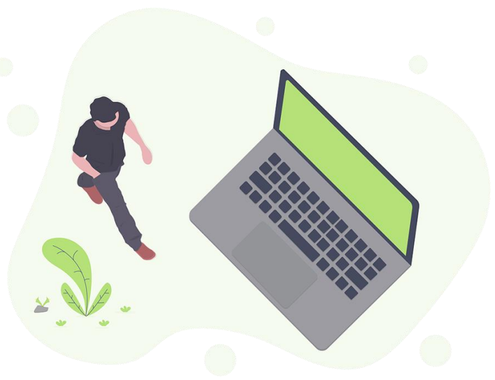
資訊及系統使用

1. 使用資訊及資通系統前應經其**管理人授權**。
2. 使用資訊及資通系統時，應留意其資通安全要求事項，並負對應之責任。
3. 資訊處理設施的授權過程應制定安全控管使用資訊及資通系統，**新增、異動或使用須經過授權程序**，資訊存取權限之設定以工作所需之**最小權限與最少資訊為原則**。
4. 非本校同仁使用本校之資訊及資通系統，應確實遵守本校之相關資通安全要求，且未經授權不得任意複製資訊。
5. 針對**有必要特別保護**系統，應嚴格管制並建立申請系統存取**特別權限之授權程序**，**權責主管審查**系統存取特別權限名單，宜以**執行業務及職務所必要者為限**。



防範惡意軟體

1. 學校之主機及個人電腦應安裝**防毒軟體**，並時進行軟、硬體之必要**更新或升級**。
   (1)經任何形式之**儲存媒體**所取得之檔案，於使用前應**先掃描**有無惡意軟體。
   (2)**電子郵件附件及下載檔案**於使用前，宜於他處**先掃描**有無惡意軟體。
   (3)確實執行網頁惡意軟體掃描。
2. 使用者未經同意**不得私自安裝應用軟體**，管理者並應每半年定期針對管理之設備進行軟體清查。
3. 使用者**不得私自使用已知或有嫌疑惡意之網站**。
4. 設備管理者應定期進行**作業系統及軟體更新**，以避免惡意軟體利用系統或軟體漏洞進行攻擊。

實體環境安全

1. 應實施**桌面淨空**，重要文件應妥善保管。
2. 將**機敏、限閱**等級的資料存放於**可攜式設備與媒體**時，應採取適當**加密處理或保護措施**，避免遺失時洩漏資訊。為降低媒體劣化之風險，無法讀取前加以**備份**。
3. 依據資訊資產處置規定，**機敏、限閱**等級的資訊類資訊資產以任何型式儲存均須**置於上鎖區域保管**，並設有存取控制。
4. 依據應用系統測試/正式環境、資料庫之安全維護規定，應將**敏感性系統隔離**。
5. 針對**存有個人資料**之紙本文件及可攜式儲存媒體，不使用或下班時，應遵守桌面淨空政策，放置於**抽屜或儲櫃並上鎖**。

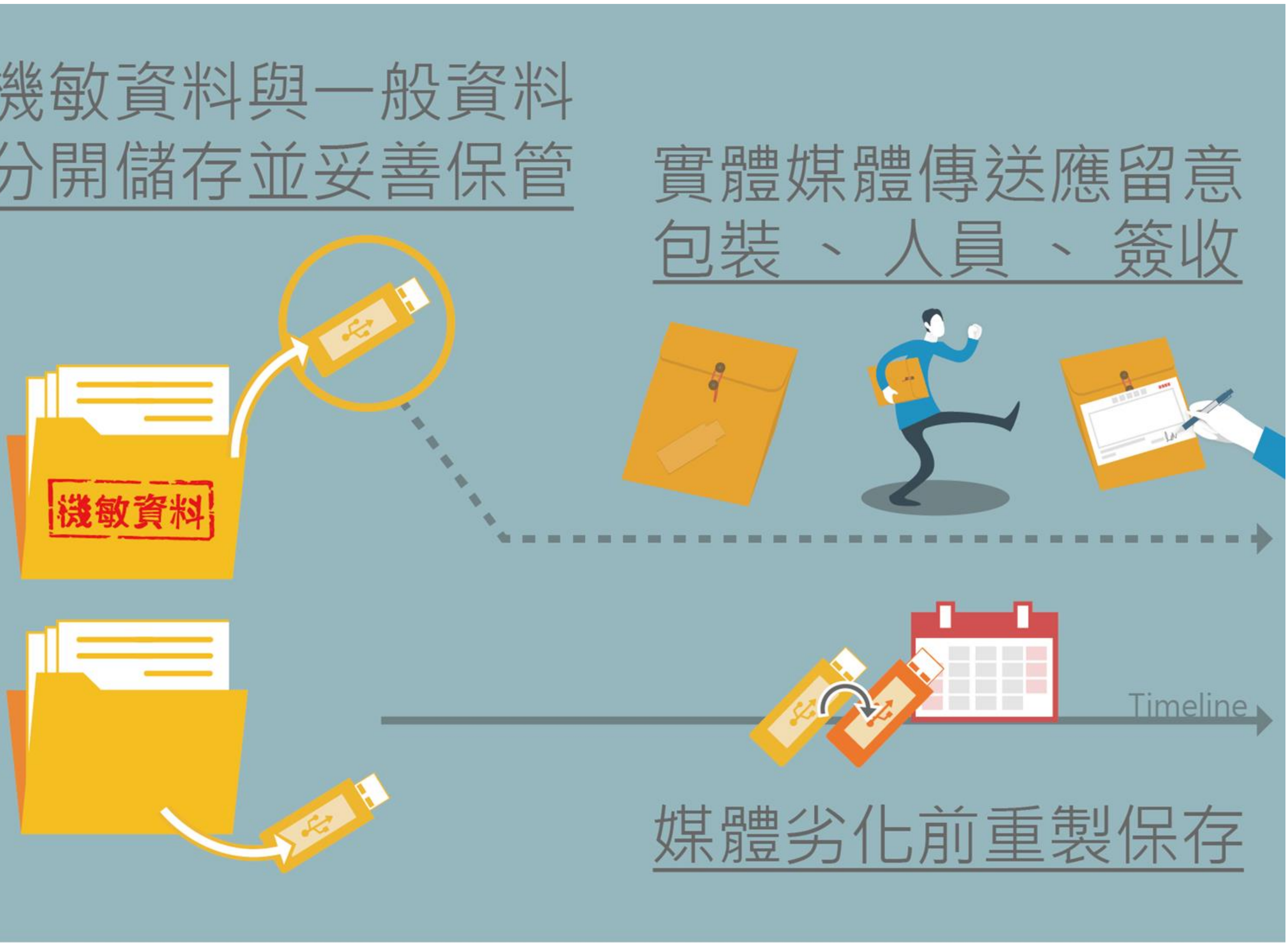
辦公室實體安全

1. 應考量採用**辦公桌面的淨空**政策，以減少文件及可移除式媒體等在辦公時間之外遭未被授權的人員取用、遺失或是被破壞的機會。
2. **文件及可移除式媒體**在不使用或不上班時，應**存放在**櫃子內。
3. **機密性及敏感性資訊**，不使用或下班時應該**上鎖**。
4. **機密資訊**或**處理機密資訊之資通系統**應**避免**存放或設置於**公眾可接觸**之場域。
5. 顯示**存放**機密資訊或處理機密資訊之資通系統**地點**之通訊錄及內部**人員**電話簿，不宜讓**未經授權**者輕易**取得**。
6. 資訊或資通系統**相關設備**，未經管理人授權，**不得被帶離**辦公室。

國立陽明交通大學　資訊技術服務中心　(03)5712121#31888

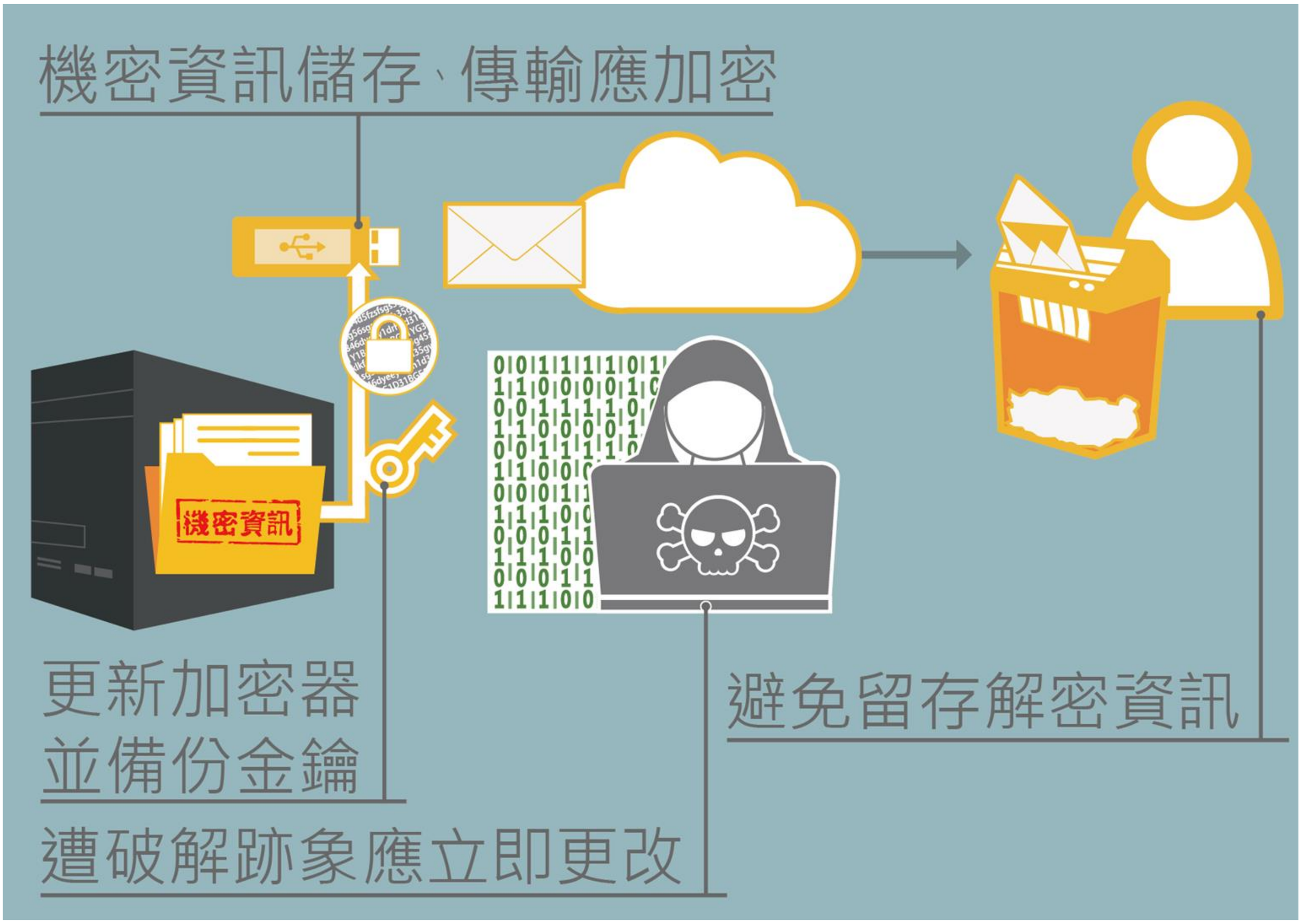
媒體防護措施

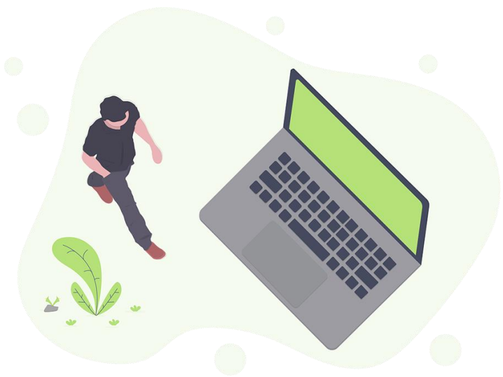
1. 使用**隨身碟或磁片**等存放資料時，具**機密性、敏感性**之資料應與一般資料**分開儲存**，不得混用並**妥善保管**。
2. 資訊如以**實體儲存媒體**方式**傳送**，應**留意**實體儲存媒體之**包裝**，選擇適當**人員**進行傳送，並應保留傳送及**簽收**之記錄。
3. 為降低媒體劣化之風險，宜於所儲存資訊因相關原因而**無法讀取前**，將其**傳送至其他媒體**。
4. 對機密與敏感性資料之儲存媒體實施防護措施，包含機密與敏感之紙本或備份磁帶，應保存於**上鎖之櫃子**，且需由專人管理鑰匙。



加密保護措施

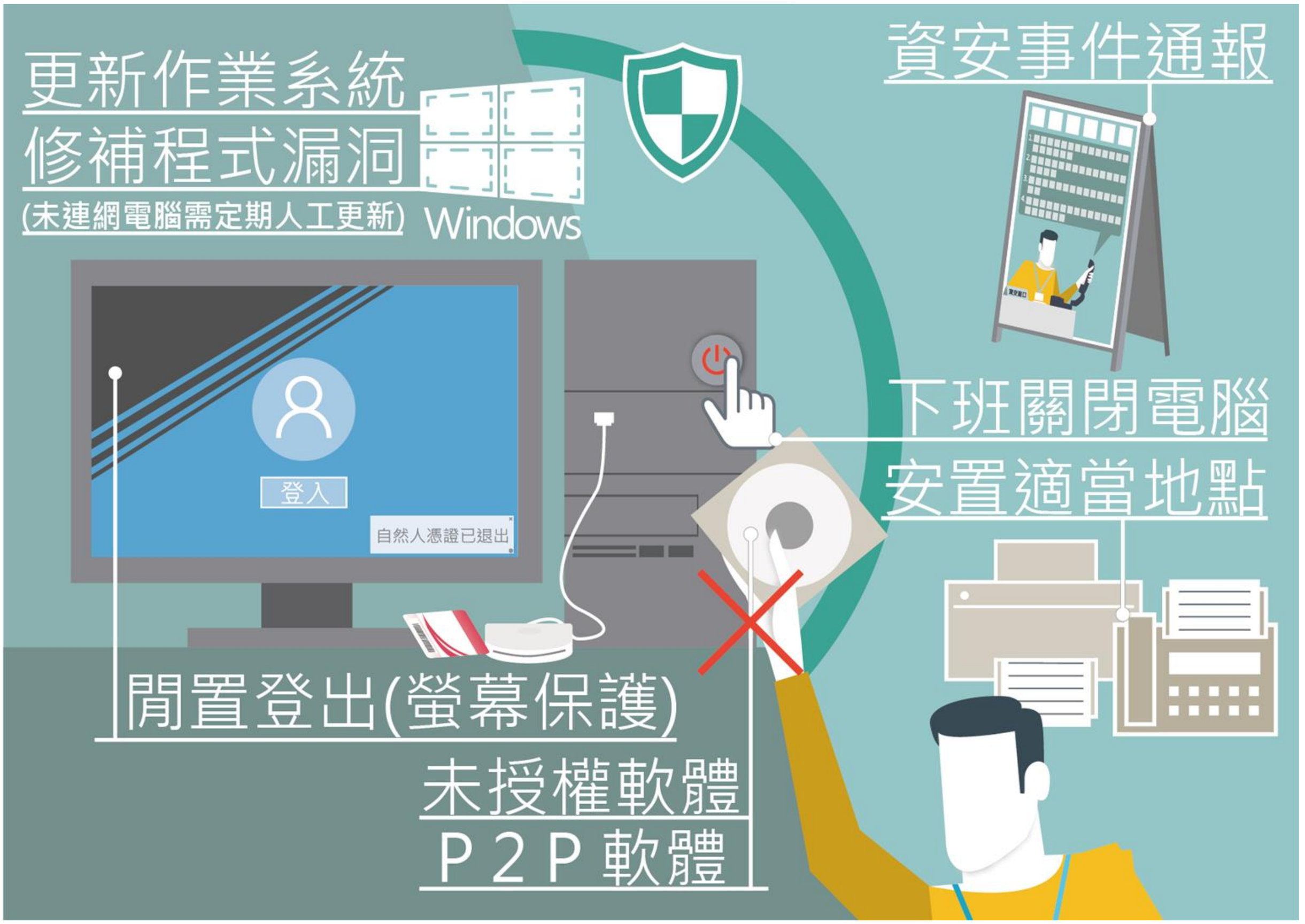
1. 學校之**機密資訊**於**儲存**或**傳輸**時應進行**加密**。
2. 將「機敏」或「限閱」等級之資訊資產**存放於可攜式設備與媒體**時，應採取適當**加密**處理或**保護**措施，避免遺失時洩漏資訊。
3. 學校之**加密保護措施**應遵守下列規定：
   (1) 應落實**使用者更新加密裝置並備份金鑰**。
   (2) 應**避免留存解密資訊**。
   (3) 一旦加密資訊具**遭破解跡象**，應**立即更改**之。

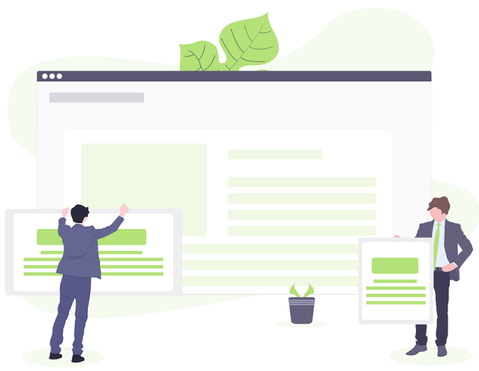




電腦使用安全

1. 電腦、業務系統或自然人憑證，若**超過十分鐘不使用**時，應立即**登出**或啟動**螢幕保護**功能並**取出自然人憑證**。
2. **禁止**私自安裝**點對點檔案分享軟體**及**未經合法授權**軟體。
3. 連網電腦應隨時配合**更新作業系統、應用程式漏洞修補程式及防毒病毒碼**等。
4. 筆記型電腦及實體隔離電腦定期以人工方式更新作業系統、應用程式漏洞修補程式及防毒病毒碼等。
5. 下班時應關閉電腦及螢幕電源。
6. 如發現**資安**問題，應主動循機關之通報程序**通報**。
7. **支援資訊作業的相關設施**如影印機、傳真機等，應**安置在適當地點**，以降低未經授權之人員進入管制區的風險，及減少敏感性資訊遭破解或洩漏之機會。





電子郵件使用

1. **機敏**公文不得以電子郵件傳送。
2. 含有**個人資料**之信件必須**加密**傳送。
3. 電子郵件**加簽**以避免發送匿名或偽造。
4. **不得**利用公務電子郵件進行**侵害他人權益、違法**之行為。
(包括以電子郵件大量傳送廣告信、連鎖信或無用之信息，或以灌爆信箱、掠奪資源等方式。以電子郵件、線上互動或類似功能之方法散布詐欺、誹謗、侮辱、猥褻、騷擾、非法軟體交易或其他違法之訊息。)

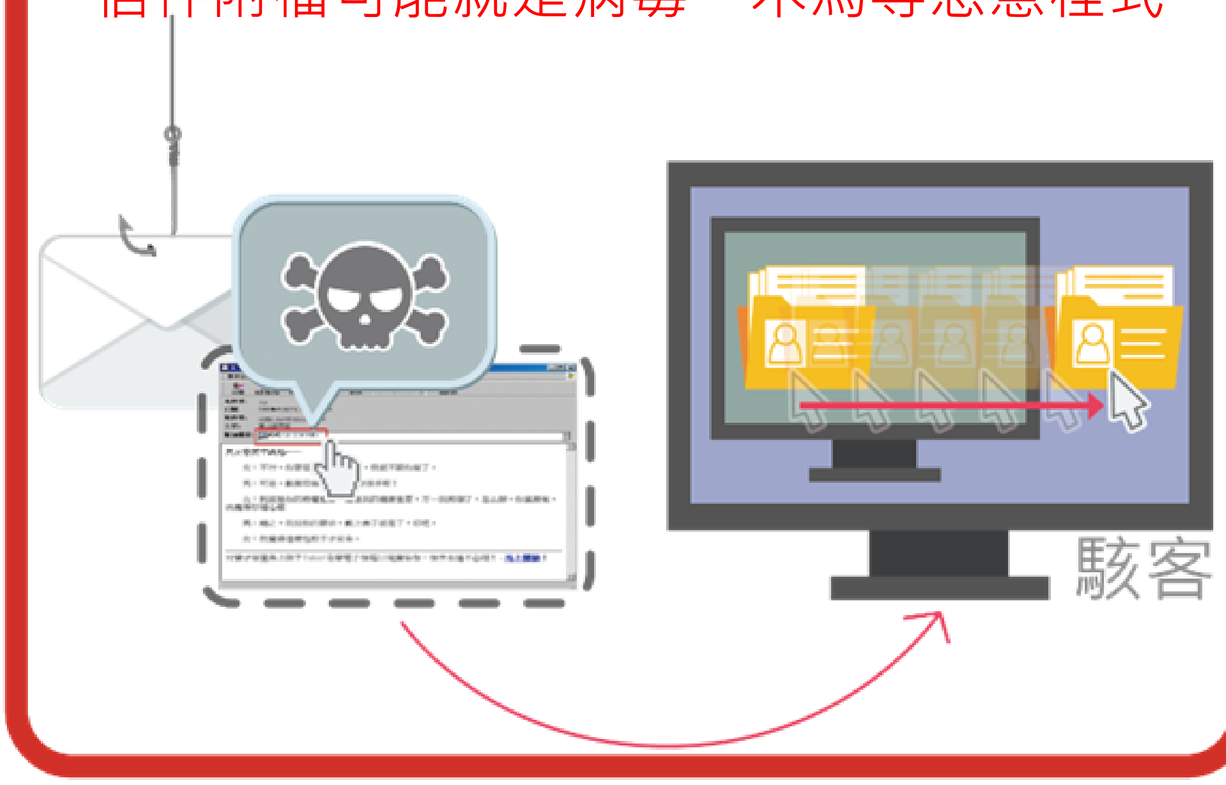
社交工程要警覺

教育部每年4月~11月都會實施社交工程演練，目的是為了模擬駭客寄送各類詐騙信件的手法，測試教職員點選各類誘騙信的比率，以強化教育機構教職員對資安等社交工程的警覺意識。

社交工程是利用人性的弱點進行詐騙，最常利用電子郵件等方式進行。往往駭客最常在這類的信件中藏惡意的軟體或連結，使用者稍不注意點擊或開啟就會讓駭客有機可趁。

駭客會弄個假冒網站來騙取你的帳號密碼

信件附檔可能就是病毒、木馬等惡意程式



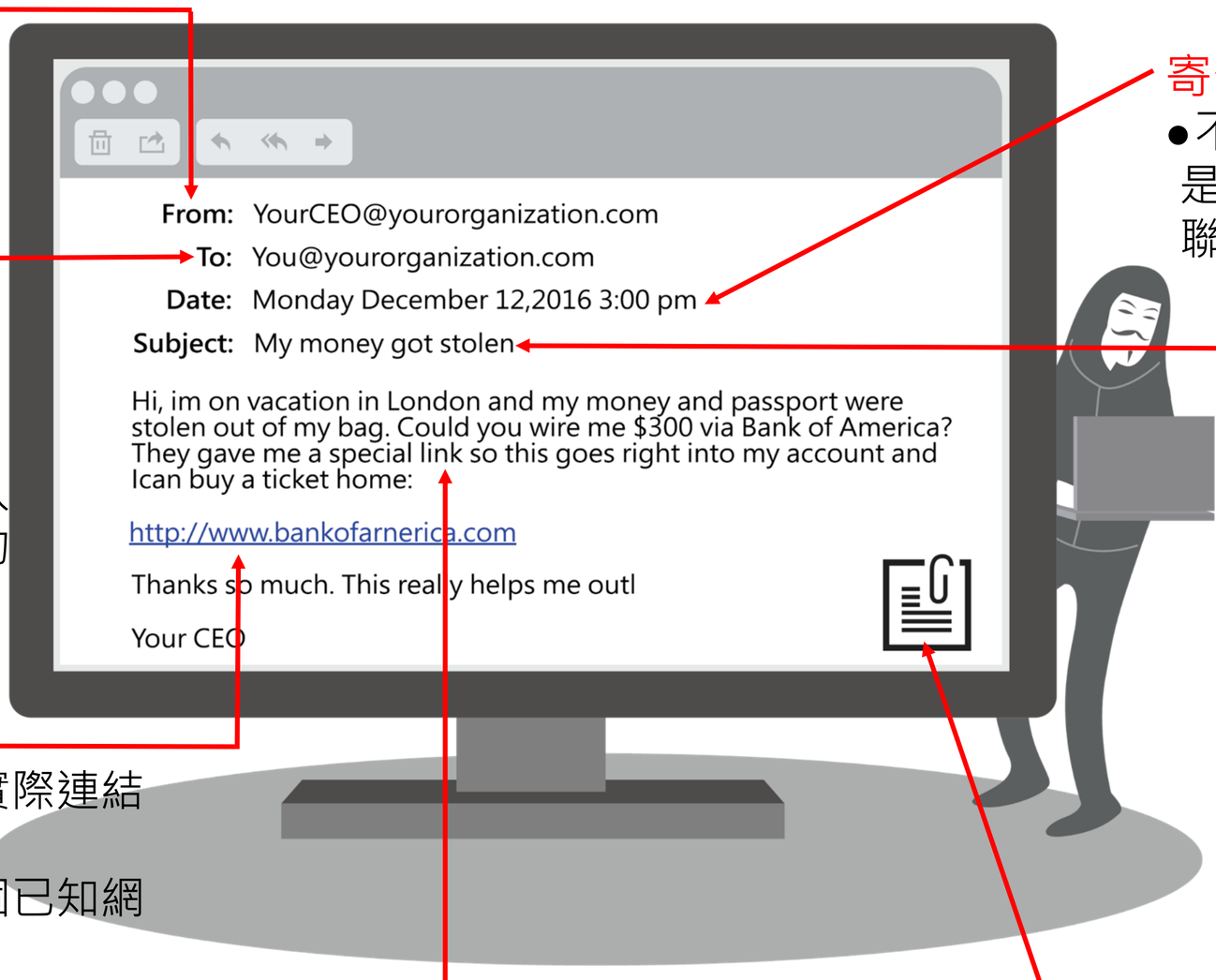
收信時必須要注意寄件者的信箱、寄件時間以及信件的主旨還有附加檔案等等...，發現這些疑點有可能是釣魚郵件就應避免開啟信件附件或點擊信件內的超連結。

寄件人信箱若是.....

- 不認得的人
- 沒有業務往來的人
- 署名某人但他應該不會跟我聯絡的信箱網域名稱蠻可疑的(像某單位的網域又有點不像、或是免費信箱)

收件人群組若是.....

- 還有其他一些不認識收件人
- 看來像是從網站把同頁面的通訊錄都納入收件人名單中



寄件時間若是.....

- 不太正常的寄件時間，像是半夜3點怎麼有人會寄信聯繫業務呢?

信件主旨若是.....

- 主旨看來跟自己無關的
- 主旨與信件內容不相關
- 主旨是回覆什麼，但之前並未寫信去問過什麼啊!

信件內的超連結若是.....

- 滑鼠移到超連結上可看到實際連結的網址與表面上的網址不同
- 超連結網址看得出來是某個已知網站但中間有些微拼錯字的
- 超長的超連結網址就要特別小心

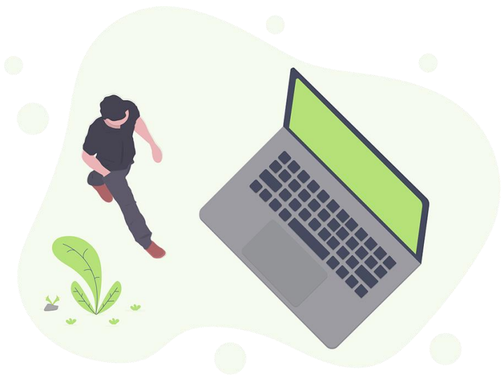
信件內容若是.....

- 不合常理
- 提到為了避免什麼不好的後果
- 提到你中獎了或你獲得什麼好處
- 提到別人或自己可能發生桃色事件或不雅照片等八卦消息
- 內容明顯文法錯誤或錯字不少，不像是一般人會嚴謹擬訂字句。
- 強調快點擊超連結或開啟附加檔案

附加檔案若是.....

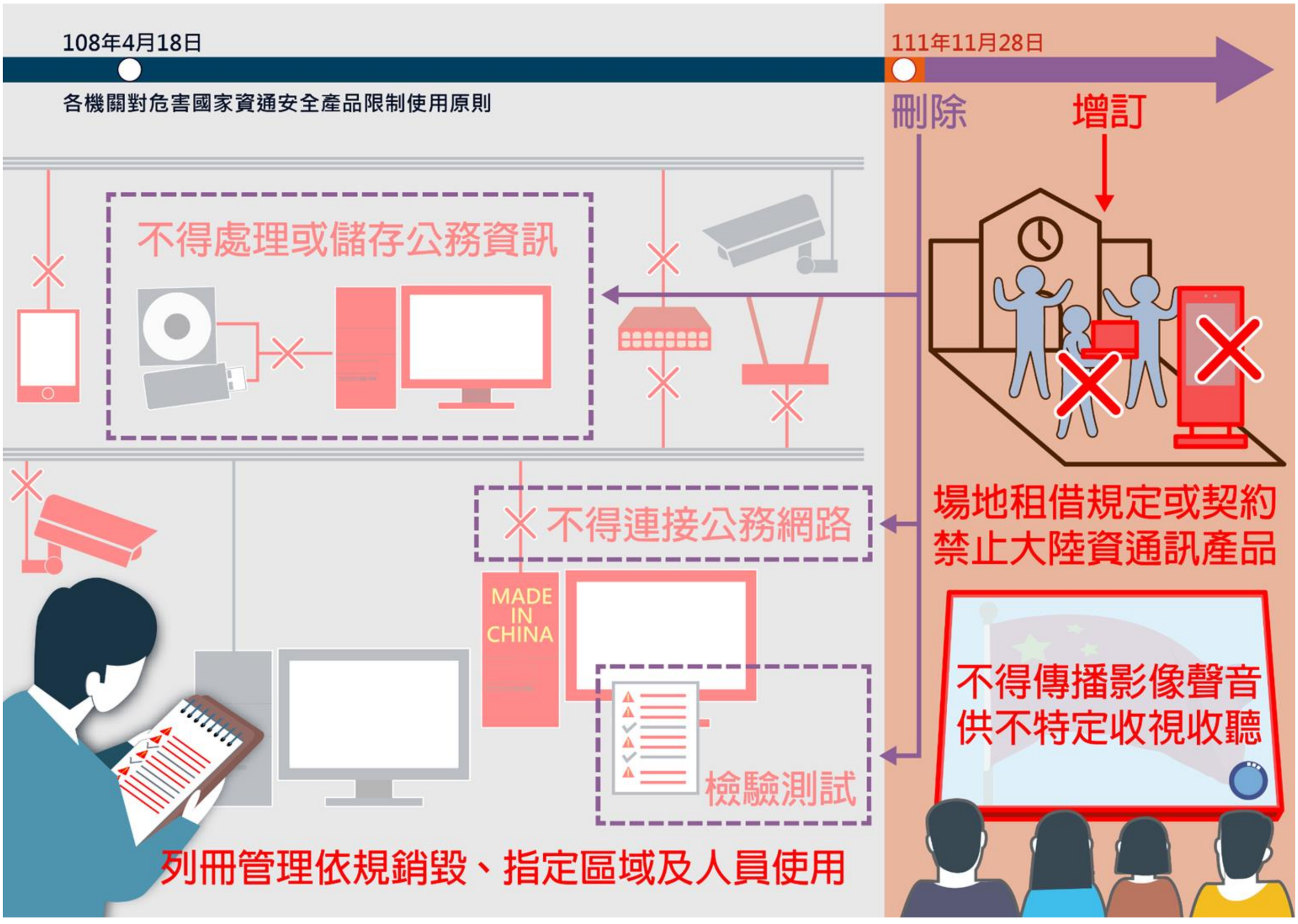
- 檔案名稱看起來不應該寄給我的
- 檔案名稱與信件內容不相關
- 署名某人來信，但應該不會寄這種檔案給自己啊!
- 除了副檔名.txt，任何檔案都有可能包藏惡意程式在內，有懷疑的話就開啟前先用防毒軟體掃描較保險。

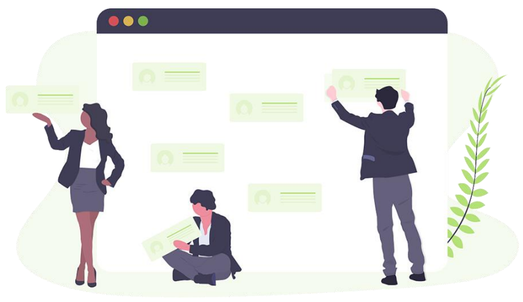
國立陽明交通大學　資訊技術服務中心　(03)5712121#31888



限制大陸製品

1. **不得採購及使用**主管機關核定屬**危害國家資通安全**之生產、研發、製造或提供之**廠商及產品**。 本校執行購案時，資通訊產品必須要求廠商在簽約時提供**無大陸製品(品牌)之切結書**。
2. 因業務需求且無其他替代方案必須採購或使用時危，應具體敘明理由，經資安長及上級機關資安長逐級核可，函報**主管機關核定**後，以專案方式購置。
3. 既有使用的危害國家資通安全產品，應**列冊管理**，且應**指定特定區域及特定人員使用**，且**不得傳播影像或聲音供不特定人士直接收視或收聽**，購置理由消失或使用**年限屆滿應立即銷毀**。
4. 各單位自行或委外營運，提供**公眾活動或使用之場地**，應將限制聲明納入**委外契約**或**場地使用規定**中，並督導辦理。





系統委外辦理

資通安全
實地稽核
第五大項

5.1 委外安全管理程序 選商/監督

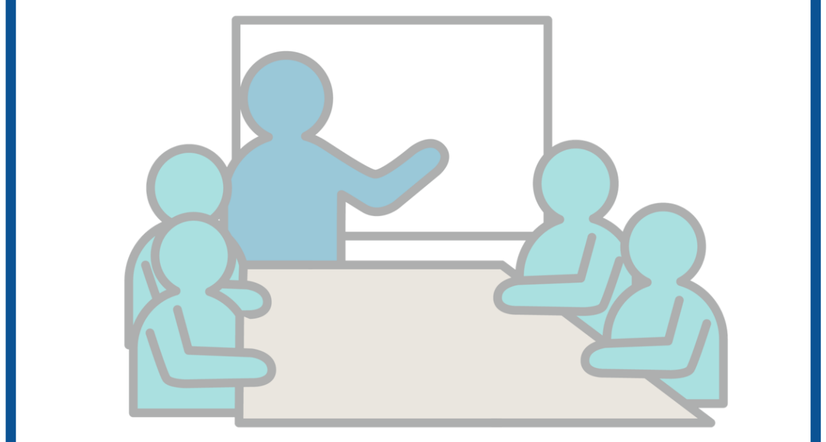
5.2 機關及委外廠商皆有PM

機關PM

廠商PM

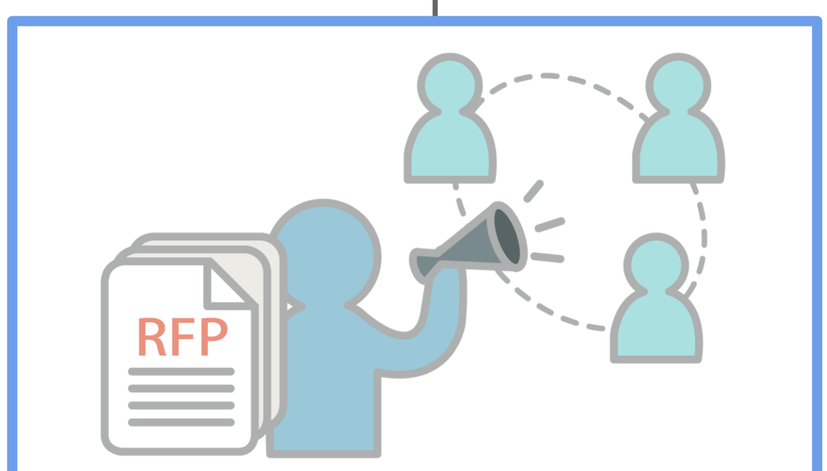
5.3 廠商ISMS人員

5.4 委外業務風險評估

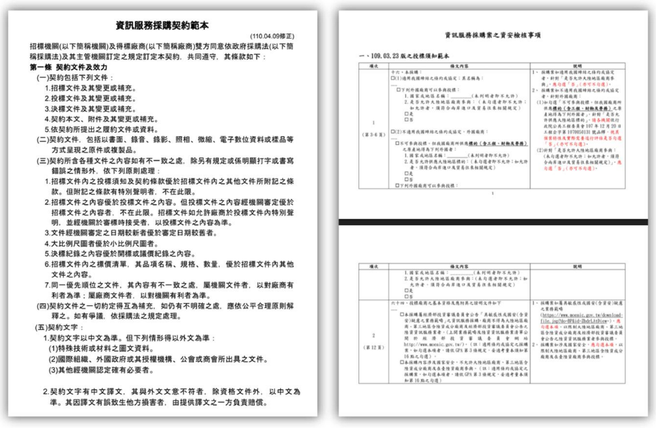


5.6 RFP規範防護基準

5.5 分(轉)包資安措施



5.7 廠商資安管理評估



資訊服務採購契約範本
(公共工程委員會)

資訊服務採購案之資安檢核事項
(行政院國家資通安全會報)

5.15 定期檢視人員媒體

5.11 資安責任保密規定

5.9 資安事件通報處理

5.12 定期或異常時稽核

5.13 廠商進出範圍限制

5.14 系統存取程序授權

5.8 系統安全檢測證明

5.10 委外關係終止解除 返還/銷毀

系統委外開發應知事項