中華民國工程技術顧問商業同業公會

因應 Covid-19 疫情居家工作指引手冊
-資訊應用篇 V1.01

編寫：資訊委員會

中華民國 110 年 6 月 10 日

目錄

一、前言

在 Covid-19 疫情爆發之後，國內對於居家工作掀起一片熱潮，而居家工作需要的資訊產品，例如視訊會議軟體、WebCAM 鏡頭、無線網卡等，一時成為不可或缺的熱門商品。本篇主要就員工居家工作時，電腦軟硬體之使用方式做探討，包括幾種可能的使用情境、居家工作可能衍生的資訊安全問題，以及軟體授權上的疑問等作一整理，供本公會會員公司參考。

二、居家工作的幾種應用情境

情境一：員工將公司之電腦攜回至家中，居家工作。

說明：公司內已有內部電腦網路及對外固定線路寬頻時，可讓員工將公司電腦攜回，再連線回公司，透過網路磁碟機、軟體授權主機等共用資源，達到分享檔案、啟動軟體授權等目的。採用此情境時，應考慮下列事項：

1. 員工的使用體驗會在跟公司內相同，居家辦公比較容易上手。
2. 可使用 VPN(Virtual Private Network)連線，將家中的電腦連線至公司：此種方式具完整網路功能，可確保網路磁碟分享、啟動軟體授權等行為正常運作。
3. 可使用公司既有電腦防火牆之 VPN 功能，亦可額外架設 VPN 閘道器。
4. 須注意公司有足夠的對外頻寬，員工家中最好使用寬頻，不得已才使用行動網路。並須注意 VPN 授權數量是否足夠。

情境二：員工使用家中自有之電腦，遙控公司電腦。

說明：員工將公司電腦留在辦公室中，回到家中操作自有電腦，遠端使用公司資源。此時，除比照情境一可使用 VPN 連線，亦可使用遠端桌面方式遙控公司電腦。使用遠端桌面時，應考慮下列事項：

1. 員工家中的電腦需確保沒有中毒或遭駭，以免成為跳板攻擊公司網路。
2. 公司作為遠端桌面之電腦不能關機或切斷電源，網路亦須保持暢通。
3. 遠端桌面相當消耗網路頻寬，員工家中最好使用寬頻。

4. 遠端桌面一般無須另購授權，較為經濟。

情境三：員工使用個人筆電或行動裝置。

說明：假如員工並未將公司電腦搬回家中，亦未使用遠端桌面方式遙控電腦，公司可以建置虛擬電腦桌面-VDI(Virtual Desktop Infrastructure)，只要員工有網際網路及行動裝置或電腦，就可以採用 VDI 進入公司網路。VDI 的建置成本相當高，但使用彈性及安全性也相對比較好，使用 VDI 應考慮下列事項：

1. VDI 需採購軟硬體、使用權，以 10 人網路版為例，需數十萬元以上。
2. 員工登入 VDI 虛擬電腦桌面時，使用的是 VDI 伺服器上的資源，因此需要準備高效能等級的硬體設備及穩定的網路頻寬。
3. 只需要電腦帳號，即使員工沒有配發公司電腦，亦可使用 VDI。

使用情境	說明	優點	限制
情境一	使用 VPN	● 使用已習慣的電腦 ● 可以使用電腦原本安裝好的程式	● 電腦設備須搬遷
情境二	使用遠端桌面	● 可以使用電腦原本安裝好的程式 ● 電腦設備不須搬遷	● 辦公室電腦不能關機或斷網 ● 須考慮資安問題 ● 相當消耗網路頻寬
情境三	使用 VDI	● 使用便捷 ● 不需要先有公司配發之實體電腦	● 較為昂貴 ● 無法直接使用電腦原本安裝好的程式

三、潛在資安問題及建議處理方式

居家工作時，必須使用公眾的網際網路，因此資安問題不可忽視。以下分成電腦防毒、檔案保全、防止駭客入侵等方面來說明。

電腦防毒:

一般公司內的電腦均會安裝防毒軟體,包括使用者的電腦及共用的伺服器,以防止病毒入侵。當員工居家時,公司網路必須接續到開放的網際網路,使用的裝置也可能有員工家中的自有電腦,因為網路架構的改變,在防毒方面可能會有漏洞，而造成檔案中毒。

因此,不論是員工將公司電腦攜回家中使用,或是員工使用自有的電腦,均應確認已安裝防毒軟體,並保持病毒碼更新。同時,應將居家工作的電腦造冊，一旦發生中毒事件，可以很快找出病毒傳播來源。

檔案保全:

目前工程顧問公司不論是工程設計圖、預算書、施工規範、招標文件等重要文件之製作都是透過電腦，因此有許多文件需要保護，不可外流。在未實施居家工作時，公司可以透過檔案加密、封鎖電腦 USB 埠、拆除光碟燒錄機、封鎖雲端磁碟機等方式，來防止檔案外流。一旦員工居家工作，上述封鎖 USB、雲端磁碟、拆除燒錄機等作為是否有效需要再做檢討。

採用模式一 VPN 技術時,檔案允許被抄錄出來,存放到員工家中的電腦,因此建議的搭配做法是讓員工將公司電腦帶回家使用,檔案即使抄錄出來,也是存放在公司所有的電腦中。採用模式二遠端桌面時,如果沒有禁用磁碟機連接,公司資料仍有可能會透過家中電腦外流。最安全的方式是採模式三 VDI,這種模式無法將檔案攜出公司網路,只是相對上需要的投資相當昂貴。

如有檔案外流疑慮時，可以考慮採用資安監控軟體，對電腦檔案進出做一紀錄，以便事後追蹤處理。

防止駭客入侵:

不論採用何種模式居家工作，基本上都有資安風險。因為原本公司網路有防火牆保護，為了達成居家工作，防火牆都需要做一些額外解禁開放，以便員工進入公司網路。但是，防火牆另一端，並不一定就是員工，也可能是虎視眈眈的電腦駭客。

防止駭客入侵，除了添購網路設備，最重要的是安全的意識。例如員工的帳號、密碼不能外流，密碼要有複雜度以免被破解、最好增加除了帳號/

密碼組合以外的第二組認證方式。一旦駭客入侵，災情往往相當慘重。公司應預想可能的狀況,擬定應變計畫,做好資料異地備份,以減輕可能的損失。

四、常見問答

Q：居家工作時，若使用員工家中自有的電腦，是否可主張是 home use 使用，安裝 home use 版本的軟體?

A：即使不是在辦公室，也不是使用公司所有的電腦，只要行為人的目的是商業使用，就應該選用合法的商用版的軟體，不應使用限非營利之家用或個人用軟體版本。

Q：員工家中居家工作時，若使用的自有電腦被查獲使用盜版軟體，是否可主張電腦非公司所有，不須負責。

A：如行為人使用該電腦的目的是公司工作所需，即使電腦非公司所有，如有侵犯軟體使用權，公司仍需負責。

Q:除了手冊中的幾種使用情境,有沒有其他的方式可以支援 WFH work from home?

A：手冊中所列三種情境是較常見的居家工作方式，當然也有其他的技術或方式可以採用，例如採用雲端服務，租用公有雲或建置雲端主機等。

五、結語

新冠肺炎帶來的衝擊前所未見，對工程顧問業者來說，一旦影響到契約執行，未來會產生不少爭議要處理。為協助本會會員公司防範於未然，公會已洽請行政院公共工程委員會就可能發生的問題預作處置。

本篇即是針對居家工作時,資訊設備方面(含軟體授權及資訊安全)如何安排做一整理及建議。在此感謝公共工程委員會、經濟部智慧財產局、中華民國資訊軟體協會提供的意見與協助。