*A01-003*

# 可攜式設備及儲存媒體安全管理

# 課程大綱

- 可攜式設備及儲存媒體介紹
- 安全管理
- 綜合整理
- 結論

# 第一章 可攜式設備及儲存媒體介紹

# 定義與特色-定義

**泛指重量輕盈，體積大小合宜而便於人類攜帶使用的電子資料處理或儲存設備，從手提電腦到電子計算機皆屬之，其最重要的特徵為:**

- 設計上便利於單一人員即可操作及攜帶的設備
- 無需長時間連接至主系統或電源設備

# 定義與特色-特色

- 輕巧，易於攜帶
- 增加工作效率，提高生產力
- 不受工作環境的限制
- 有利於大量資料的傳遞
- 有利資料傳遞的安全性
- 有益於資料的可用性(**availability**)

# 可攜式設備有哪些(1/7)

## 手提電腦

即一般所稱之筆記型電腦(notebook, laptop…)，同時具備運算、資料儲存、傳輸甚至燒錄功能、無線傳輸功能、記憶卡外接功能等等…多種功能。

# 可攜式設備有哪些(2/7)

## 次級手提電腦

即一般所稱之掌上型電腦，約為B5 size大小，仍具備筆記型電腦的大部分功能。

# 可攜式設備有哪些(3/7)

## Personal Digital Assistants

個人數位助理(PDA)，其體積較筆記型電腦小，功能也很強大，攜帶性與隱密性高，在合理使用下亦為具備效率的工具之一，具備了照相、攝影、無線網路傳輸等功能。而網路安全顧問也常使用PDA的高度攜帶性，進行線路檢測工作。

# 可攜式設備有哪些(4/7)

## 電子文字處理器

此類設備僅具備文字處理功能，例如藉由鍵盤輸入或語音輸入，而後轉化成文字儲存於記憶體中或列印成紙本文件，目前較為少見，但其仍可儲存資料。

# 可攜式設備有哪些(5/7)

## 電子書及電子速記本

電子速記本及平常所稱之平板電腦，其具備一般電腦的所有功能，但攜帶更方便。


# 可攜式設備有哪些(6/7)

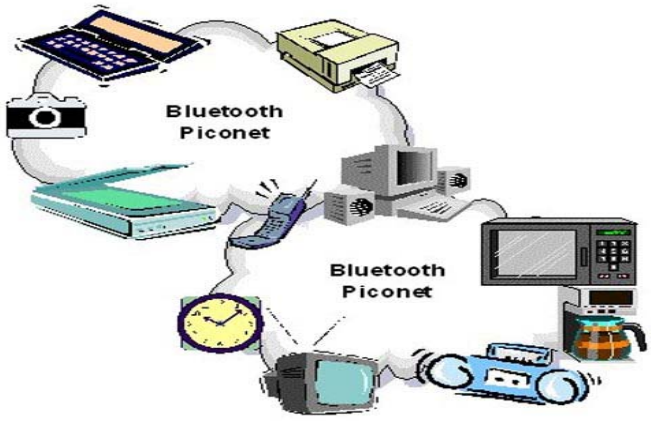
## 電子通訊設備(GPRS, WLAN, Bluetooth)

電子通訊設備種類廣泛，包含GPRS、PHS、3G手機、無線網路、藍芽產品、甚或未來發展熱門的WiMAX應用產品，擴充設備後即具有傳輸資訊的能力。

# 可攜式設備有哪些(6/7)


Compact Flash Card
GPRS
ANYCOM


Bluetooth
LINKSYS
Bluetooth USB Adapter


Bluetooth
Piconet
Bluetooth
Piconet

# 可攜式設備有哪些(7/7)

**其他週邊設備，如GPS...**

多半採用封閉式架構，不允許隨意儲存資料，具有供使用者查詢電子地圖、導航目前位置所在的功能。

# 可攜式儲存媒體有哪些(1/5)

所謂的可攜式儲存媒體泛指一般不具運算功能，但可儲存大量資料的小型資訊硬體，例如：外接式硬碟、燒錄機、隨身碟、數位相機記憶卡、MP3 player…等等。

# 可攜式儲存媒體有哪些(2/5)

外接式、抽取式、移動式硬碟

# 可攜式儲存媒體有哪些(3/5)

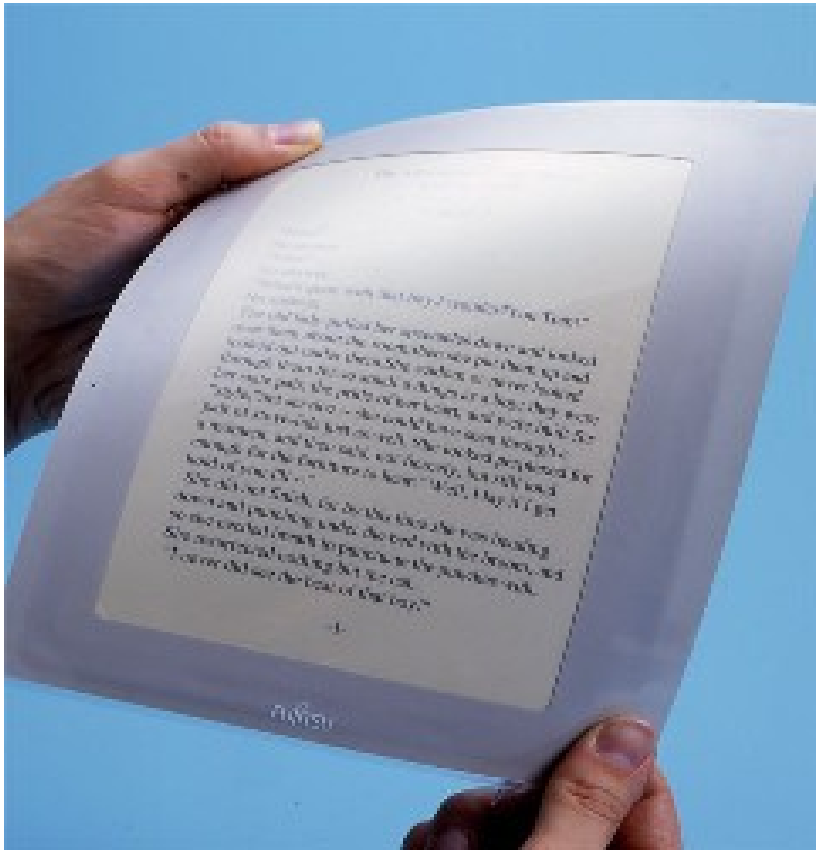
外接式光碟燒錄機

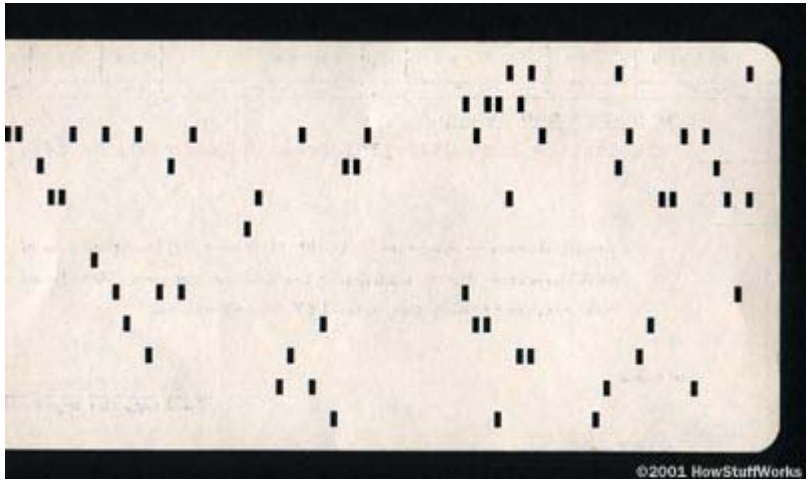
# 可攜式儲存媒體有哪些(4/5)

**USB、SD、CF 快閃存取記憶體**


# 可攜式儲存媒體有哪些(5/5)

## 其他可攜式儲存媒體

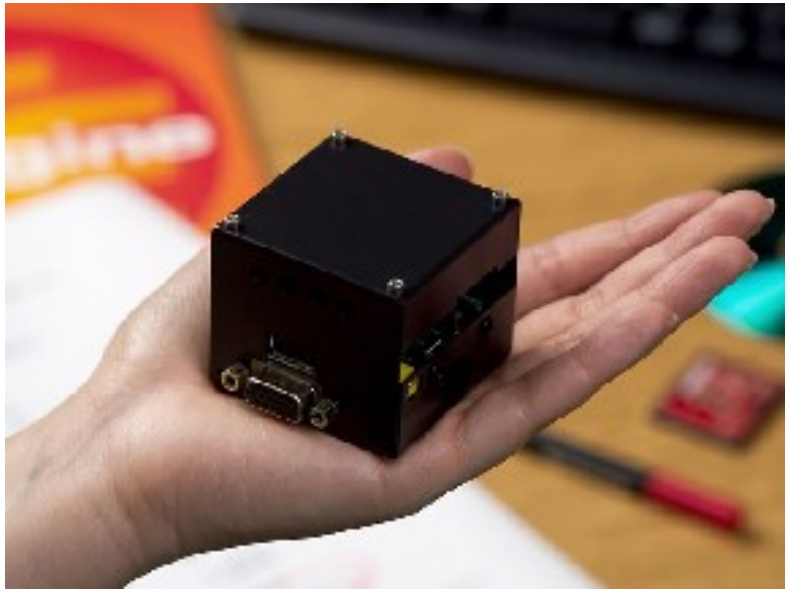




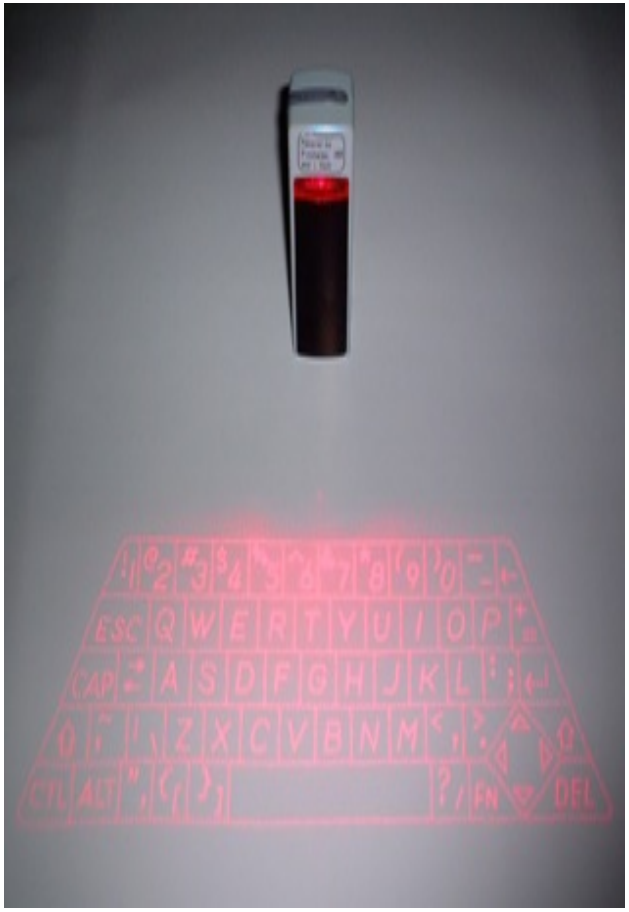
# 未來發展趨勢(1/5)

- 價格大幅降低，運算能力更強，使用將更為深入一般作業，也將更為普及於一般人
- 設計上將更趨於輕便，更易於攜帶
- 外觀及功能設計上與其他隨身用品結合(如**PDA**)
- 通訊能力將更為完備與並且成為標準配備
- 企業將大量使用可攜式設備，並安裝企業應用系統
- 資料承載的容量更高、傳輸速度更快、傳輸距離更遠
- 將解決可攜式設備的電力持續問題，而使運作的時間更長

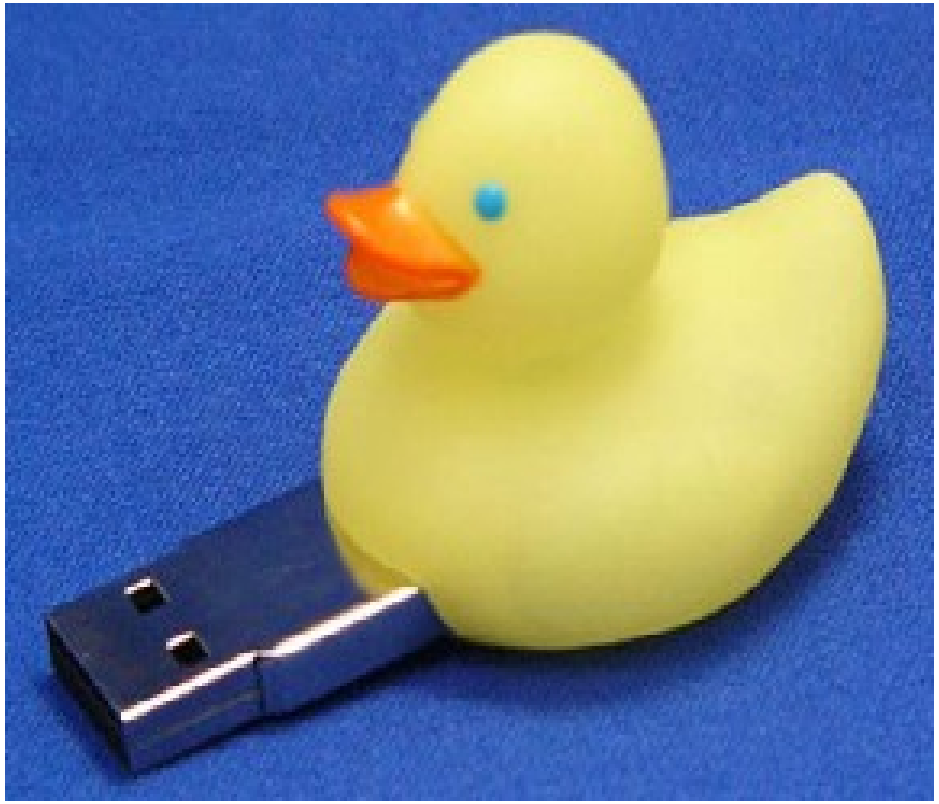
# 未來發展趨勢(2/5)

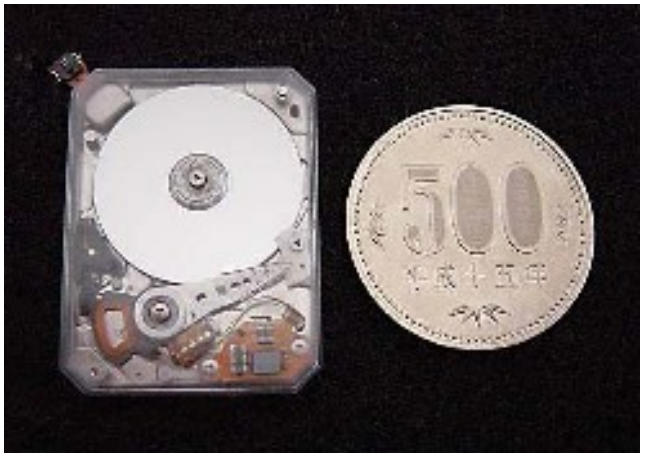
# 未來發展趨勢(3/5)



# 未來發展趨勢(4/5)



# 未來發展趨勢(5/5)

# 第二章 安全管理

# 威脅與風險-威脅

可攜式設備/儲存媒體與一般電腦設備所面臨的威脅大致相同，但卻比較容易被忽視，從過去發生的相關事例中，發現常見的威脅有下列:

- 病毒

  案例: 使用者將自家中或他處所下載已受電腦病毒感染的電子郵件或文件儲存於隨身碟，在不知情及未經掃毒處理的情況下，在公司電腦上使用，病毒透過公司內部網路散佈，癱瘓公司網路造成公司營運中斷。

- 惡意程式碼

  案例: 某高科技公司研發單位工程師將從國外軟體蒐集網站所下載內含木馬/後門程式的工具程式儲存於攜帶式硬碟，攜帶至公司使用，無意中啟動木馬/後門程式，重要的個人及機密研發資料在毫無警覺的情況下被傳遞出去，造成重大的研發資料外洩事件而遭解職。

- 不滿員工及有心人士

  案例: 某金融業員工因故遭公司解職，在離職之前，利用私自夾帶的攜帶式硬碟複製大量客戶敏感資料，交予將任職的同業競爭對手，被發現之後，面臨司法訴訟。

- 資料遺失

  因可攜式設備/儲存媒體的輕積較小，使用者往往稍一疏忽便會將其誤置而造成設備裏的資料遺失，無法取回。

- 硬體相容性

  因可攜式設備/儲存媒體常於不同的主機及不同的工作場合中使用，如果規格不相容，很可能會造成可攜式設備/儲存媒體的損害，而使資料毀損，最常見的是將可攜式設備/儲存媒體連結至較老舊的機器，因電壓不穩定而造成記憶晶片的毀損

- 非法軟體

  案例: 使用者將未經合法授權的商業軟體儲存於攜帶式硬碟，攜帶至公司並安裝於公司的個人電腦上使用，讓公司面臨侵犯智產權的法律風險

# 威脅與風險-風險(1/2)

- 因為其輕便性，易於毀損及遺失或遭竊。
- 外型設計多樣化，容易通過安全檢查，不易偵測
- 功能多樣化，在管理政策中難以定義，實際作業上不易杜絕員工使用。
- 某些可攜式設備週邊(紅外線及藍芽)及通訊功能設計上安全性保護不足，在公共場合使用時，易被有心人士失竊取資料或進行破壞。
- 存於可攜式設備及儲存媒體多數為重要或具機密性之資料，資產價值較高，容易成為有心人士竊取的目標
- 因資料的安全保護不足和使用方式不當，易被竊取、竄改、誤用損毀。
- 可攜式設備及儲存媒體常被共享使用，讓資料的不當存取及病毒擴散情形更為嚴重，甚至進入內部網路進行擴散。

# 威脅與風險-風險(2/2)

- 有心人士可利用技術或是外部可攜式設備，進入內部網路資源，進行不法或是竊取機密的活動
- 因不易杜絕使用，大量的機密資料容易被攜出
- 較新的作業系統提供了內建的驅動程式，讓具有USB隨插即用功能的可攜式儲存媒體能輕易的與內部系統連結下載資料
- 缺乏適當管制措施之下，有心人士可透過可攜式通訊設備將機密資料傳出
- 大多數可攜式設備及儲存媒體無法產生事件記錄，故無法追蹤其使用過程
- 可攜式設備和儲存媒體的使用，增加管理者在侵權軟體管制上的難度

# 制定管理政策(1/2)

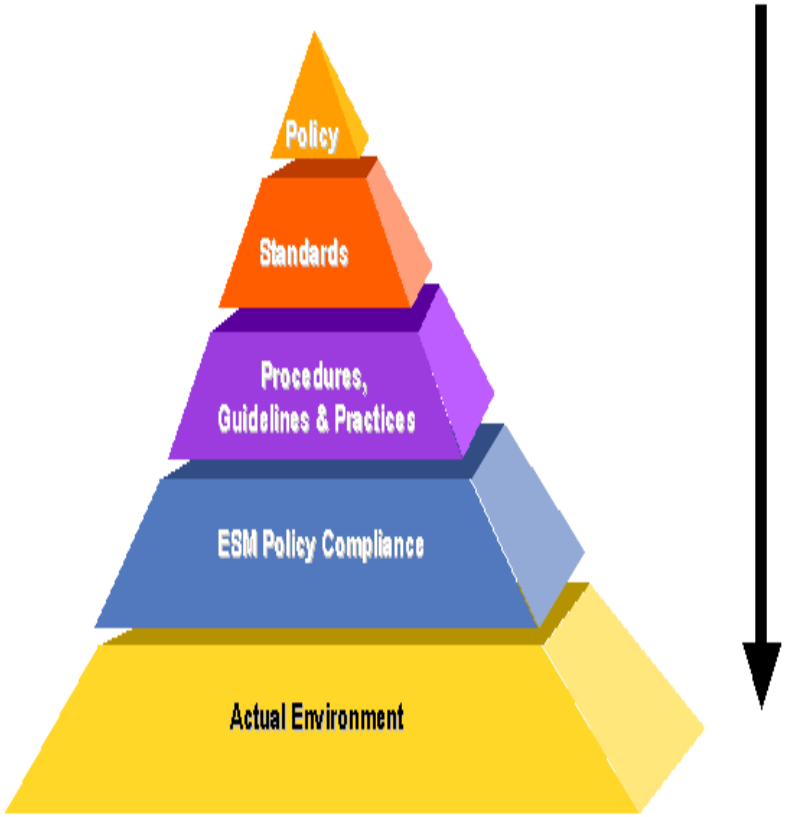
制定相關的安全政策，明確定義可攜式設備的使用規範及使用者的相關權責，並同時訂定誤用及濫用的罰則。

# 制定管理政策(2/2)

**制定可攜式設備或儲存媒體的管理政策，應考量到以下層面：**

- 組織政策層面，組織必須訂定明確的政策，告知同仁什麼樣的可攜式設備及儲存媒體可以使用或不可以使用，並且讓同仁瞭解應該遵守什麼規範。
- 人員認知教育層面，提升人員的資訊安全認知，使人員瞭解可攜式設備及儲存媒體的風險、因應對策及使用程序，避免可攜式設備及儲存媒體誤用濫用的情形發生
- 作業程序層面，藉由使用規則的制訂，要求使用者使用前申請、使用後檢查等程序，避免未經授權的可攜式設備及儲存媒體使用。
- 技術管制層面，利用資訊技術對可攜式設備及儲存媒體進行備份、管制及使用記錄，確保可攜式設備及儲存媒體均為授權內的使用，並確保其安全機制，以避免因遺失所造成的損害。

# 單位管理(1/2)




從圖來看可知---

- 政策的制訂最為重要，單位或組織沒有明確的政策，同仁將不知道如何遵循
- 訂定了政策之後，應該要告訴同仁什麼是被允許或什麼又是被禁止的，因此需要制訂規範標準
- 有了規範標準，負責的部門應該要制訂明確可行的程序，讓同仁瞭解並遵循如何去申請與使用
- 同仁依照程序申請與使用，組織又如何能知道同仁是否真的依照規範標準行事呢? 此時就必須靠技術方案來進行管制和監督，以確保每位同仁都確實遵循
- 將以上幾個層面確實執行，即能將資訊安全保護落實到實際的作業環境之中

# 單位管理(2/2)

**就高階管理者而言，制訂一個完整的政策，政策內容應該包含：**

- 哪些設備屬於可攜式設備和儲存媒體？哪些可攜式設備和儲存媒體可以被使用？
- 組織允許什麼樣的情形可以使用可攜式設備和儲存媒體？哪些資料可以被儲存在可攜式設備和儲存媒體？
- 使用前應該遵循什麼程序申請？
- 使用時應該遵循什麼規範？
- 使用後應該遵循什麼程序歸還？
- 使用者對於可攜式設備和儲存媒體的使用、保管和傳遞有什麼權責？
- 違反使用規範的時候有什麼樣的處罰？

# 如何制定作業流程

- 首先可先詢問同仁或檢視現行作業流程業務上是否有必要使用可攜式設備及儲存媒體，此時可請同仁分別列出使用與不使用的優缺點以供比較。
- 在確認何種業務活動需要使用可攜式設備及儲存媒體後，亦需確認各業務活動需要使用何種可攜式設備及儲存媒體。
- 確認以上兩點後，再來即需鑑別目前使用的方式、頻率、現有控管與風險為何。
- 在瞭解單位內可攜式設備及儲存媒體需要使用的目的、種類、方式、頻率、現有控管之後，我們需要考慮現行的方式是否具有風險。
- 如果尚有未能控管的風險存在，即需考慮我們需要增加什麼樣的控制措施。
- 最後，在決定單位內可攜式設備及儲存媒體需要使用的目的、種類、方式、頻率、現有控管及可接受風險後，徵詢高階主管、使用者部門、資訊、政風的意見，制訂合理的申請核准流程，並將流程文件化。
- 一個適合的流程例如：使用者使用可攜式設備及儲存媒體前需先經過申請，且資訊室資訊安全相關負責人員必須評估使用風險及確認使用者資訊環境安全性（例如：病毒碼及掃毒引擎是否已更新至最新版本、可攜式設備及儲存媒體內儲存之檔案是否經掃描確認無風險性)。
- 使用者使用可攜式設備及儲存媒體完畢後，必須確認儲存媒體內未含機密性資料，避免機密性資料因而外流，以確保資料安全性。若為公用之設備需立即歸還保管部門。

# 使用者管理-如何遵守管理制度面(1/2)

- 使用者在使用各式電腦資源及設備時，應先確實了解機關的資安政策或相關的資安管控規定
- 使用者在使用可攜式設備及儲存媒體時，首先應該確定此設備的使是否已被管理階層允許使用？如果不被允許，在任何情況下皆不可使用。
- 如果可攜式設備及儲存媒體的使用被允許，則使用者在使用前，首先應先考慮其使用是否為執行業務所必需，如非必需，請儘量避免使用，以降低可能的風險。
- 如果是業務上必須使用，則應考量所儲存及用於傳遞的資料是否具有機密敏感性，並依”行政院及所屬各機關資訊安全管理規範”或機關內文件分級所規定的處理方式來作處理。
- 切勿自機關辦公室電腦複製未經授權存取或與職務無關的文件資料。
- 如果是業務上必須使用，且所儲存或傳遞的資料具有機密敏感性，則所使用的設備應具備有身份驗證的功能(例如指紋辨識或帳號密碼登錄)或利用加密程式將重要資料予以加密。
- 應避免將具機密敏感性的資料長期置於可攜式設備及儲存媒體，定期檢視所儲存的資料內容，如有無須儲存於其上的重要資料，應立刻移除。
- 應該妥善保管相關設備與媒體，以免遺失、遭竊導致資料遺失。
- 若可攜式設備及儲存媒體上儲存有經常性使用之重要資料，使用者應養成定期備份的習慣，以免重要資料因設備的遺失、遭竊及毀損而無法使用。

# 使用者管理-如何遵守管理制度面(2/2)

- 使用者應定期自行檢視可攜式設備及儲存媒體裏的資料內容，如有來源不明的程式或資料及非法的軟體，應立刻進行移除及進行掃毒。
- 個人的可攜式設備及儲存媒體，如被允許使用，使用者在連接至辦公室設備之前，應先自行或委請資訊人員進行掃毒。
- 可攜式設備及儲存媒體如為機關內共同使用，使用者切記在使用完畢後將所有的資料文件移除，以免資料遭他人誤用。
- 當外部人員攜帶有可攜式設備及儲存媒體時，接待的人員應確切告知外部人員，機關在可攜式設備及儲存媒體上的相關資安規定，並依照辦理。
- 例如：委外廠商或別的單位的人員要進入內部辦公區域時，使用者要確認他們所攜入之可攜式設備及儲存媒體已經依機關資安規範予以適當的檢查與管制。
- 案例：某I資訊廠商人員為收發電子郵件，而在沒有經過單位的同意，單位同仁亦忘了先進行檢查或制止，就將其筆記型電腦私自接上該單位網路，結果因為筆記型電腦原已感染電腦病毒，導致病毒程式大量傳送垃圾訊息，導致該單位網路中斷48小時。
- 如果同仁或外單位人員有使用內部網路之需求時，應該主動填具申請表單，由所屬主管與資訊部門審核，而後再由資訊部門提供妥善的設備或透過適當之管制程序管控後，開放給同仁或外單位人員使用。
- 而同仁在使用可攜式設備及儲存媒體時，如果發現異常狀況發生（如發現有未經授權的使用、設備或媒體遺失等），應立即向主管進行通報，提早發現才能使損失降到最低。

# 使用者管理-如何配合技術方案

- **利用身分驗證技術來管制可攜式設備及儲存媒體上的資訊存取**
  - 同仁應設定複雜性密碼，使用者必須在帳號與密碼兩者能同時符合的情況下，才能被接受
  - 同仁可透過生物特徵辨識系統之身分驗證技術，包含包括指紋辨識系統、掌紋及聲紋辨識系統、電子簽字系統等等，以管制媒體之使用
- **利用加密技術來保護可攜式設備及儲存媒體裏的重要資料**
  - 同仁應妥善保存密碼，不可與他人共用密碼，以確保可攜式設備及儲存媒體內重要資料之安全性
- **病毒及惡意程式的掃描及清除工具**
  - 同仁應定期檢視病毒碼及掃描引擎是否更新至最新版本。
  - 例如：每天早上開機時，應自行確認防毒軟體的版本是否更新，一般常見的防毒軟體，其病毒碼版本更新頻率至少一個星期一次，如果沒有更新至近期的版本，即需由同仁手動更新或通知資訊人員。
  - 同仁應定期使用惡意程式掃描軟體進行系統掃描
- **使用資產管理和網路管理工具(硬體及軟體)**
  - 同仁應定期盤點部門或自身領用的可攜式設備及儲存媒體，確認是否存在與保管妥善，並配合資訊人員藉由資產管理工具產生的報表定期進行盤點對照。
- **備份機制的設計及技術使用**
  - 配合單位的備份要求及使用資訊人員設計之備份方式與工具進行備份作業，同時同仁應確認備份作業是否正常結束且備份是否可正常還原。
  - 例如：單位要求同仁需定期將可攜式設備及儲存媒體上的資料備份至檔案伺服器或個人電腦，且需不定期測試一下在檔案伺服器或個人電腦上的備份是否可使用。

# 使用者管理-使用者的自我管理(1/3)

- 所有同仁均應瞭解單位對「可攜式設備」的管理規定，瞭解什麼事情可以作、什麼事情不能作。
- 在使用可攜式設備時，應注意各項細節，多一分小心，就多一分安全。
- 例如：可攜式設備是否已經過掃毒，確認沒有病毒或木馬程式、機密性的資料不適合存放在可攜式設備內、可攜式設備不可以落單、若儲存機密資料於可攜式設備內時，應考慮予以加密保護。

# 使用者管理-使用者的自我管理(2/3)

**使用者層面可以從兩個角度來看，一是同仁必須主動參加相關訓練或是積極瞭解資訊安全的目標與要求。在瞭解組織訂定的資訊安全的目標與要求後，必須知道自己的責任是什麼，又當需要使用相關設備的時候，風險如何，使用的程序和方法如何。**

- 教育訓練的部分，同仁應該主動進修，瞭解資訊安全知識以及組織目標，例如參加教育訓練講座、外部訓練、線上學習等，以加強對資安的認知。
- 同仁應該要認識可攜式設備與儲存媒體的風險與控管方式，例如使用筆記型電腦或隨身碟的時候，常常是會在辦公場所、家裡兩邊輪流使用，而家裡電腦的防護措施通常較為薄弱，因此使用時極可能感染電腦病毒，所以當回辦公室接上內部網路時，極有可能將電腦病毒散播在組織內部，故組織多會要求設備禁止攜出使用或者當設備連接組織的電腦或網路時，需要經過檢查。
- 或者我們常常因為需要攜帶資料外出而使用可攜式設備與儲存媒體，但在使用完畢後卻忘了將資料刪除就交給下位同仁接續使用，甚至因為體積較小而遺失，此時即可能造成資料洩漏。

# 使用者管理-使用者的自我管理(3/3)

- 例如經常使用到的隨身碟或是辦公室公用筆記型電腦，因為洽公需要很常會將資料暫時存放在裡面，結果忘記刪除，也在無意之中讓其他非相關人士看到資料的內容。如果是有企圖的駭客，就可以利用這樣的機會將病毒種入電腦，或是竄改偷竊重要資訊，就可能會造成部門甚至整個組織的運作癱瘓和嚴重損失，因此同仁在使用後，應該自我進行檢查，確認設備裡面已經沒有存放資料後，才循程序將設備歸還。
- 例如因為設備的可攜性高，同仁在使用的時候可能因一時的疏忽而遺失或遭竊，這個時候除了資料或財產的損失之外，還有可能因此而發生資料洩漏的情事，因此同仁必須妥善保管相關設備，不使用時務必妥善收置，另外亦可使用加密機制，以避免萬一設備遭竊時，資料也同時洩漏的情形。
- 同仁必須隨時隨地注意自己的行為是否符合組織的規範，並且在使用前瞭解風險所在、在使用時確實遵守使用規範、在使用後進行自我檢查、保管與傳遞方式要注意安全、傳遞對象要確保正確無誤，如此即可確保使用可攜式設備和儲存媒體的安全了。

# 第三章 綜合整理

# 綜合整理(1/4)

- **引言**

  因為資訊科技的進步，可攜式設備和儲存媒體已經日漸普及於大家日常工作環境中。

- **可攜式設備的定義**

  課程中所提到的可攜式設備及儲存媒體，是指在重量上十分輕便，在體積也大小合宜，便於人類攜帶使用的各式電子資料處理或儲存設備。包括筆記型電腦、次級手提電腦、PDA、電子書、電子速記本等。

- **可攜式儲存媒體的定義**

  可攜式儲存媒體主要是指不具運算功能，但可大量儲存電子資料的小型硬體裝置，在工作環境週遭隨處可見。比如外接式抽取式硬碟，外接式燒錄機，或是隨身碟。

# 綜合整理(2/4)

- 可攜式設備和儲存媒體的發展趨勢
  - 價格大幅下降
  - 速度和容量等倍增加
  - 外觀將更多元化
  - 續電力問題改善，工作時間延長
  - 功能更加多樣化，結合其他產品 。
- 風險
  - 輕便性體積小，易因個人疏失遺失
  - 容易成為有心人士竊取目標
  - 遭到病毒或木馬程式攻擊
  - 成為竊賊盜取組織重要資料工具
  - 容易無意間產生侵權問題

# 綜合整理(3/4)

- **制定政策控管**

  為有效管理可攜式設備及儲存媒體，管理者必須制定相關的安全管理政策，並規劃相關的申請及管控流程，明確定義可攜式設備的使用規範及使用者的相關權責，並同時訂定誤用及濫用的罰則。

- **採用技術方案控管**

  應該使用技術方案來作適當的控管。例如監控網路或是電腦輸入輸出的監控。

# 綜合整理(4/4)

- **人員的自我管理**

  可攜式設備和儲存媒體的安全管理，光仰賴政策面及技術面是不夠的，使用者本身的自我管理才是讓可攜式設備及儲存媒體的安全管理落實的最重要關鍵。

- **了解並遵守組織規範**

  使用者應該主動 了解組織資安政策要求、遵循事項和細則 。

- **主動告知外部人員資安規範**

  使用者也應該主動告知外部人員相關規定和要求。

# 第四章 結論

# 結論

- 單位應審慎評估可攜式設備及媒體之風險。
- 管理者須制定可攜式設備的使用規範及相關權責。
- 使用者配合執行單位內制定的管理制度並加強自我管理。
- 資訊安全的維持靠全體同仁一起努力。