將存有個資之資料放置於校外網站平台上，因合約到期但無法將網站存放之個資刪除導致個資外洩情況。

- 個資保護注意事項請務必參閱秘書室個人資料保護專區

社交工程電子郵件

- 近年來社交工程郵件日新月異，去年因遭社交工程郵件釣魚導致公務帳號密碼外洩事件層出不窮
  - 109年發生有同仁收到主管信箱發出之業務信件(但實際非由主管自己寄出)
  - 教育部通報有教職員工生帳號密碼存在暗網
- 公務帳號使用之密碼避免用於校外私人帳號或因公務註冊之網站

防火牆相關C3-1表格說明

- 申請表填寫時機：
  - 需申請C3-2防火牆服務埠新增異動申請表
  - 依需求須請計網中心協助弱點掃描

機密等級：□機密■敏感□一般
109.12.25

國立臺北科技大學計算機與網路中心

防火牆申請前置作業-主機網站弱點掃描申請表

填表日期：　年　月　日

單位		員工編號	
申請人姓名		職稱	
連絡電話(分機)		電子郵件	@ntut.edu.tw

申請主機資訊

主機 IP：(範例：140.124.13.1)　　主機類型：□網站□資料庫□其他：

主機用途詳細說明：　　網站路徑：

單一主機若有多網站，請全部填寫，
防火牆將依送測之網址/路徑進行設定與開放

備註說明：

(範例：www.ntut.edu.tw/)

(範例：www.ntut.edu.tw/home/)

(範例：www.ntut.edu.tw/admin/)

申請次數	申請人簽章	單位主管職章 必須使用職章不得簽名	掃描結果(風險)	掃描結果(是否通過)
第一次			高：___中：___	□是 □否 □有條件通過
第二次			高：___中：___	□是 □否 □有條件通過
第三次			高：___中：___	□是 □否 □有條件通過

請詳讀並務必遵守下列規範與注意事項：

1. 本表格不得任意變更塗改文字、欄位或表格字型，但可調整申請用途表格高度以保持本表為單頁，各項表格文字不得跨頁，各欄位若填寫空間不足，請另以附件方式說明，並**請務必使用最新版本**

防火牆相關C3-2表格說明

- 申請表填寫時機：
  - 管制網段之主機須開放外部連入時

機密等級：□機密■敏感□一般
109.12.31

國立臺北科技大學計算機與網路中心

防火牆服務埠新增/異動 申請表

填表日期：　年　月　日　　申請編號：AFWR

單位		員工編號	
姓名		職稱	
連絡電話(分機)		電子郵件	@ntut.edu.tw
來源 (IP 或國家)	請詳閱申請用途 第二點後再填寫	申請之 服務埠與協定	□開放 □封鎖 格式：Port(Protocol)
目的 (IP 或國家)	若超過一個 IP 請參閱 申請用途第二點後再填寫	使用期間	核准日起 至 (年) / (月)
證明文件	教職員工請浮貼教職員證影印本或附本學年度聘書影印本。相關證明文件短缺將不予受理。 注意：申請人必須為 IP 登記使用人相同 (若該 IP 登記人為學生，請以指導教授/導師身分申請)。		申請人簽章 單位主管職章 必須使用職章不得簽名
申請用途	(填寫時請務必將本申請單紅字內容詳讀後刪除，且使用電腦繕打詳述申請用途，不得手寫) 一、依據本校 ISMS 管理規範，防火牆規則每年需進行盤點，申請期限至多一年。 二、填寫來源若非針對特定 IP 開放請填寫台灣，若須開放全球請詳述原因。 三、同一申請人若申請多 IP 時，可於本處或以附件方式分別註明各 IP 之用途與說明，以節省紙張之使用，避免表格變形。		

請詳讀並務必遵守下列規範與注意事項：

1. 本表格不得任意變更塗改文字、欄位或表格字型，但可調整申請用途表格高度以保持本表為

議程1
Q&A

學術單位行政體系IP調整說明

TAIPEI TECH Since 1912 國立臺北科技大學 National Taipei University of Technology

IP分配政策調整預告

- 起因與解決方案
  - 因應部分系所反應系上IP數量不足
    - 將行政體系與教學體系進行區分，將公務或公共環境空間使用之IP回歸教學使用
  - IP順號調整，需要緩衝IP方才能進行
    - 未來教師最多配發10(5)個IP、學生最多5(3)個IP，IP回歸使用者面登記，網管分層分權，避免濫發浪費(網管不會有數量限制)
    - 系統自動註銷半年未使用之IP釋放閒置IP
  - 網管將IP設定到其他網管身上
    - 避免此一狀況，未來系統會限制具有網管身份之帳號除自己本身不能夠由其他人設定IP分配
- 透過上述措施活化IP，增加可用IP數量

學術單位IP調整說明

- 學術單位分為三個方向進行IP重新調整
  - 行政體系(院/系/所辦公室、非教學用之空間與設備)
  - 教學體系(教師)
  - 教學體系(學生、一般教室與電腦教室)

- 將IP釋放給教學環境使用，提升IP整頓效率與彈性
- 符合法規並為教學單位解套：
  公務機關使用資通訊產品(含軟體、硬體及服務)相關原則

學術單位IP調整說明-行政體系

- 行政體系之院系所
  - 辦公室
  - 職員研究室/休息室
  - 公務使用之空間(會議室、系上演講廳等)
  - 系所自行建置之環控、監視器、門禁...等
  - (會議現場補充遺漏之範圍)

- 不含教職員管理之教學空間(電腦教室、一般教室等)
- 總務處演講廳等公共空間將另配發IP，不在此範圍內

學術單位IP調整說明-行政體系

- 行政體系IP重新挑整
  - 網段以院為單位，各院/系/所仍為自己網段之一階網管
  - 例如以電資學院為例(以下為舉例非實際狀況)
    - 院辦：140.124.110.1-50
    - 電機系：140.124.110.51-249、140.124.111.1-100
    - 電子系：140.124.111.101-249
- 故IP盤點非常重要，影響未來IP所配發之數量範圍
- 計網中心仍會保留彈性空間供未來擴充IP之用，避免全面重新調整，但勿浮報盤點IP總數

學術單位IP調整說明-教學體系

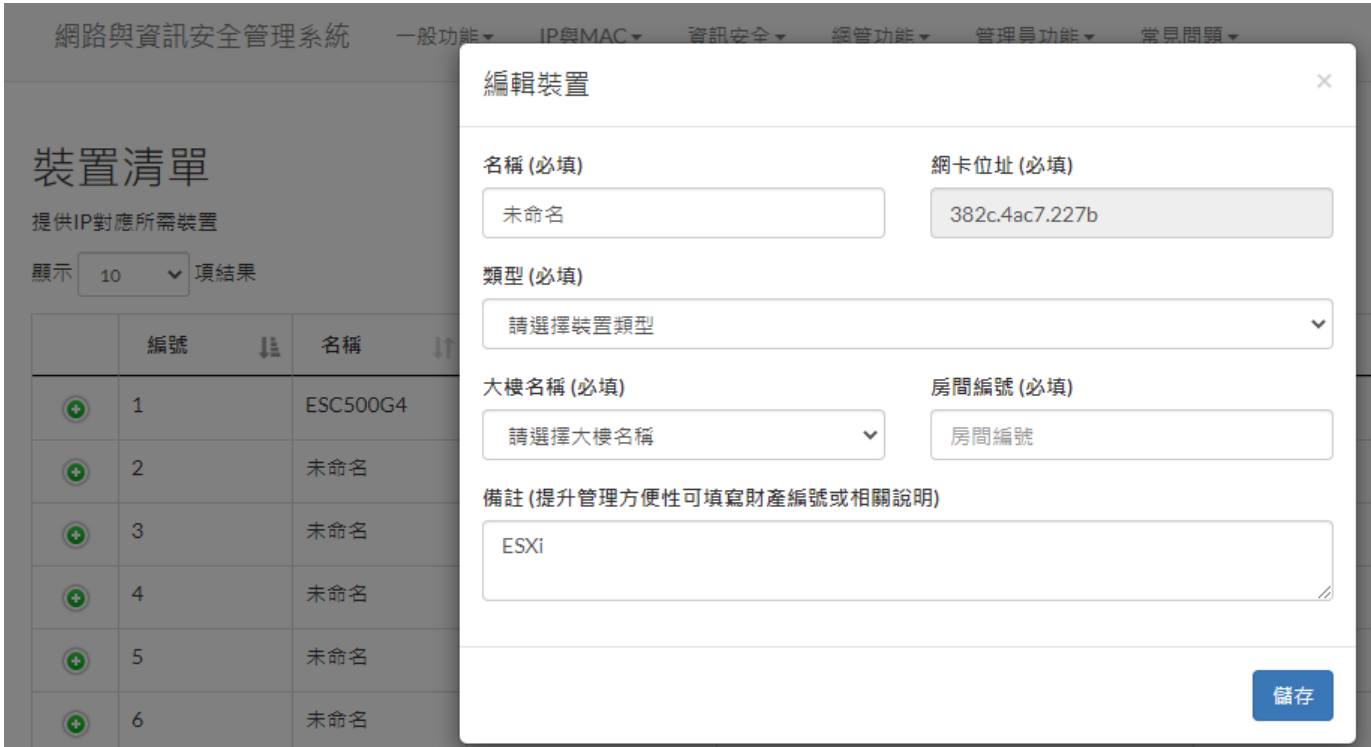
- 教師與學生網段區分
  - 本校在IP分配初期原有針對教師與學生網段區分，但幾十年來因需求大量增加在未全面重新分配下，其界限已非常模糊
  - 因應資通安全管理法規範，教師為法規規範之範圍內
- 本年度將先以行政體系IP調整後之狀況再行調整教學體系
  - 將教師與學生使用之IP範圍進行調整以強化資安

學術單位IP調整說明-整體說明

- 行政體系比照行政單位之資安提升措施
- 教師網段因考量研究彈性，相關措施將待本次調整後再行討論，以資通安全管理法應辦措施辦理
- 學生網段(含授課教室、系所電腦教室)
  將盡量放寬”資安管制措施”為原則以提升教學與研究彈性
- 政府獎補助與行政委託之計畫將依據今年IP調整後再另行開會討論

設備資訊登載

- 為加速教育部資安通報後續矯正預防措施
- 未來網管設定IP與MAC對應後，使用者應盡速進入管理平台登載設備詳細資訊
- 目前尚未強制，未來未登載詳細資訊者將僅能於校內連線



議程2
Q&A

資訊系統向上集中說明

資訊系統向上集中原則

- 為配合資通安全管理法相關措施，要求之範圍為「全機關」
- 行政單位內自建之系統(無論對內或對外)，均為資通安全管理法要求範圍
- 需向上集中系統範圍：
  - 行政/學術單位內自行建置之共用/共通性系統
  - 各研究計畫對外提供服務平台
  - 各校級單位平台
- 學術研究之自建主機不在向上集中範圍內，但不得讓外部連入使用

資訊系統向上集中原則

- 因法規規範嚴謹，應辦措施眾多，考量教學體系應著重在教學研究，盡可能採用機關共用/共通性系統
- 如單位內自行建置但本中心已有提供之共用/共通性系統(如RPage)，請逐步導入不再開放自建，以免重複性系統造成公帑之浪費

資訊系統向上集中原則

- 機關主要網站(首頁)為主要向上集中之目標，以下為仍使用自建首頁平台之單位：
  - 圖書資訊處
  - 華語文中心
  - 電機工程系
  - 資訊工程系
  - 應用英文系
  - 建築系
- 校級/院級研發中心將在下一波向上集中清查清單中，將另行通知

資訊系統向上集中原則

- 各單位共用/共通性平台仍未向上集中之單位：
  - 圖書資訊處(官網與內部系統)
  - 電機工程系(DNS、Email、官網與內部系統)
  - 資訊工程系(DNS、Email、官網與內部系統)

資訊系統自行管理原則

- 以系統為單位，依據本校ISMS規範及資通安全管理法B級機關要求完成該系統之ISO 27001驗證。
  並下列條件均須達到之系統：
  - 單位須具有2位法規要求符合資格之資安管理人員
  - 自建合規之資安控管措施(IPS/IDS、防火牆、WAF)
  - 依據教育部資通安全稽核要求備妥
    「稽核相關佐證紀錄及文件推薦準備列表」共計53項表格文件

- 達到上述條件之單位經本中心派遣內稽人員與第三方稽核人員確認無誤後，上簽並加會計網中心並經機關首長同意，則可自行管理免向上集中。
- 相關文件依據ISMS規範要求副本交付本中心備查。

資訊系統向上集中方式

- 全校性系統服務，備妥所需規格與環境需求，上簽並加會計網中心經機關首長同意後依據本中心「國立臺北科技大學雲端虛擬主機租用管理要點」申請，無須付費
- 非全校性系統服務(系所自建、計畫自建等)，依據「國立臺北科技大學雲端虛擬主機租用管理要點」申請，並依所需規格支付相關費用

- 相關費用回歸學校貴重儀器經費統籌使用

資訊系統向上集中方式

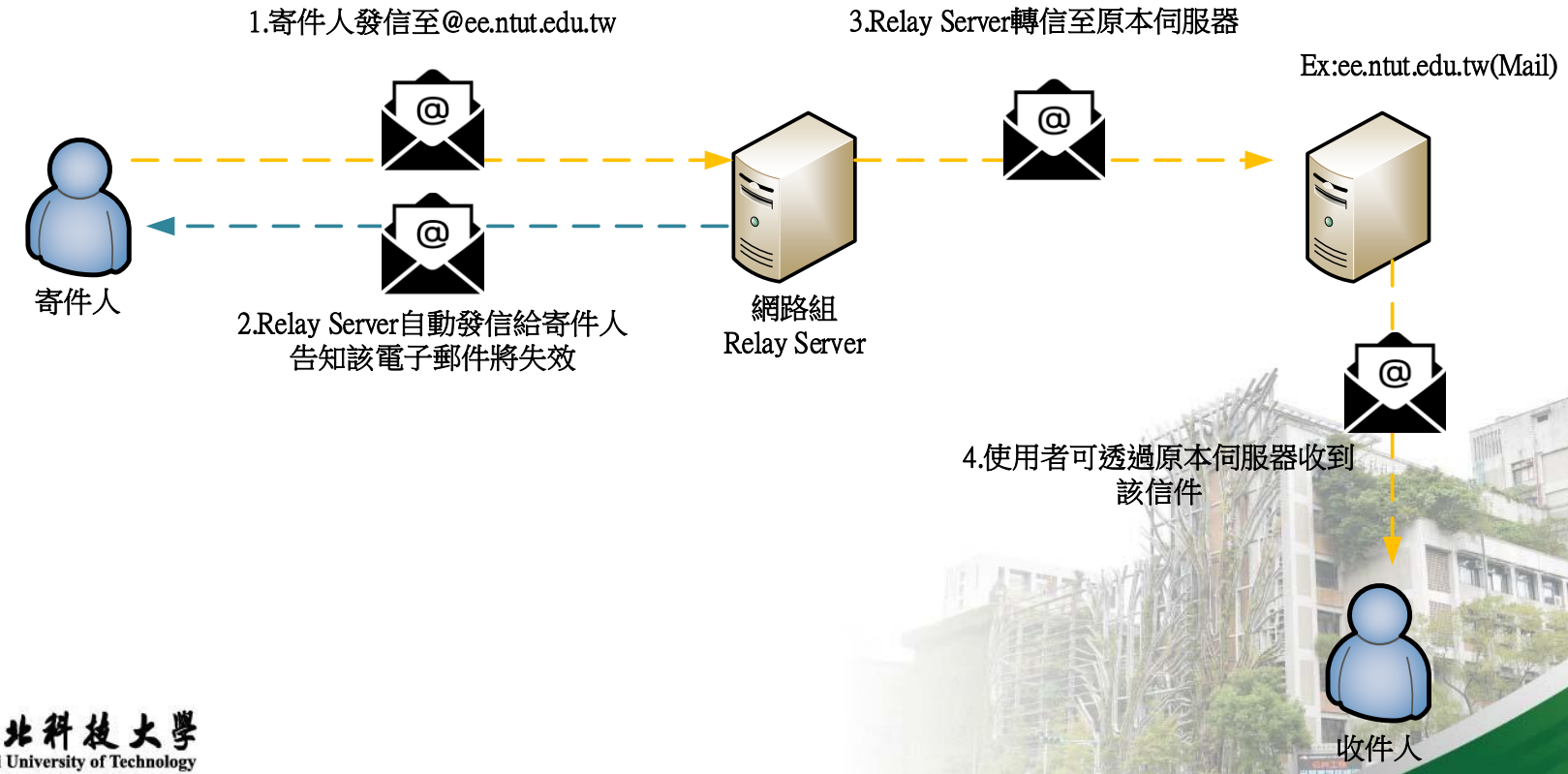
- 考量各單位本年度預算配置並鼓勵各單位今年度配合稽核要求向上集中
- 系所共用性/共通性系統仍須緩衝評估進行汰除或改用本中心共用性/共通性系統等過渡
- 向上集中選擇使用B方案虛擬主機者2年內免支付租賃費用

資訊系統向上集中方式

- 網站伺服器
  - 向上集中，建置於本中心並依前頁相關規定辦理
- 網域名稱伺服器
  - 清查確認仍有使用之網域名稱後，提供清單交付網路組，並於每年定期清查
- 電子郵件伺服器
  - 給予兩年緩衝進行汰除作業，統一改為使用@ntut.edu.tw集中管理，詳細方式請參考下一頁
- 其他類型伺服器
  - 依伺服器類型將專案方式並依前頁相關規定辦理

資訊系統向上集中方式-電子郵件

- 以電機系為例，原先伺服器無須變動，僅需修改MX對應至網路組特殊Relay Server



資訊系統向上集中管理方式

- 計網中心向上集中系統防護區分：
  - 高度防護：
    - 行政單位建置之全校共同/共通性系統
    - 政府機關構獎補助或行政委託計畫，其資通系統如屬委託機關之核心資通系統或委託案件金額在1,000萬元以上者
    - 其他有高度防護之需求但不在上述範圍內
  - 中度防護：
    - 一般性租用本中心虛擬主機適用

資訊系統向上集中管理方式

防護基準			
	中	高	備註
入侵偵測防護 (IPS/IDS)	有(*)	有	*需導入憑證集中管理方才能達到最大防護
第七層次世代防火牆 (NGFW)	有(*)	有	*需導入憑證集中管理方才能達到最大防護
網頁應用程式防火牆 (WAF)	選配	有 (僅網頁伺服器)	
日誌集中管理 (Log Server)	選配	有	
憑證集中管理 (SSL Offload)	選配	有	
負載平衡 (Server LoadBalance)	選配	選配	

資訊系統向上集中管理方式

- 本中心提供之虛擬主機為基礎設施服務(IaaS)，即虛擬主機建置後系統管理與使用為申請單位負責
- 由本中心依需求開啟虛擬主機後，以遠端管理通訊協定(如RDP、SSH等)方式進行連線
- 所需套件及環境可依照自身需求安裝使用
- 作業系統更新、套件更新由申請方自行管理

- 虛擬主機在本中心儲存空間有餘時將提供一日一次虛擬機完整備份，並保存14天
  仍強烈建議參照備份321原則(備份3份、2種儲存媒體、1份異地備份)，自行進行完整備份

資訊向上集中差異比較

主管機關要求或查核時			
	有向上集中	無向上集中	備註
ISO27001/資安法 (基礎建設)	**計網中心負責**	單位自行負責	本中心機房通過ISO27001驗證
ISO27001/資安法 (網路管理與防護)	**計網中心負責**	單位自行負責	本中心管理機制通過ISO27001驗證
資安法 (專責資安人員)	**計網中心負責**	單位自行負責	本中心具備2位法規要求之專責資安人員
資安法 (網路資安監控SOC)	**計網中心負責**	單位自行負責	網路組具備SOC相關機制
ISO27001/ISMS/資安法 (應用系統)	單位自行負責	單位自行負責	系統面由單位自行維護適法性

議程3
Q&A

防火牆防護提升說明

校內網段間納入資安防護措施

- 避免惡意程式校內攻擊流竄並強化機敏感資料保護
  - 強化單位間防護措施，各單位網段將納入防火牆防護作業
  - 以不阻擋正常連出流量為主，但不允許連入流量
  - 行政單位各網段間將不開放互通

- 無線網路政策調整尚待評估中

外連內防火牆防護措施提升

- 為提升校內防護已導入以下措施
  - 學術單位遠端連線管理通訊協定僅台灣開放連入(107年)
  - 行政單位外部連入防護阻擋(108年)
  - 如防火牆可辨識出，則不開放使用兩年內發生過資安事件或主管機關要求禁用之軟體連線
    (如TeamViewer、AnyDesk及Zoom等)

- 第一階段全校防護提升作業預計111年前導入
  - 除本校對外服務及向上集中依需求開放之系統外，為阻擋國際大量攻擊，將僅允許台灣IP連入，以利資安事件追查與提出損害賠償告訴
  - 評估進一步全面阻擋外對內連線達到有效管理與防護措施

政策實施時間表

- 第一季
  - 召開會議廣納各方想法意見進行分析與評估
  - 盤點各系所IP
  - 3月啟動IP調整作業
  - 委外廠商VPN強化管控措施
- 第二季
  - 相關院系所IP調整作業(另行通知)
  - 4月向上集中基礎建設建置
- 第三季
  - 相關院系所IP調整作業(另行通知)
  - 7-8月啟動向上集中政策執行，開始收容
- 第四季
  - 教育部稽核滿一年，繳交稽核缺失與改善作為成果報告
  - 校園防火牆防護措施提升

Q&A與臨時動議


工業推手一世紀．企業搖籃一百年
100 Years of Excellence · Cultivating Entrepreneurs of Tomorrow
TAIPEI TECH
Since 1912
國立臺北科技大學
National Taipei University of Technology
國立臺北科技大學