

# 資安宣導

## 遠端存取控制

# 大綱

- 一、依據
- 二、遠端桌面連線
- 三、外部存取控制
- 四、參考資料

# 一、依據

- 依教育部110年3月9日臺教資(四)字第1100029358號函轉行政院資通安全處請各機關加強遠端存取控制機制相關事宜，要求如下：

- 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。
- 未依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」規定予以逞處。

## 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  
類別：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

## 二、遠端桌面連線

- 110年5月31日已阻擋校外IP以微軟遠端桌面連線本校行政單位網段設備。
- 自111年2月1日起，阻擋校外IP以VNC、微軟遠端桌面等遠端存取應用程式，連線本校網段設備。
- 如有自校外IP透過遠端桌面工具連線需求者，請登入VPN後連線。

### 三、外部存取控制

- 自111年3月1日起，本校對外服務僅開放常用通訊埠(80、443)，其餘校外對校內連線均予以阻擋。
- 如對外提供資訊服務非使用常用通訊埠，請填寫資安及網路設備異動申請表，申請開放特定通訊埠。

資安及網路設備異動申請表					
文件編號	ISMS-207-02	機密等級	限閱	版次	1.0
紀錄編號：		申請日期：11X 年 XX 月 XX 日			
*申請單位	00處/系/所	*申請人	林00		
*申請用途/專案名稱	NAS/WiFiAP/XXX 設備申請阻擋校外連線				
*來源 IP	ALL	*目的 IP	140.123.XXX.XXX		
*有效日期	自__年__月__日__時起 至__年__月__日__時止 ※最長1年，到期重新申請	*Port	TCP：All UDP：All		
長時間開啟（連線日期一年以上）說明：					
*申請人	申請人核章	*申請單位主管	申請單位主管核章		
審核結果	<input type="checkbox"/> 同意 <input type="checkbox"/> 不同意		執行日期		
設備名稱					
處理紀錄：					
設定檔備份 <input type="checkbox"/> 是					
承辦人		承辦單位主管			

(\*表必填寫欄位)

### 三、外部存取控制

- 各單位教職員工生如需自校外IP連線公務電腦或資通設備，請**先登入**本校**VPN**服務後連線，VPN服務使用手冊已更新於資訊處網站，請自相關頁面下載運用。
  - 教職員工專用VPN：詳見遠距辦公專區（網址：[https://it.ccu.edu.tw/network\\_source.php?section=8](https://it.ccu.edu.tw/network_source.php?section=8)）。
  - 教職員工及學生共用VPN：詳見虛擬校園網路服務專區（網址：[https://it.ccu.edu.tw/network\\_source.php?section=7](https://it.ccu.edu.tw/network_source.php?section=7)）。

### 三、外部存取控制

- 各單位如需開放**廠商**自校外維護資通系統設備，可循以下方式辦理：
  - 本校已建置特權帳號管理平台，提供遠端桌面連線、Putty及Chrome等遠端連線工具，並側錄操作歷程，請填寫遠端連線管理申請表（填寫範例）申請平台帳號。
  - 不以特權帳號管理平台連線者，可填寫資安及網路設備異動申請表，申請開放廠商點對點連線，並應遵守資通系統防護基準遠端存取相關規定，建立並落實管理機制。

### 三、外部存取控制

- 重要資通訊設備及個人電腦開放遠端管理時，請啟用本機**防火牆**，僅開放**特定來源IP**連線。
- 資通安全責任等級分級辦法
- 個人電腦遠端桌面防火牆設定方式，請參考[安全居家\(遠距\)辦公連線服務](#)說明。



## 四、參考資料

- 公務機關所屬人員資通安全事項獎懲辦法
- 資通系統防護基準
- 遠距辦公
- 虛擬校園網路服務(VPN)



資訊處  
Office of Information Technology

感謝閱讀