國立臺中教育大學遠端連線申請資安自主檢核表

v11211

項次	檢核內容	自主檢核情形	備註：未符合/不適用原因
1	依據112年3月21日本校112年第1次資通安全暨個人資料保護推動委員會管理審查會議決議，重點如下： (1)本校人員及廠商連線至校內，原則以 SSL VPN 連線，校內人員請依本校帳號密碼原則辦理（長度至少八碼、系統管理者至少十二碼、每九十天更換、複雜度四取三，每月執行系統更新、安裝與更新防毒軟體)；廠商校外連線則由業務主辦單位依變更管理程序進行檢視、審查及記錄，並於廠商結束遠端存取期間後，應更換 SSL VPN 登入密碼，確實關閉網路連線。 SSL VPN 安裝說明：http://www.ntcu.edu.tw/cc/sslvpn/sslvpn.htm 網頁路徑：本校全球網/資訊服務/SSLVPN 教學服務	□知悉	
	(2)請配合落實全校資通系統（網站）及物聯網設備盤點，盤點範圍如下： A.資通系統（網站)：包含主機使用本校網路，或使用本校網域名稱之資通系統(網站)及設備，如：XXX.ntcu.edu.tw。 B.物聯網設備：包含但不限於：網路印表機/多功能事務機、網路攝影機、門禁設備、環控系統、無線網路基地台(AP)/路由器、連網電子看板、能源管理系統(EMS)、網路儲存設備(如 NAS)等。 C.於112年5月30日之後，如發現未在盤點清冊內之資通系統(網站)或物聯網設備，計網中心將關閉校外連線，如須開放，請敘明原因並簽奉本校資通安全長(副校長)同意後，始可開放校外連線。 D.個人電腦及伺服器主機仍使用已停止支援的作業系統，如 Window7、Server2003及 Server2008等將於112年5月30日之後關閉校外連線，如須開放，請敘明原因並簽奉本校資通安全長(副校長)同意後，始可開放校外連線。 E.填寫網址： https://cc.ntcu.edu.tw/front/isms/isms02/news.php?ID=bnRjdV9jYyZpc21zMDI=&Sn=50	□知悉 □不適用	
1-1	依據行政院資通安全處110年3月2日院臺護字第1100165761號函(如下圖)，請各單位加強遠端連線存取控制機制，重點如下：		

國立臺中教育大學遠端連線申請資安自主檢核表

v11211

	(1)本校內部人員及委外廠商進行遠端維護資通系統，應採「原則禁止、例外允許」方式辦理，例外允許之先決條件如下： □地理限制，說明: □專案特性，說明: 建議每次**開放期限至多一週(週一至週五)**，到期後需重新設定 VPN 密碼，每天可連線時段建議設定為上午8時至晚上8時。 □緊急維護(因處理時效，如有重大安全性弱點需立即修復、有重大異常需立即排除等情形) 建議每次**緊急維護開放期限至多一日**，預設至當天晚上8時。	□知悉：左列請擇1勾選，並適度說明 □不適用	
	(2)於符合上述條件後，得開放前揭人員自遠端存取資通系統時，應至少辦理下列防護措施： A.依資通安全管理法施行細則第4條及資通安全責任等級分級辦法附表十中有關遠端存取相關規定辦理（應依據國家資通安全研究院發布之議價時最新版資通系統防護基準驗證實務(https://www.nics.nat.gov.tw/資安規範及報告/共通規範/))，並建立及落實管理機制。 B.開放遠端存取期間原則以短天期為限，並建立異常行為管理機制：系統管理單位應稽核帳號登入時間與執行紀錄，以確認時間與作業項目皆與實際情況相符。 C.校外連線由系統管理單位依變更管理程序進行檢視、審查及記錄，並於結束遠端存取期間後，應更換 SSL VPN 登入密碼，確實關閉網路連線。 申請方式請參考 https://drive.google.com/drive/u/1/folders/1zOQQD8MfsOub48u_lWx_h_dMXqqtYvKG	□知悉	

國立臺中教育大學遠端連線申請資安自主檢核表

v11211

行政院資通安全處 函

地址：10058 臺北市忠孝東路1段1號
聯絡人：侯舜仁
電子信箱：hsr@ey.gov.tw

受文者：教育部

發文日期：中華民國110年3月2日
發文字號：院臺護字第1100165761號
速別：普通件
密等及解密條件或保密期限：
附件：

主旨：近期迭發生機關開放委外廠商自遠端進行資通系統維護致存取機制遭駭客利用，間接攻擊機關資通系統事件，為降低資安風險，請各機關加強遠端存取控制機制如說明，請查照並轉知所屬。

說明：

一、各機關開放機關內部同仁及委外廠商進行遠端維護資通系統，應採「原則禁止、例外允許」方式辦理，若機關因地理限制、處理時效及專案特性等因素，須開放前揭人員自遠端存取資通系統時，應至少辦理下列防護措施：

(一)依資通安全管理法施行細則第4條及資通安全責任等級分級辦法附表十中有關遠端存取相關規定辦理，並建立及落實管理機制。

(二)開放遠端存取期間原則以短天期為限，並建立異常行為管理機制。

(三)於結束遠端存取期間後，應確實關閉網路連線，並更換遠端存取通道(如 VPN)登入密碼。

二、未依前述規定辦理遠端存取控制措施，致機關發生資安事件，情節重大者，機關應依「公務機關所屬人員資通安全事項獎懲辦法」規定予以懲處。

正本：總統府第二局、國家安全會議秘書處、立法院資訊處、司法院資訊處、考試院資訊室、監察院綜合業務處、各部會行總處署、各直轄市政府、各縣市政府、各直轄市議會、各縣市議會、本院資訊處

副本：電子公文交換章 2021/03/02 10:04:09

2	本校校內人員及廠商應檢核，所管電子郵件/個人電腦/筆記型電腦、所屬資通設備(如：事務機)及廠商登入帳號密碼，包含但不限於作業系統、應用系統、資料庫等各類帳號，不得使用弱密碼、預設帳號密碼，並符合規範之密碼複雜度要求，以及依業務需求設定適當網路存取限制，請確認系統(網站)設定帳號密碼原則已符合規定： (1) 網站、相關伺服器、網路芳鄰、路由器、交換器、儲存設備(如 NAS 等)、作業系統及資料庫等軟硬體設備應設定使用密碼，且預設之帳號（如 administrator、admin、root、sa）原則應停用。	□知悉	

國立臺中教育大學遠端連線申請資安自主檢核表

v11211

	(2) 通行密碼長度應至少八碼(系統管理者應至少十二碼)。 (3) 使用者每九十天應更換通行密碼，密碼最短使用期限應至少一天。 (4) 通行密碼應避免重複使用前三次變更之通行密碼。 (5) 禁止使用者共用帳號及通行密碼。 (6) 禁止使用身分證字號、學校/機關代碼、易猜測之弱密碼或其他公開資訊等作為帳號及密碼。 (7) 密碼禁止使用與帳號名稱相同。 (8) 不包含使用者的帳戶名稱全名中，超過兩個以上的連續字元。 (9) 密碼應包含下列四種字元中的三種： A. 英文大寫字元(A 到 Z)。 B. 英文小寫字元(a 到 z)。 C. 10 進位數字(0 到 9) 。 D. 非英文字母字元(例如：!、$、#、%)。		
3	應確認本校遠端連入之資通訊設備內無一般公務機密、敏感資訊或國家機密 (或以加密或其他適當方式儲存)，以避免不當揭露或遭不法蒐集、處理、利用等其他侵害情事，並應負損害賠償責任。 PS： (1)所稱一般公務機密，參考行政院訂定之文書處理手冊第五十一點規定，係指公務機關持有或保管之資訊，除國家機密外，依法令或契約有保密義務者。 (2)所稱敏感資訊，指包含個人資料等非一般公務機密或國家機密之資訊，如遭洩漏可能造成機關本身或他人之損害或困擾，而具保護價值之資訊。 (3)所稱國家機密，依國家機密保護法第二條規定，指為確保國家安全或利益而有保密之必要，對政府機關持有或保管之資訊，經依該法核定機密等級者。	□知悉	
4	本校設備與校外設備間資料分享須強化安全性；一般公務機密、敏感資訊或國家機密(例如：個資)勿下載至校外設備，必要時適度安全管控(如檔案加密碼、去識別化)，完成後須刪除；上傳至本校設備檔案須事先掃毒後再上傳。	□知悉	
5	**建議每月至少1次進行本校設備與校外設備之軟體元件漏洞修復與更新，包含作業系統、資通系統伺服器、開發框架，以及第三方函式庫等軟體元件**： 1.應用系統平台相關維護。 2.log 與帳號(OS event, web, AP, logon)異常事件檢視及整理。 3.平台效能調校(tuning)。	□知悉	

國立臺中教育大學遠端連線申請資安自主檢核表

v11211

	4.配合本校進行除錯、更新、漏洞修補與弱點修正：含系統相關主機作業系統、系統元件及防毒軟體病毒碼更新(防毒軟體授權可至校園資訊系統下載安裝)。 5.硬碟空間檢查及整理。 6.排程每日向校時國家時間與頻率標準實驗室進行校時。 7.拒絕所有連線，只開放必要之通訊埠連線及管理者 IP 連線。 [應關閉未使用 Protocol 及 Port，包含但不限於 Port 22、23、80、443、445、3389、8080、8081；遠端連線服務應限制連線來源 IP]		
6	為資安及用電考量-本校內設備原則下班時間請關機，有需求時再請同仁協助開機，使用後請關閉本校設備。	□知悉	
7	瀏覽器避免使用密碼記憶功能。	□知悉	
8	不瀏覽不明網站、不開啟來路不明信件、不安裝不明來源軟體、APP、線上遊戲軟體，以避免資通設備中毒。	□知悉	
9	使用即時通訊軟體不可涉及個人隱私資訊，並禁止傳輸機密資訊；必要時傳輸資訊必須適度安全管控(如檔案加密碼、去識別化)。	□知悉	
10	避免在公共使用之電腦登入公務系統帳號、密碼或傳輸公務資訊。	□知悉	
11	大陸廠牌資通訊產品一律禁止處理公務事務或介接公務環境。	□知悉	
12	請依本校 ISMS 程序書「ISMS-2-005實體與環境安全管理程序書」規定，將個人電腦、筆記型電腦、系統(網站)主機依據「ISMS-2-005-06個人電腦安全檢查表」中之各項檢查項目進行自評，並調整至符合規定。 PS：系統(網站)伺服器主機**建議原則**亦應依「ISMS-2-005-06個人電腦安全檢查表」中之各項檢查項目進行自評，並調整至符合，惟建議先行於測試機確認功能正常，確認功能正常後再套用至正式機。 「ISMS-2-005-06個人電腦安全檢查表」：https://docs.google.com/document/d/1D-WBwV8tAqycA0H1Wh835ClI9MsL7TOt/edit?usp=sharing&ouid=109066203372320544452&rtpof=true&sd=true 「ISMS-2-006網路安全管理程序書」：https://drive.google.com/drive/folders/140fRauxek_JijVrBqnrmid1jZQ0XGbzj?usp=sharing 「ISMS-2-012-01委外受託單位資通安全要求查核表」：https://drive.google.com/drive/folders/1uhrWvSlyBj8KQDptlC4nLmyrjVXxd2jn?usp=sharing 以上文件須以@mail.ntcu.edu.tw 帳號登入	□知悉	

國立臺中教育大學遠端連線申請資安自主檢核表

v11211

承辦人	單位主管