遠端工作 – 革命性的改變

資訊韌性與營運持續管理技巧

01 實體安全

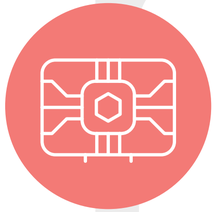
往來辦公室和住家時，遺失企業資產的可能性會增加。

02 軟體修補程式

需要長時間在家工作時，可考慮調整用戶端裝置設定。

03 密碼

包括螢幕逾時、螢幕鎖定、個人身份確認碼（PIN 碼）和/或生物辨識安全性功能（倘有相關功能可用）

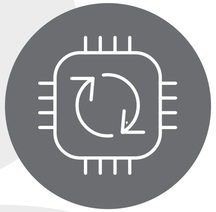


04 加密

應該使用額外加密功能，如電子郵件加密或安全的文件傳輸工具，以確保資料不論是在靜止、傳輸、共享還是使用時，都能受到保護。

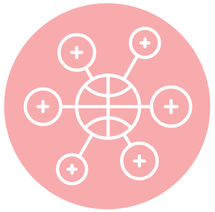
05 身份和特權帳號管理

建議使用「身份提供者」（IdP），以確保透過集中式的管理入口網站管制使用者，並啟動進階的安全功能，例如多因子驗證、政策管理，帳戶和應用程式的開通和通報。



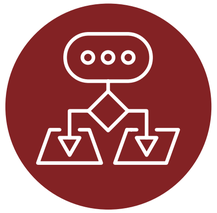
06 備份

制定並實施資料保護計畫，了解資料所處位置，對其進行相應的分類，確保公司在資料遭刪除、損毀、中斷或處理時，仍具有資料恢復能力。



07 網路連結

建立使用者的網路連結，確保連結速度和品質兼能符合使用者完成工作所需的水準。



08 網路攻擊

將游標停在連結上，以確認網址的有效性；不要打開您不熟悉的電子郵件；總體來說，您應該對源自網際網路的任何內容和消息抱持零信任。

09 衛生

對於遠端工作的團隊成員，以及他們使用的設備而言，此時此刻的個人衛生尤為關鍵。

10 政策管理

公司應考慮以雲端為基礎的政策管理平台，藉此執行資訊安全、資料保護和其他相關政策，並能夠回報相關執行成果。

bsi.

了解更多資訊

BSI 英國標準協會台灣分公司
電話 +886 (0) 2-2656-0333
電子郵件 infotaiwan@bsigroup.com
官方網站 bsigroup.com/zh-tw