沒有百分之百的資訊**安全**，

得靠**每個人**從**小地方**一起努力！

1.不明人士要盤查

- 不明人士，在辦公區域內走動，應該主動詢問其來意。
- 發現可疑狀況應加以制止或通知相關人員處理。
- 即使是認識之同仁，進出其沒有權限出入之區域，也要加以勸阻或通知相關人員處理。
- 委外服務人員出入本局，應一律配掛臨時工作證並遵守門禁之規定。
- 委外服務人員進入本局時，應直接到指定之工作區域，禁止到非工作區域；離開時，應直接出大門，禁止在本局內逗留。

2.電腦不用要登出(1)

- 離開座位，電腦應該設定螢幕保護程式（須設定開機密碼，時間最長不得超過20分鐘）或是其他控制措施保護
- 離開座位致所使用資訊設備有遭入侵之虞者，應於離開前將螢幕鎖定
- 長時間離開辦公室，建議將電腦關機
  - » 杜絕來自網路破壞
  - » 防止帳號或密碼被盜用
  - » 防止重要資料遭竊

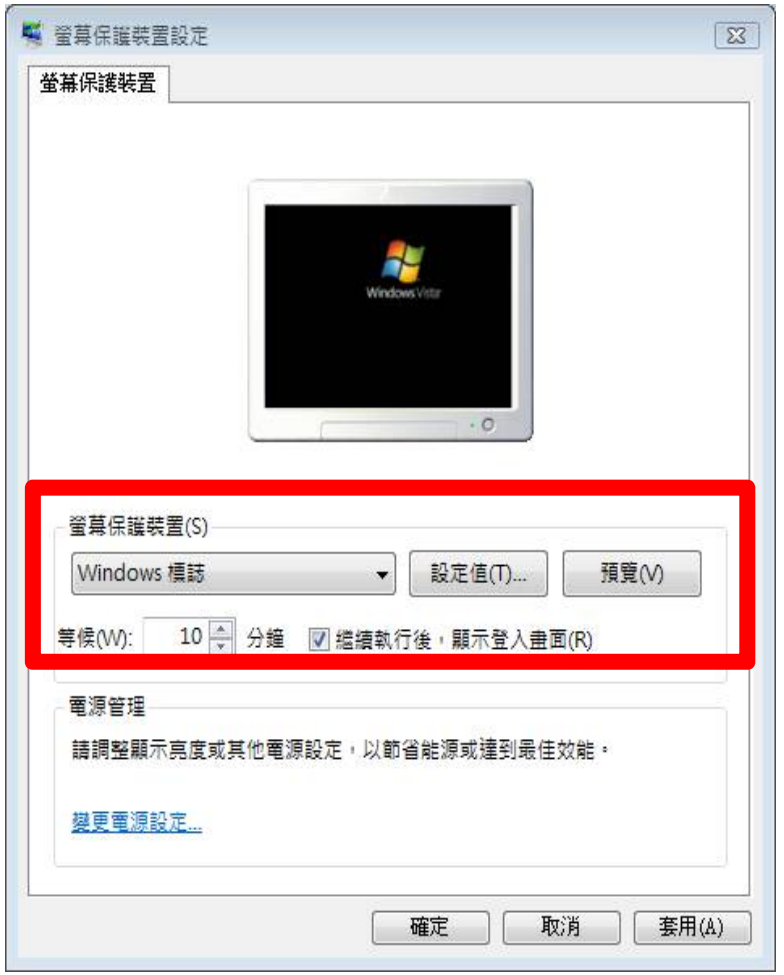
2.電腦不用要登出(2)

自我檢查

- 檢查作業系統之「螢幕保護程式」設定，確定一段時間未動作後會進行鎖定，避免他人誤用。

執行重點

1. 檢視是否依單位規定時間已設定「等候時間」。
2. 檢視已勾選「繼續執行後，顯示登入畫面」項目。
3. 若單位內以AD目錄服務進行控管，檢視GPO之設定是否包含「螢幕保護程式」設定。



3.機密資料要保護(1/2)

- 員工可能會把機密性資料文件、備忘紙、以及記載個人相關資訊等文件，隨意放置於桌上。
- 或者將資料進行完善的分類，並且儲存在電腦桌面上，這些動作都很容易導致資料的外洩。
- 因處理業務保有敏感性、機密性電腦資料或檔案者，應加強安全保護措施，如下班時應該上鎖或以其他方法妥為收存。

3.機密資料要保護(2/2)

- 連接網際網路的個人電腦、筆記型電腦
  - » 不得處理機敏公務
  - » 不得放置機敏公務資料
  - » 禁止連接儲存機敏公務資料之可攜式儲存媒體（磁片、光碟片、隨身碟、外接式硬碟等），以防止後門（木馬）程式竊取資料
- 避免**USB儲存裝置**讓電腦系統感染病
  - » 預防電腦病毒傳給USB儲存裝置
    - 建議：在USB行動碟內建立 autorun.inf (ini) 資料夾
  - » 避免USB儲存裝置傳病毒給電腦
    - 關閉USB儲存裝置自動執行設定（Auto Run）
  - » 常見USB儲存裝置病毒
    - kavo.exe, taso.exe, mpsvbtk.exe, wjftxbl.exe, meex.exe, hfhludy.exe

4.重要資料要備份

- 不論是紙本或電子檔的重要資料，皆應：
  - » 定期備份
  - » 存放在不同地方(異地備份)。
- 資料備份原則
  - » 資料價值較高時應優先備份。
  - » 選擇適合之儲存媒介進行資料備份工作。
  - » 按所欲備份的資料型態，選擇方法進行備份(如：完份、漸進式(增量)備份)。
  - » 備份的資料需定期做資料回復測試，以確認備份資料的可用性。

5.電腦防毒要更新(1/2)

- 電腦中毒徵兆：
  - » 電腦系統運行速度異常緩慢。
  - » 上網速度越來越遲緩。
  - » 異常的系統訊息通知。
  - » 螢幕顯示異常，例如畫面突然一片空白。
  - » 來自防毒軟體的警告訊息。
  - » 電腦無故自動關機或不斷重新開機。
  - » 瀏覽器自動出現產品廣告或色情網頁。
  - » 網路流量異常，例如沒有使用網路服務或收發電子郵件，但網路的連線燈號卻一直閃爍。

5.電腦防毒要更新(2/2)

- 防毒軟體的偵測與防範功能只有在該軟體有在運作、且有時常更新病毒碼情形下，才會產生效用。
- 防範訣竅：
  - » 隨時注意防毒軟體的病毒碼是在最新的狀態（四個病毒碼版本之內，如有問題立即連絡單位資通安全業務承辦人員）。
  - » 安裝防毒軟體或反間諜軟體。
  - » 不關閉、不刪除防毒軟體。
  - » 定期執行掃毒。
  - » 不要隨意複製或下載不明檔案。
  - » 不要隨意開啟檔案。

6.應用系統要更新(1/2)

- 當軟體被使用一段時間後，通常會出現一些小問題或安全漏洞，這些漏洞也是駭客容易利用的弱點，零時差攻擊即目前駭客最喜歡利用的手法。
- 防範訣竅：
  - 檢查以下重要應用程式或軟體是否為最新版本：
    - 作業系統(Windows 7 或2000、Mac、Linux...等)
    - 網頁瀏覽程式(IE、FireFox...等)
    - 辦公室應用軟體(Office、Adobe PDF...等)
    - 電子郵件收發軟體(如outlook、outlook express...等)
- 大部分的軟體都會提供一項「自動更新」功能，啟動自動更新功能為最方便也最迅速的一種定時更新方法。

6.應用系統要更新(2/2)

自我檢查

- 檢查作業系統之「Windows Update」是否已更新至最適狀態。

新增或移除程式

執行重點

1. 作業系統進行Windows Update前，是否先進行測試，確認新版修補程式(Path)不會影響系統服務提供，才佈署至正式環境。

2. 是否定期檢查電腦之更新狀態，確保無系統長期未安裝修補程式之情事發生。(尤其新進同仁所配發之個人電腦)。

3. 檢視作業系統變更程序文件
   - 使用者帳號異動控管。
   - 作業系統物件與存取權限異動控。
   - 作業系統檔案內容存取控管。

7.使用網路要注意

- 公務電腦原則上限公務使用，且必須加入網域。
- 不得任意更改個人電腦IP 位址與網路卡。
- 個人電腦不得安裝數據機或架設無線網路等相關對外連線設備。
- 非經本局同意不得自行與外界網路相連結；未經核准不得於本局網路私自架設網站。
- 不得將私人個人電腦、筆記型電腦連接公務網路(內外網)。
- 除因公務需要且經本局核可外，不得使用點對點（Peer-to-Peer, P2P）分享軟體。

8.電腦軟體要授權

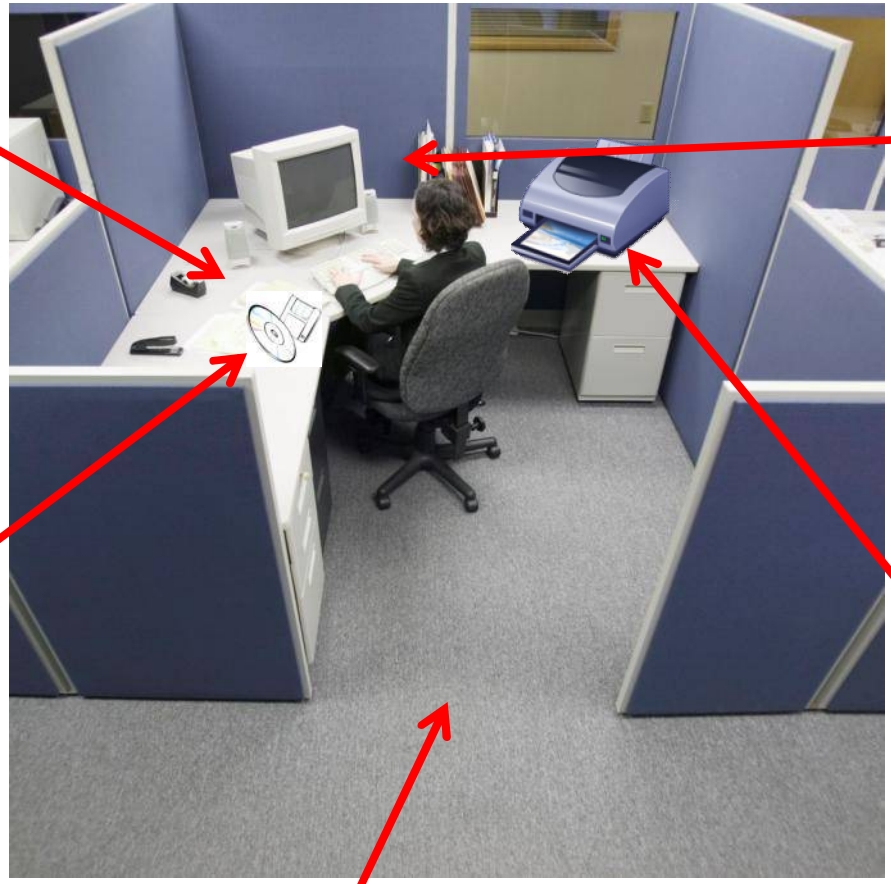
- 個人電腦原則僅安裝業務所需軟體，安裝前應確認取得合法授權。
- 連接網際網路之電腦，不得安裝本局公務使用之軟體，亦不得有本局標識之圖示或機關銜稱。
- 不得將授權軟體轉借或給予未經授權人員使用。
- 不得任意移除或卸載本局所安裝之資安防護軟體。
- 使用私有、試用、免費或共享軟體時應考量系統安全性，避免危及本局電腦或網路的安全。
- 如發現使用非授權的軟體，由使用者自行負相關法律責任。

9.資訊傳輸要注意

- 機密性資料及文件，不得以電子郵件或其他電子方式傳送
- 機密性資料以外之機敏性資料及文件需以適當的加密或電子簽章等安全技術處理
- 應確認對方的郵件地址，不要隨意轉寄未確認來源之信件
- 機密文件以人工傳遞需妥善保護（如：專人親送、密封）
- 機敏性資料及文件以書面方式傳遞時，須密封交專人傳遞，封套應註明收件人，並由其當面簽收，嚴禁他人拆封。

資訊安全宣導 - 辦公室設備使用注意事項

- 離開座位時，機密文件不應置於辦公桌
- 下班前需清理工作場所



- 電腦閒置時，應設定螢幕保護程式或鎖定螢幕
- 不應將使用者之帳號密碼紀錄於紙本
- 定期檢視防毒軟體及Windows Update是否確實更新

- 儲存媒體(如USB隨身碟)應妥善保管
- 使用、移動及存取多媒體應遵循管制程序
- 報廢的儲存媒體需確實銷毀

- 印表機、影印機應有專人負責
- 紙本文件回收前應確認是否含有機密資訊
- 文件銷毀需確實
- 會議後須將會議室桌面及白板淨空

- 限制區域應有門禁管制非經允許與陪同，外部人員不得進入
- 辦公區域檔案櫃、抽屜、辦公室應上鎖