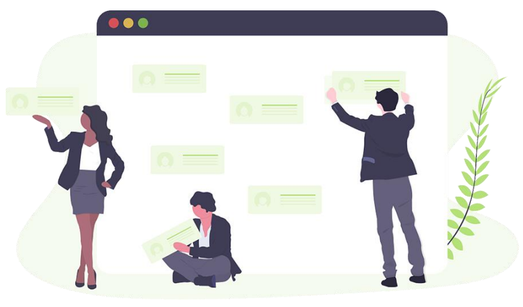
# 臺中市立大道國民中學

# 資安宣導

1. 資安宣導：密碼換新、程式更新、下載要當心。
2. 辦公環境內必須使用機關提供之資訊設備、網路，及規定之軟體，不得使用個人私有設備及中國廠牌產品，公務設備亦不得連結個人私有手機上網。若有業務上的需求，必須經資安長同意後，列冊管理並定期檢討。
3. 上班期間不應連結非公務需要之網站，並避免連結惡意網站或釣魚網站，如發現異常連線，請通知資安窗口。
4. 不得使用公務電子信箱帳號登記做爲非公務網站的帳號，如社群網站、電商服務等。
5. 公務資料傳遞及聯繫必須使用公務電子郵件帳號（如：@ddjhs.tc.edu.tw、@st.tc.edu.tw、@tc.edu.tw），不得使用非公務電子郵件（如：@gmail.com、@yahoo.com.tw、@pchome.com.tw）傳送或討論公務訊息。
6. 即時通訊軟體（Line、Facebook、Message）使用應注意不得傳送公務敏感資料。
7. 傳送公務資訊應有適當保護，如：加密傳送、檔案加密、檔案壓縮加密…。
8. 帳號密碼必須妥善保存，並遵守機關規定，如有外洩疑慮，除儘速更換密碼外，並應通知資安窗口；密碼設置應包含英文大小寫、數字、特殊符號…。
9. 應主動通報資安事件或可能資安風險。未遵守機關資安規定，初次予以告誡，若持續發生或勸導不聽者，依規定懲處；若因而發生資安事件，加重處分。
10. 有資安疑慮或異常時，應即時通報資安窗口。
11. 應遵守個人資料保護法及資通安全管理法。
12. 資安訊息網址： https://reurl.cc/2gzv9E

、本校資安通報窗口 資訊組長：蔣翔能 (04)26992028#713.

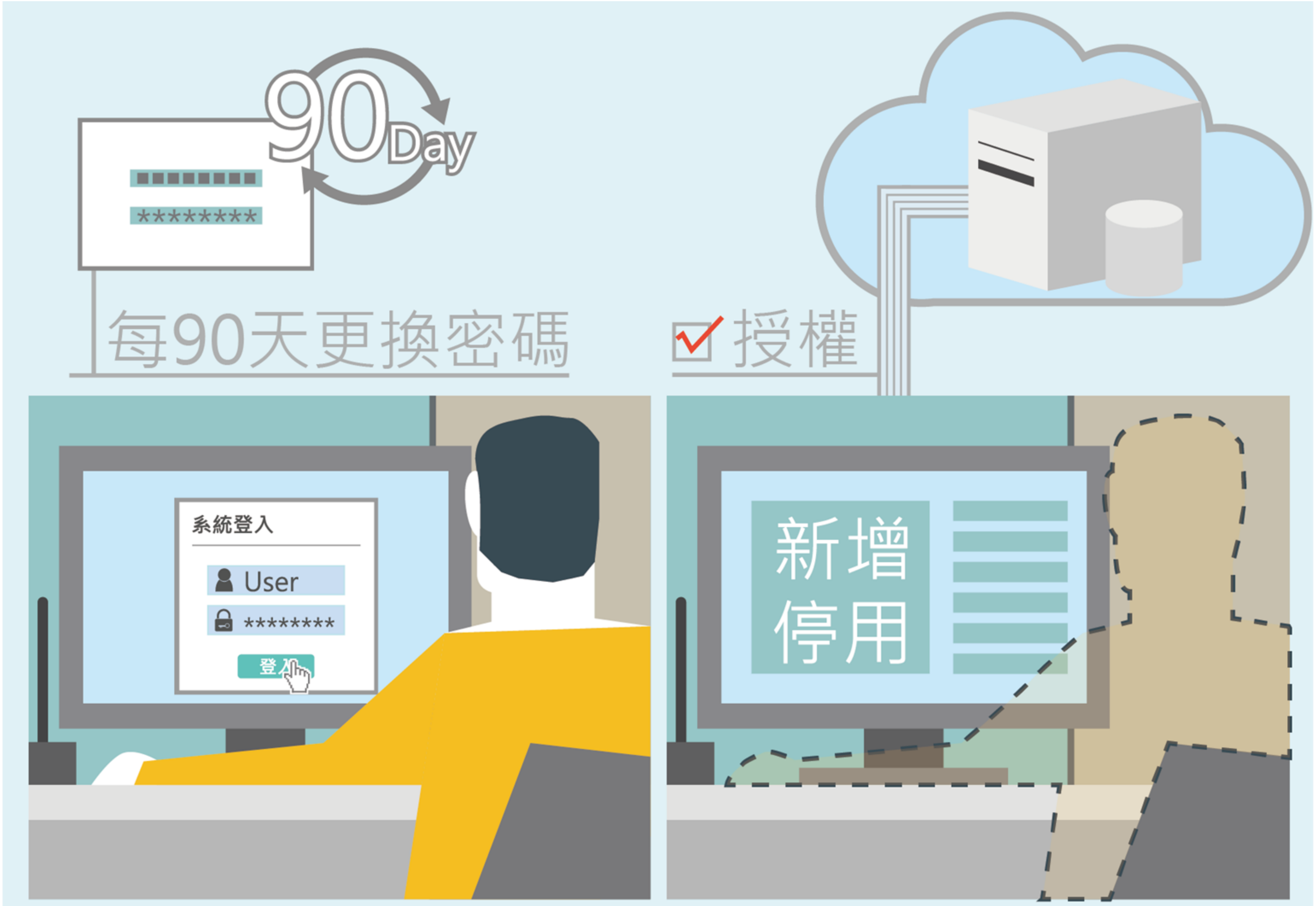


# 資訊資產分類

1. 人員(People)：包含全體同仁，以及委外廠商。
2. 文件(Document)：以紙本形式存在之文書資料、報表等相關資訊，包含公文、列印之報表、表單、計畫等紙本文件。
3. 軟體(Software)：作業系統、應用系統程式、套裝軟體等，包含原始程式碼、應用程式執行碼、資料庫等。
4. 通訊(Communication)：網路設備、網路安全設備、提供資訊傳輸、交換之線路或服務。
5. 硬體(Hardware)：主機設備等相關硬體設施。
6. 資料(Data)：儲存於硬碟、磁帶、光碟等儲存媒介之數位資訊。
7. 環境(Environment)：相關基礎設施及服務，包含辦公室實體、實體機房、電力、消防設施等。

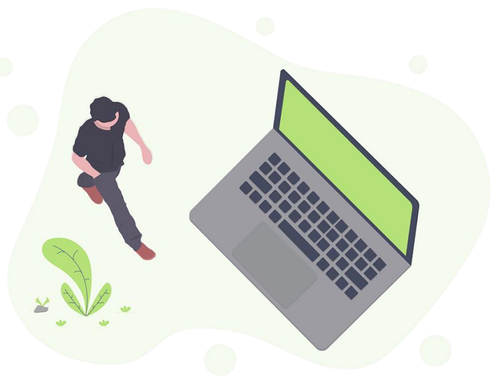
# 系統通行碼管理

1. 資通系統應設置通行碼管理，通行碼要求需滿足：
   (1)通行碼長度 8碼以上。
   (2)通行碼複雜度應包含英文大寫小寫、特殊符號或數字三種以上。
   (3)使用者每90 天應更換一次通行碼。
2. 使用者使用資通系統前應經**授權**，並使用唯一之使用者ID，除有特殊營運或作業必要經核准並記錄外，**不得共用ID**。
3. 使用者無繼續使用資通系統時，應立即*停用或移除*使用者ID，資通系統管理者應**定期清查**使用者之權限。



# 加密管理

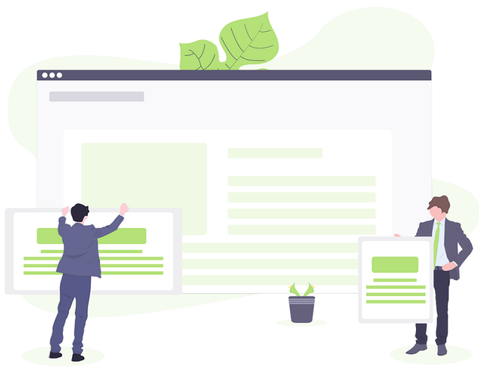
1. 學校之機密資訊於儲存或傳輸時應進行加密。
2. 學校之加密保護措施應遵守下列規定：
   (1) 應落實使用者更新加密裝置並備份金鑰。
   (2) 應避免留存解密資訊。
   (3) 一旦加密資訊具遭破解跡象，應立即更改之。



# 防範惡意軟體

1. 學校之主機及個人電腦應安裝<u>防毒軟體</u>，並時進行軟、硬體之必要<u>更新或升級</u>。
   (1)經任何形式之<u>儲存媒體</u>所取得之檔案，於使用前應<u>先掃描</u>有無惡意軟體。
   (2)<u>電子郵件附件及下載檔案</u>於使用前，宜於他處<u>先掃描</u>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<u>不得私自安裝應用軟體</u>，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<u>不得私自使用已知或有嫌疑惡意之網站</u>。
4. 設備管理者應定期進行<u>作業系統及軟體更新</u>，以避免惡意軟體利用系統或軟體漏洞進行攻擊。


、本校資安通報窗口 資訊組長：蔣翔能 (04)26992028#713.



# 電子郵件使用

1. 使用者使用電子郵件服務時，**不得**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，導致**他人權益受損**。
2. 使用者使用電子郵件服務時應**尊重智慧財產權**，不得有違法傳送或侵害他人智慧財產權之行為。
3. 使用者辦理**公務、及重要(或敏感)專案**使用之電子郵件信箱(可規劃專用電子郵件信箱)，不**得轉至外部私人信箱**收發公務資訊。
4. 使用者使用電子郵件服務時，應**尊重網路隱私權**，不得任意窺視其他使用者之個人資料或有其他侵犯隱私權之行為。**不得**盜用他人或系統資源，或**以任何方式影響系統正常運作**。
5. 使用者使用電子郵件服務時**不可作為商業用途**。
6. 教職員如**轉任或借調**至公務機關服務者，**不得使用學校電子郵件信箱**收發公務機關相關電子郵件。



.本校資安通報窗口 資訊組長：蔣翔能 (04)26992028#713.

# 辦公室實體安全

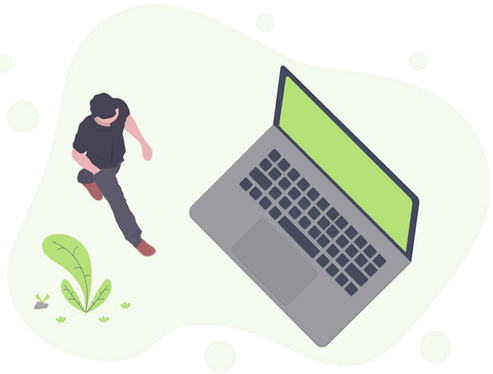
1. 應考量採用辦公桌面的淨空政策，以減少文件及可移除式媒體等在辦公時間之外遭未被授權的人員取用、遺失或是被破壞的機會。
2. 文件及可移除式媒體在不使用或不上班時，應存放在櫃子內。
3. 機密性及敏感性資訊，不使用或下班時應該上鎖。
4. 機密資訊或處理機密資訊之資通系統應避免存放或設置於公眾可接觸之場域。
5. 顯示存放機密資訊或處理機密資訊之資通系統地點之通訊錄及內部人員電話簿，不宜讓未經授權者輕易取得。
6. 資訊或資通系統相關設備，未經管理人授權，不得被帶離辦公室。



.本校資安通報窗口 資訊組長：蔣翔能 (04)26992028#713.

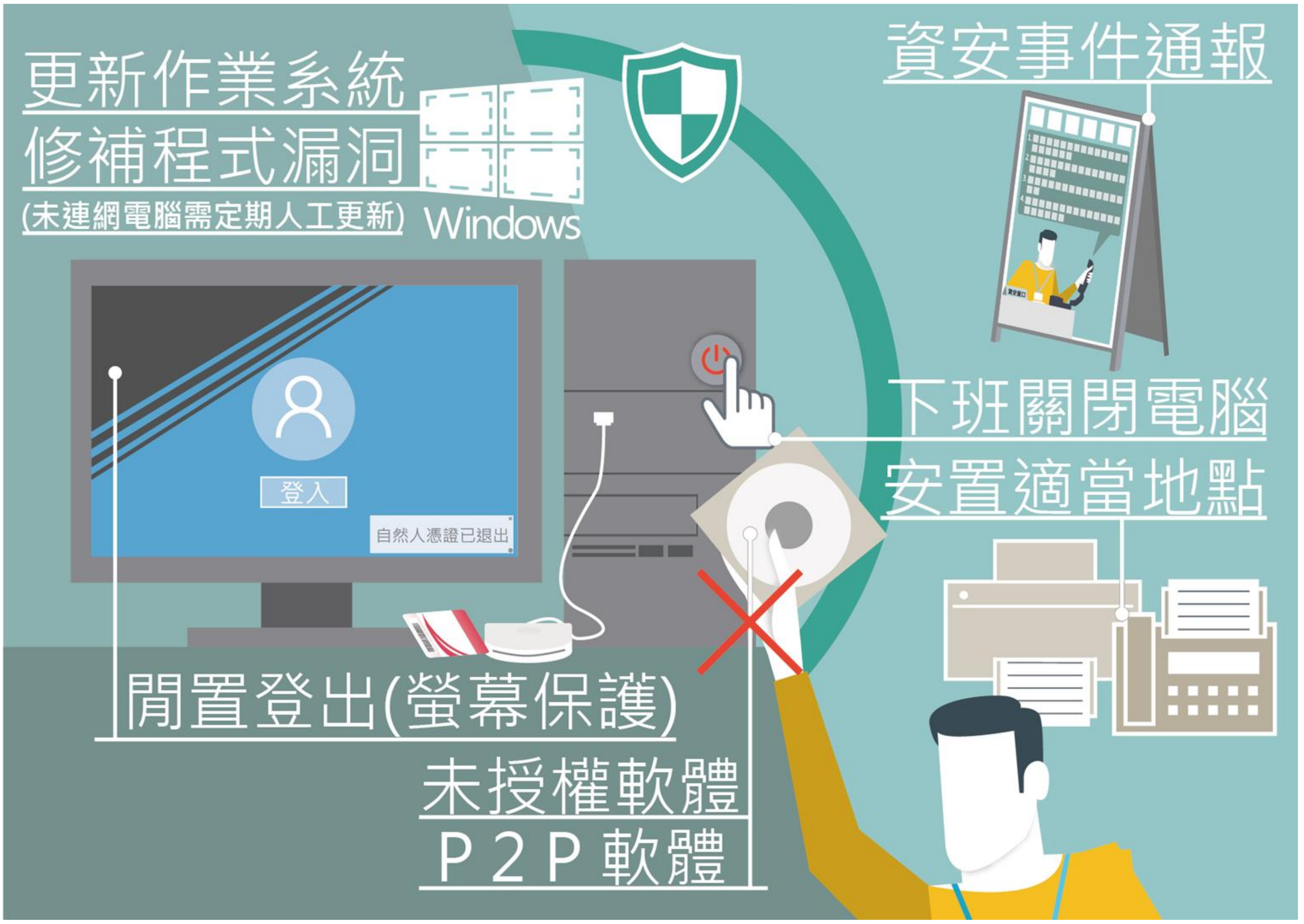
# 媒體防護措施

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. 爲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。



# 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*或啓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、傳眞機等，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。





本校資安通報窗口 資訊組長：蔣翔能 (04)26992028#713.

# 行動設備安全

1. **機密資料**，不得由**未經許可之行動設備**存取、處理或傳送。
2. **機敏會議或場所**，**不得攜帶未經許可之行動設備**進入。


、本校資安通報窗口 資訊組長：蔣翔能 (04)26992028#713.