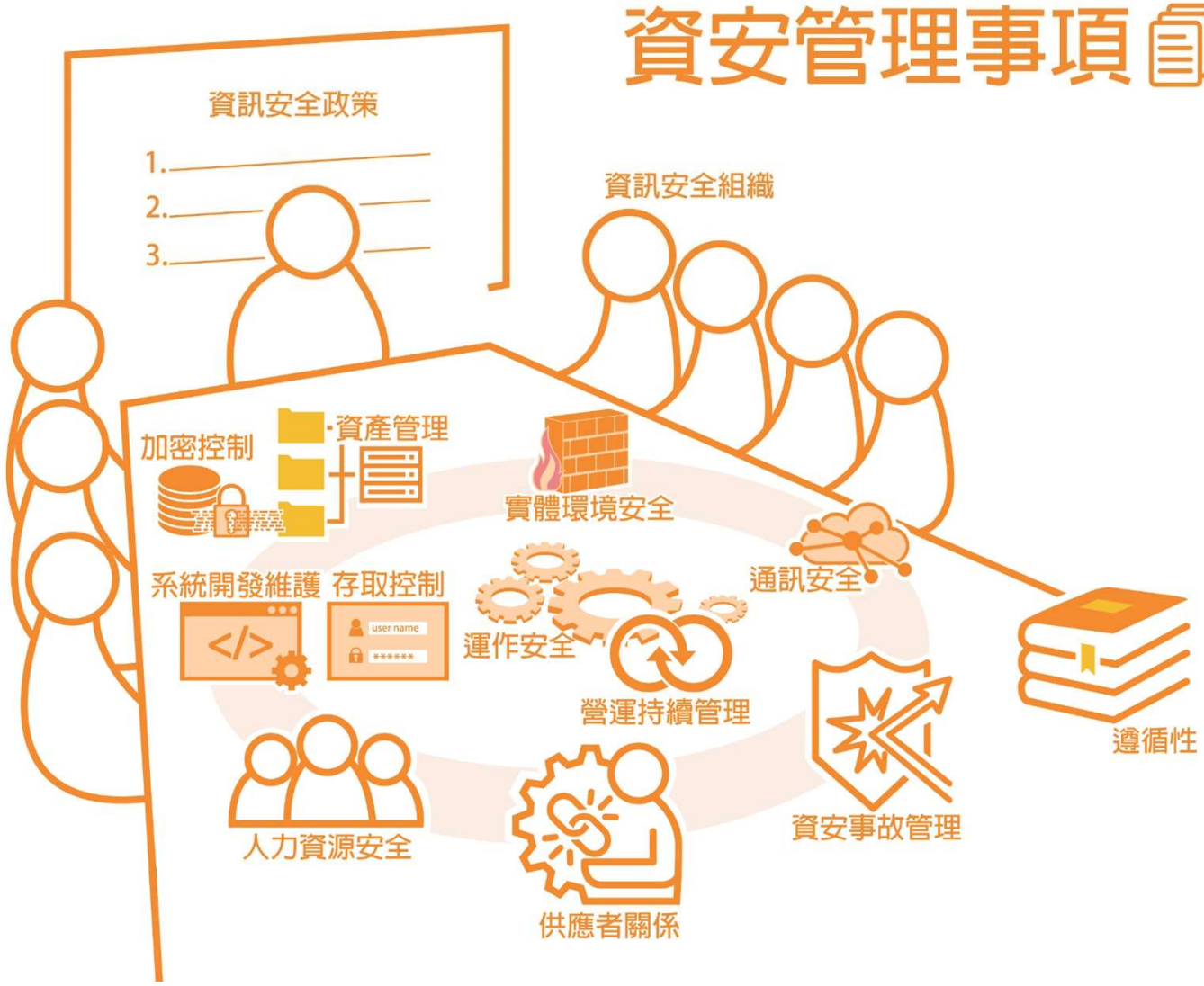
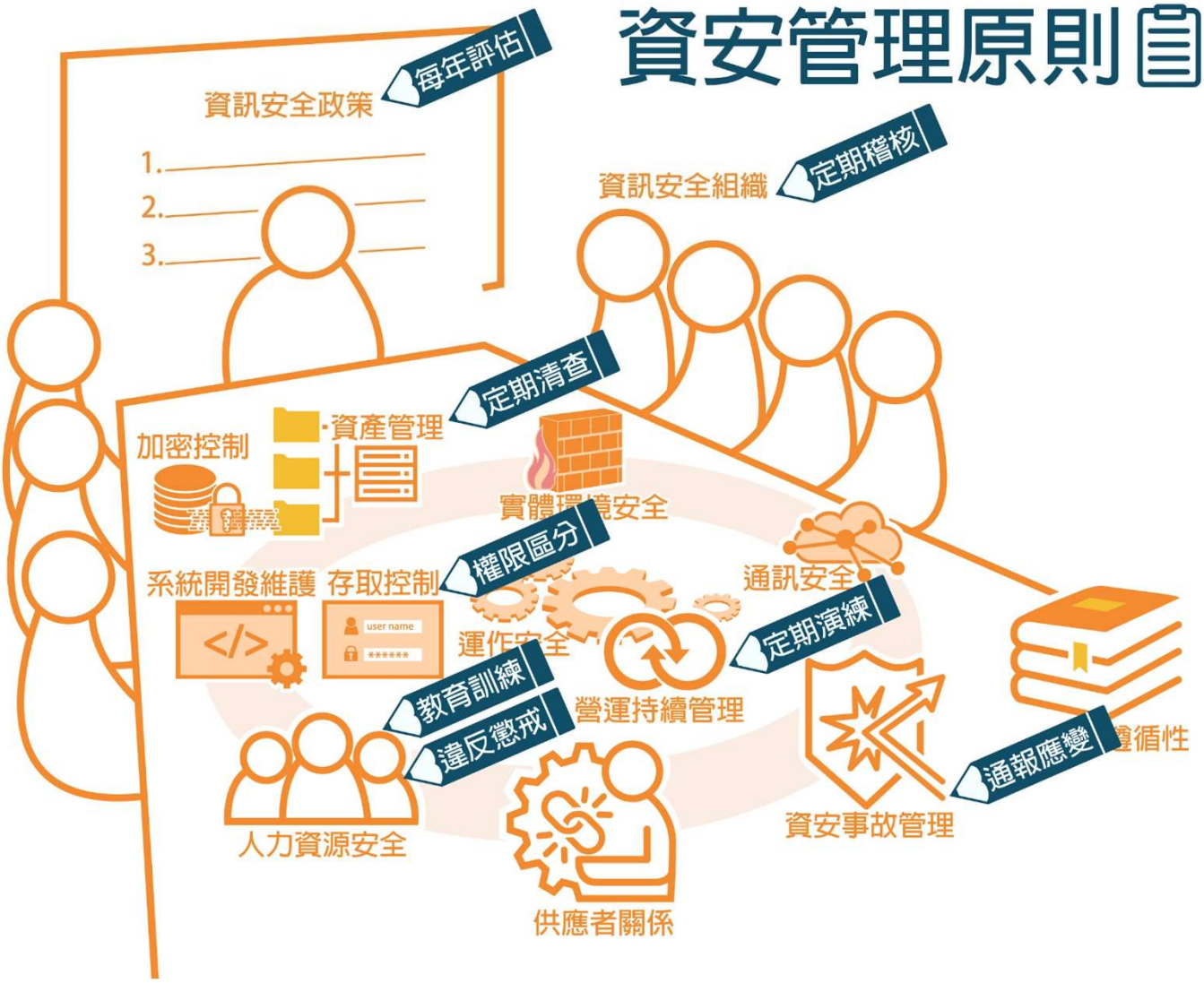
# 資安管理事項




1. 資訊安全政策
2. 資訊安全組織
3. 人力資源安全
4. 資產管理
5. 存取控制
6. 密碼學(加密控制)
7. 實體與環境安全
8. 運作安全
9. 通訊安全
10. 資訊系統取得、開發及維護
11. 供應者關係
12. 資訊安全事故管理
13. 營運持續管理之資訊安全層面
14. 遵循性

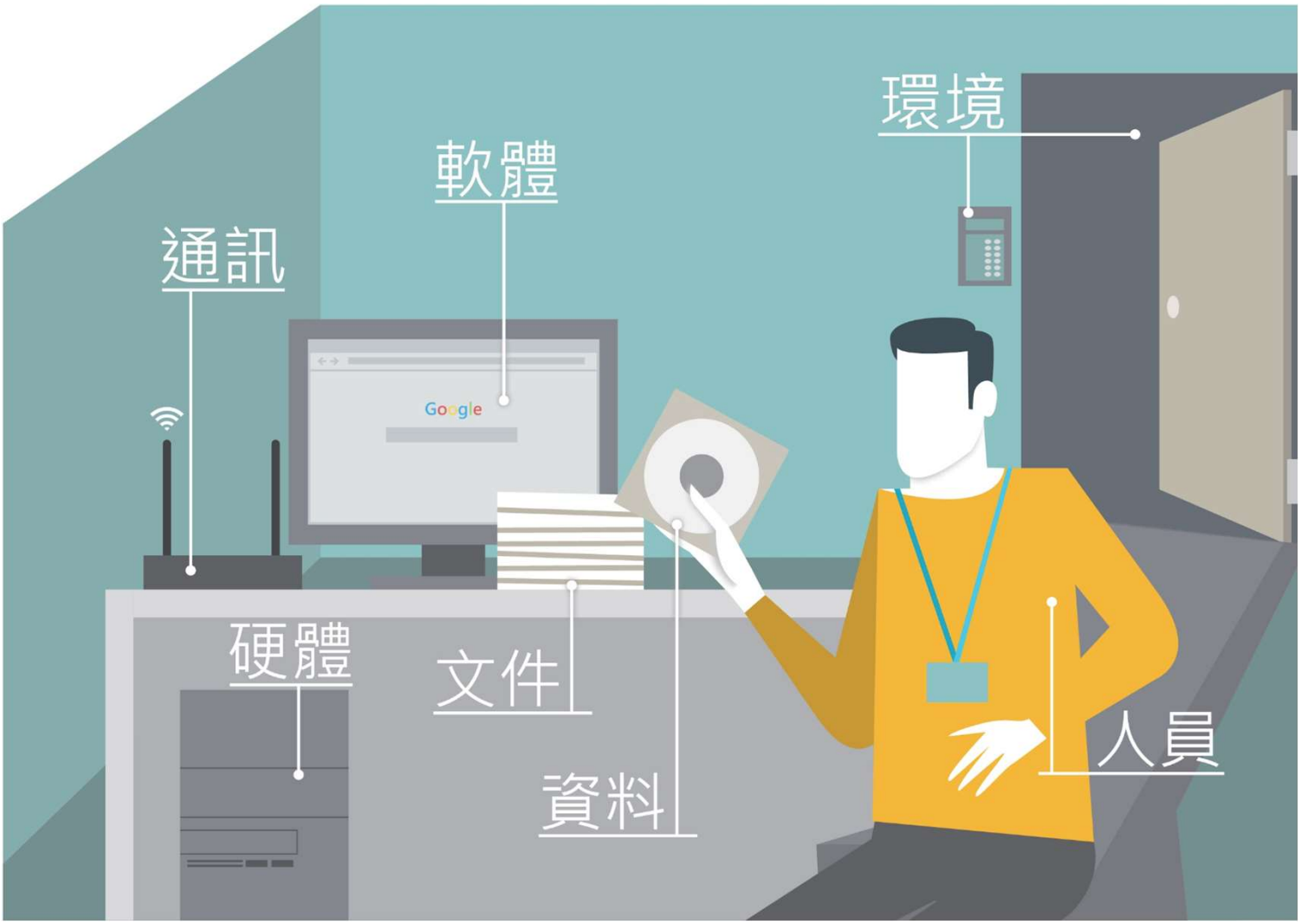
# 資安管理原則




1. 重要之資訊資產應**定期清查**、分類分級與進行風險評鑑，並據以實施適當的防護措施。
2. 重要資訊資產存取**權限**應予以**區分**，考量人員職務授予相關權限，必要時得採行加解密(例rar)及身分鑑別機制，以加強資訊資產之安全。
3. 對於資訊安全事件須有完整的**通報**及**應變措**施，以確保資訊系統、業務的持續運作。
4. 應訂定營運持續計畫並**定期演練**，以確保重要系統、業務於資安事故發生時能於預定時間內恢復作業。
5. 相關人員應依規定接受資訊安全**教育訓練**與宣導，以加強資訊安全認知。
6. **定期**執行資訊安全**稽核**作業，檢視存取權限及資訊安全管理制度之落實。
7. **違反**本政策與資訊安全相關規範，依相關法規或本校**懲戒**規定辦理。

# 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。



# 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**，並制定相關規定以維護其安全。
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. 對於本校圖書暨資訊處管理之資訊及資通系統，遵循規定確保與資訊處理設施相關的資訊資產加以適切的分類分級，並界定與定期審查資訊資產機密等級與存取限制，以及考量可適用的存取控制政策。

# 防範惡意軟體

1. Windows作業系統之主機及個人電腦應**安裝防毒軟體**，須安裝至最新之**修補程式及病毒碼**，並即時修補相關安全漏洞。如需使用外來的**可攜式設備或媒體**，應確認設備未遭受病毒感染。**電子郵件**須先經過防毒軟體掃描，並禁止開啟來路不明之檔案或電子郵件及其附加檔案，以避免遭受病毒攻擊。正確配置**瀏覽器之安全設定**，建議設定在中級風險等級(含)以上。
2. 為有效控制「**免費軟體**」或「**共享軟體**」的使用，使用人員須事先瞭解其相關版權規定，並且不得任意自行安裝及散佈未經授權之軟體。
3. 不得私自使用已知或有嫌疑惡意之網站。

# 電子郵件使用

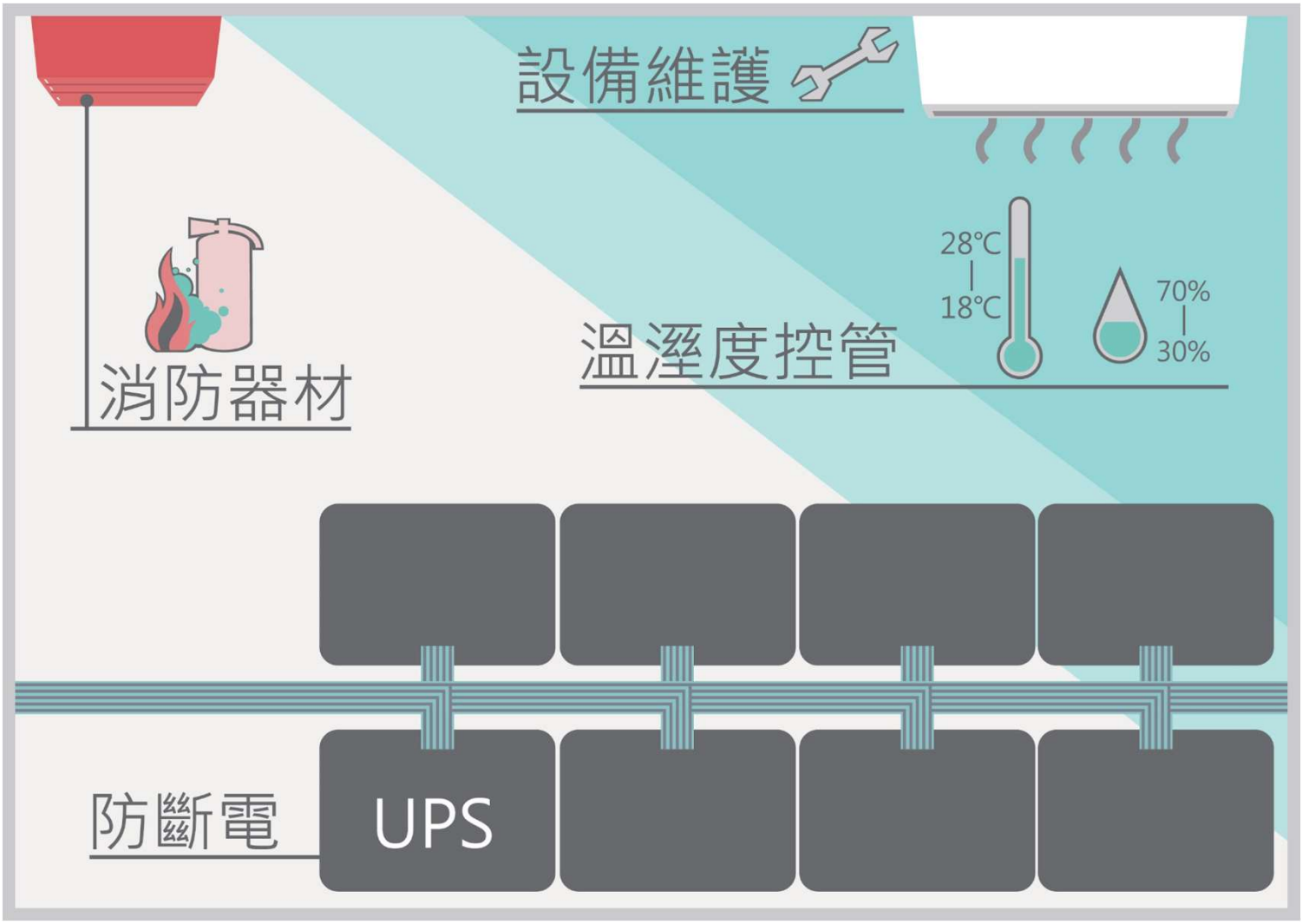
1. **密等**以上的公文不得以電子郵件傳送。
2. 含有**個人資料**之信件必須**加密**傳送。
3. 電子郵件**加簽**以避免發送匿名或偽造。
4. **不得**利用公務電子郵件進行**侵害他人權益、違法**之行為。(包括以電子郵件大量傳送廣告信、連鎖信或無用之信息，或以灌爆信箱、掠奪資源等方式。以電子郵件、線上互動或類似功能之方法散布詐欺、誹謗、侮辱、猥褻、騷擾、非法軟體交易或其他違法之訊息。)
5. 訂「**校園網路使用規範**」，納入電子郵件使用限制相關條文。

# 實體環境安全

1. 為確保設備及資料之安全，應採用**有身分識別功能之安全門**，做為必要之安全控管。
2. 除機房管理人員外，其他因業務需要進入電腦機房作業時，應由機房管理人員陪同進入並於「電腦機房進出管制登記簿」上**登記**。
3. 內部人員於進出時應隨時注意是否有**非經授權人員**跟隨進入。
4. 外部人員或委外人員應配帶原公司所製發之**員工證或相關證明**，並應於指定環境內執行作業。
5. **門禁系統之進出記錄**應定期備份、審閱；記錄存放於安全區域並保存一年備查。

# 實體環境安全

1. 應保護設備免於**電源**失效，及因其他支援之公用服務事業失效，所導致之中斷。
2. 電腦機房**溫濕度**採固定區間控制，溫度應維持在18℃至28℃，相對溼度維持在30%至70%。
3. 電腦機房應設置專用之**消防**器材或系統，如熱感應、煙霧偵測、火災警報、滅火設備、火災逃生設備等，同時應符合相關法規並定期檢測、記錄。
4. 電腦機房維運設備(如消防、電力、空調設備等)或重要資訊設備(如主機、網路設備等)應與合格專業廠商簽訂**維護合約**，定期實施保養與妥善維護，以確保設備的完整與安全。

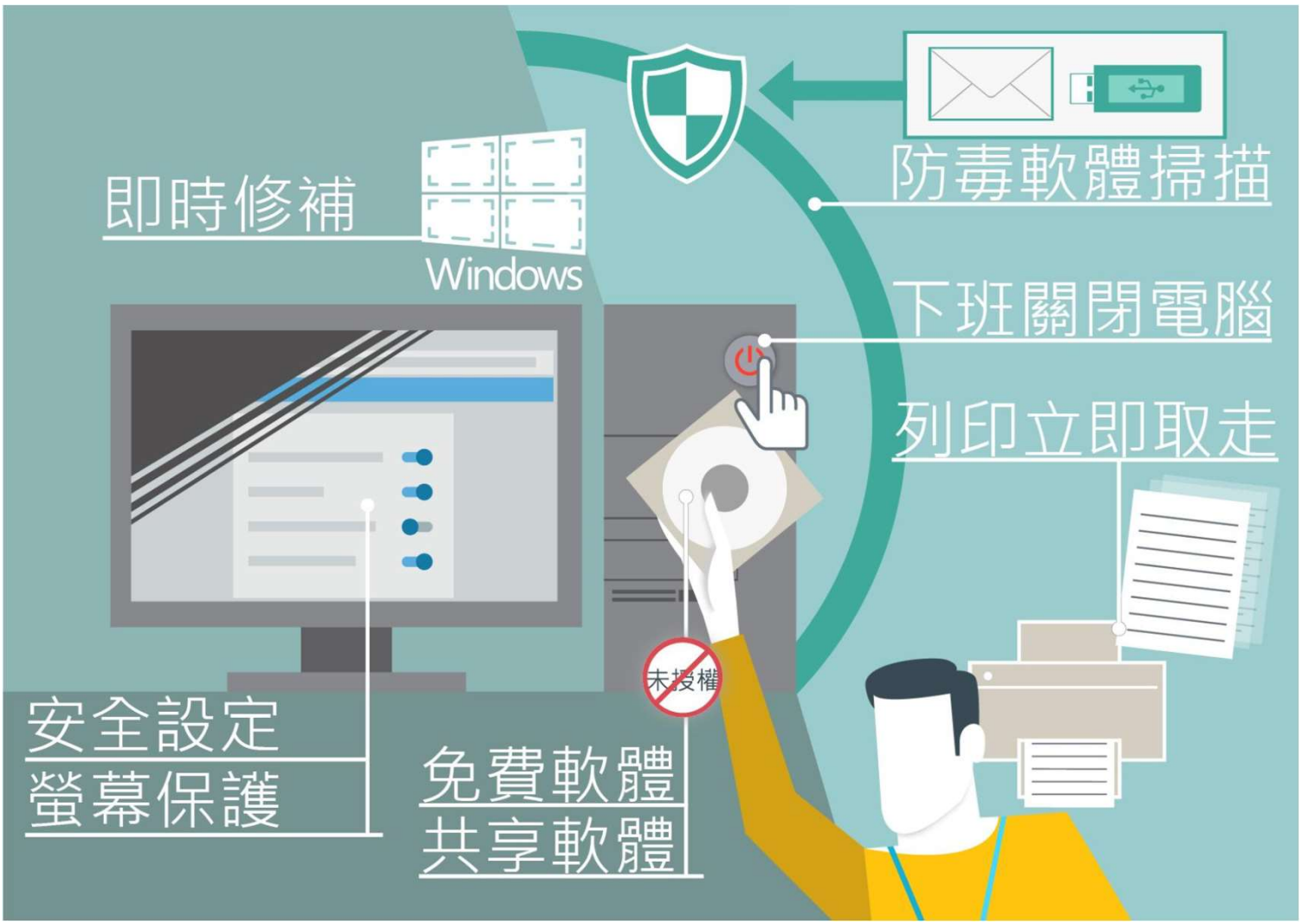


# 實體環境安全

1. 依據桌面淨空與螢幕淨空安全控管規定，應實施**桌面淨空**，重要文件應妥善保管。
2. 依據可移除式媒體的管理規定，將機密資料存放於**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，**密級、限制使用、內部使用**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。

# 電腦使用安全

1. 本校同仁應遵循桌面淨空與螢幕淨空安全控管規定，個人電腦、伺服器或主機應設定**螢幕密碼保護程式**，下班時應**關閉**不需使用之個人電腦。
2. 本校同仁應遵循軟體安裝之限制，為有效控制「**免費軟體**」或「**共享軟體**」的使用，須瞭解其相關版權規定，並且**不得任意安裝及散佈未經授權軟體**。
3. 本校同仁應遵循防範惡意軟體規定，Windows主機與個人電腦皆須安裝**防毒軟體**。
4. 本校同仁應遵循運作中系統之軟體安裝規定，主機系統、網路設備、軟硬體常更新**修正程式**。
5. 本校同仁應遵循保全之辦公室、房間及設施規定，**列印後應立即將資料取走**。



# 行動設備安全

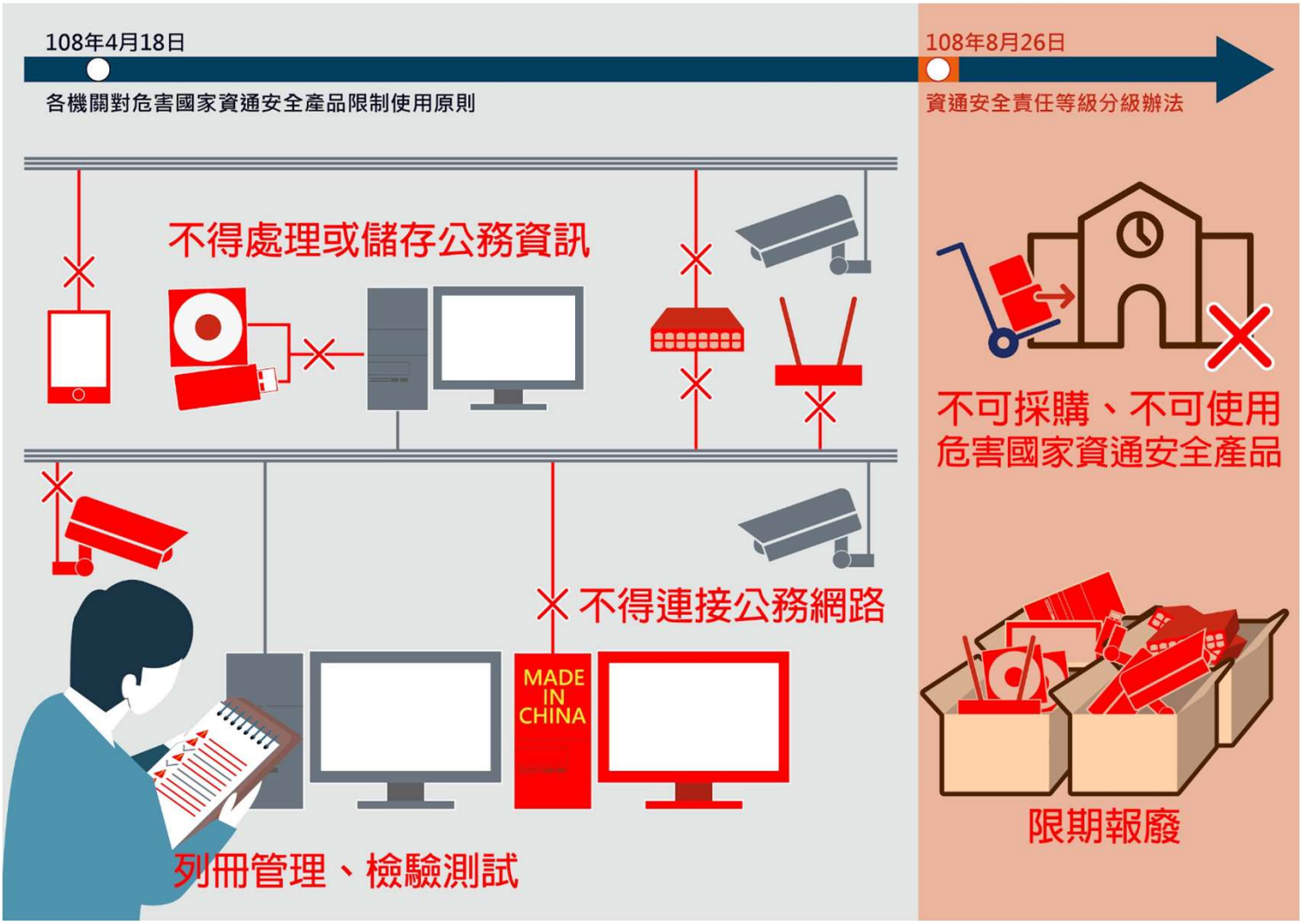
1. 本校同仁應遵循「可攜設備管理辦法」管理規定，使用**可攜式設備與媒體**時，應謹慎防範資訊洩漏或妨害組織利益等情節發生，資料攜入或攜出，主管應盡控管之責，提醒使用人員自我要求。私人可攜式設備與媒體，應**評估風險**後方可存取公務資料。
2. 處理**內部使用等級以上資料工作區域**，未經許可禁止使用相關設備進行拍攝或是螢幕畫面捕捉之行為，使用時需有**工作區域管理人員在場陪同**。

# 即時通訊軟體

1. 本校同仁應遵循網路通訊服務傳遞規定，利用網路通訊服務，如電子郵件、**即時通訊軟體**或外部應用系統或資訊交換平台時，應依據資訊資產處置規定，針對**不同等級的資訊類資訊資產，建立適當的資訊控管程序**，以確保資訊資產受到適當等級之保護。
2. 避免非授權人員取得機密性資料，**建立存取權限管理原則**，並據以執行。

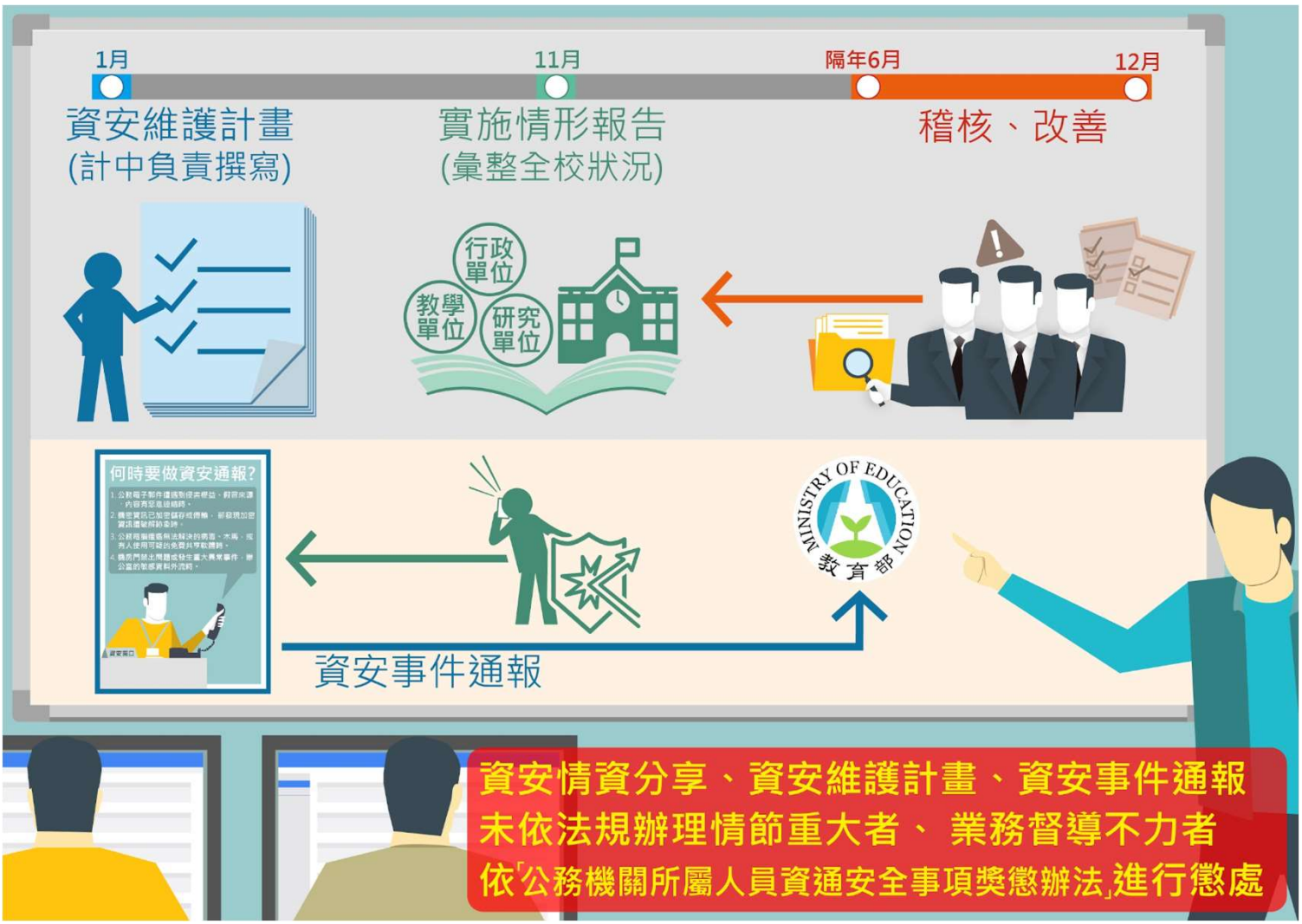
# 限制大陸製品

1. 除因業務需求且無其他替代方案外，**不得採購及使用**主管機關核定之廠商生產、研發、製造或提供之**危害國家資通安全產品**。
2. 必須採購或使用危害國家資通安全產品時，應具體敘明理由，**經主管機關核可後**，以專案方式購置。
3. 對本辦法修正施行前已使用或因業務需求且無其他替代方案經主管機關核可採購之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**，**不得與公務網路環境介接**，**不得處理或儲存機關公務資訊**，**測試或檢驗結果應產出報告**，購置理由消失或使用**年限屆滿應立即銷毀**。
4. 本校每個單位在執行購案時，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**。



# 資安懲處辦法

1. **未依法規**或機關內部規範**辦理**下列事項，**情節重大**：
   （一）**資通安全情資分享**作業。
   （二）訂定、修正及實施**資通安全維護計畫**。
   （三）提出資通安全維護計畫**實施情形**。
   （四）辦理資通安全維護計畫實施情形之**稽核**。
   （五）配合上級或監督機關資通安全維護計畫實施情形稽核結果，提出**改善報告**。
   （六）訂定**資通安全事件通報及應變機制**。
   （七）資通安全事件之通報或應變**作業**。
   （八）提出資通安全事件**調查、處理及改善報告**。
2. 辦理資通安全業務經主管機關、上級或監督機關評定績效不良，經疏導無效，情節重大。
3. 其他違反本法、本法授權訂定之法規或機關內部規範之行為，情節重大。
4. **對業務督導不力**，致其屬員、所屬或所監督機關之人員有前三款情形。




本校資安通報窗口 圖書暨資訊處 (04)8511888#1654

# 何時要做資安通報?

1. 公務電子郵件遭遇到侵害權益、假冒來源、內容有惡意連結時。
2. 公務上使用通訊軟體未重視資安問題，像是群組傳遞敏感資料時。
3. 公務電腦遭遇無法解決的病毒、木馬，或有人使用可疑的免費共享軟體時。
4. 各單位機房的門禁出問題或發生重大異常事件，辦公室的敏感資料外流時。


本校資安通報窗口

圖書暨資訊處

(04)8511888#1654