交通部公路總局臺中區監理所政風室
公務機密維護宣導

遠距辦公資安小錦囊

越來越多企業單位讓員工遠距辦公，來因應企業可能遭遇之各種緊急事件。因此遠端視訊會議相關系統的使用量遽增，引發相關資安議題。身為遠端視訊會議的使用者，我們該如何做好資安防護呢？以下八點資安防護提醒：

1、選用無資通安全疑慮的視訊會議軟體

2、選擇可信賴的下載軟體管道

在可信賴的官方網站或 app store 下載軟體，以避免安裝到含有惡意程式的偽冒軟體或 APP。

3、謹慎確認會議邀請與連結

來路不明的會議邀請或連結，極有可能是惡意連結，請勿點選避免受駭。

4、限制會議參與者

所有的會議建議設定密碼限制，並由會議發起人於會議開始前確認參與成員的身分。

5、避免在公開社群分享會議連結

請直接提供給與會者連結，如此可以最大限度地避免不相關的人員得知會議並混入會議中竊取商業機密。

6、謹慎使用螢幕共享的功能

會議中若需使用螢幕共享的功能，需限制特殊指定人士才可使用並共享。

7、更新至最新的軟體版本

8、確保使用設備的安全性

使用者參與線上視訊會議的資訊設備以及網路連線方式，皆需符合企業訂定之資安標準(ex: 限定使用資訊設備、不使用免費網路連線等)。

遠距辦公政策實施同時，企業與員工應積極做好資安準備，以避免發生資安事件，守護企業重要商業資產的安全性。

遠距辦公資安小錦囊

遠距會議篇

選用無資通安全疑慮的視訊會議軟體

企業選用遠距會議軟體，需考量安全性，避免使用有資安漏洞和疑慮的軟體，落實資安防護。

選擇可信賴的下載軟體管道

在可信賴的官方網站或app store下載軟體，以避免安裝到含有惡意程式的偽冒軟體或APP。

謹慎確認會議邀請與連結

來路不明的會議邀請或連結，極有可能是惡意連結，請勿點選避免受駭。

限制會議參與者

所有的會議建議設定密碼限制，由會議發起人於會議開始前確認參與成員身分。

避免在公開社群分享會議連結

請直接提供與會者連結，如此能最大限度地避免不相關人員得知會議並混入會議中竊取商業機密。

謹慎使用螢幕共享的功能

會議中若需使用螢幕共享的功能，需限制特殊指定人士才可使用並共享。

更新至最新的軟體版本

視訊會議軟體皆會因應各種資安漏洞進行修補更新，隨時更新到最新版本，可以確保使用上的安全。

確保使用設備的安全性

使用者參與線上視訊會議的資訊設備及網路連線方式，需符合企業訂定之資安標準(ex: 限定使用資訊設備、不使用免費網路連線等)。

官網：
https://twcert.org.tw/

FB：
台灣電腦網路危機處理暨協調中心
- TWCERT/CC

E-MAIL：
twcert@cert.org

資料來源：【台灣電腦網路危機處理暨協調中心】
https://www.twcert.org.tw/tw/cp-142-3528-62838-1.html