

馬偕學校財團法人馬偕醫學大學校園遠端連線軟體管理要點

115 年 05 月 07 日資訊發展暨安全委員會會議新訂通過

115 年 09 月 09 日馬偕醫大圖資字第 1150007317 號公告發佈

一、目的：

為確保本校校園網路安全與合規性，建立完善的遠端連線管理機制，防範未經授權之遠端桌面軟體及私人VPN隧道繞過防火牆形成資安監控盲區，特訂定「馬偕學校財團法人馬偕醫學大學校園遠端連線軟體管理要點」（以下簡稱本要點）。

二、適用對象與範圍：

本要點適用對象包含但不限於本校教職員工、學生及委外供應商。

範圍涵蓋所有使用包含但不限於個人電腦、行動裝置或各類終端設備，經由包含但不限於 VPN、第三方遠端軟體或加密隧道技術，存取校內任何資訊系統或網路資源之行為。

三、遠端連線軟體使用限制與禁止行為：

為避免網路防護遭繞過，引發跨網段污染與勒索軟體大規模感染等極高資安風險，除經專案申請核准外，嚴禁於校園網路環境內使用下列遠端連線方式：

1. 第三方遠端工具：包含 AnyDesk、TeamViewer 等商業軟體。
2. 私人加密隧道：包含自建開源 OpenVPN、WireGuard 或使用商業 VPN 等。
3. 瀏覽器擴充功能：如 Chrome Remote Desktop 等。

網路使用者不得任意使用未經規範之 IP 位址，或利用工具軟體隱藏 IP 位址進行連線。

四、遠端連線申請與審核機制（圖書資訊處專案核可）：

為確保連線行為的可視性與可溯源性，網路使用者若因行政業務、教學研究或系統維護等需求，必須進行遠端連線時，應依下列規定辦理：

1. 申請制與圖資處審查：所有 VPN 及遠端連線權限皆採事前申請制。申請人須提出正式作業申請，且必須經過「圖資處」網路管理人員審核核可後，方能完成 VPN 申請與權限開通作業。
2. 未經圖資處核可，任何單位或個人不得私自架設或開放遠端連線通道。

五、違規處理：

網路使用者如違反本要點規定，將停止VPN使用權限

1. 本校教職員工，將先行暫停其網路使用權利，並通知所屬單位，俟資安問題排除後再行評估開放。
2. 若因違規連線導致校園網路遭受攻擊、資料外洩，或涉及違反法律時，行為人尚應依相關法令負連帶法律責任。
3. 若情節重大或造成實質資安損失者，除暫停權利外，應依校內教職員工獎懲規定報請處理。

六、本要點經資訊發展暨安全委員會議通過後發布實施，修正時亦同。