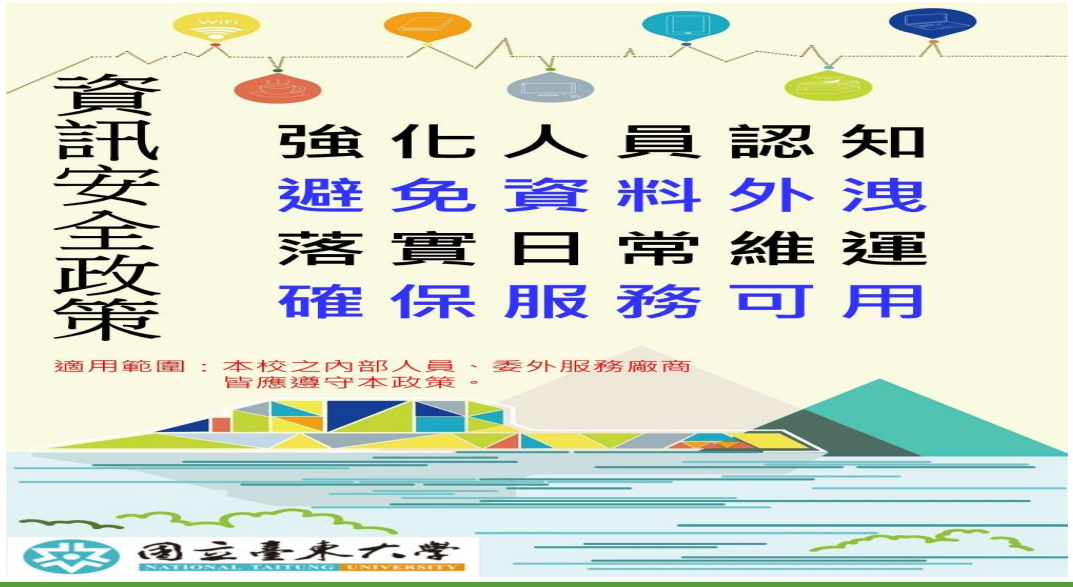
本校資通安全應注意事項

報告人：圖書資訊館網路組

112.11.09（星期四）

本校資訊安全政策



蒐集個人資料者，應注意事項

- 資料蒐集最小化
- 存取控制
- 使用雲端資通服務應確實做好相關設定檢查
- 傳輸之機密性
- 資料儲存安全
- 應訂定個人資料保存期限

發文日期：中華民國110年9月8日
發文字號：臺教資(四)字第1100122001號
速別：普通件
密等及解密條件或保密期限：
附件：學校使用資通系統或服務蒐集及使用個人資料注意事項（附件一 0dba373f40214d2cffcf5e9879000d4a_A09000000E_11027122001_doc1_Attach1.pdf)

主旨：檢送各級學校使用資通系統或服務蒐集及使用個人資料之注意事項(如附件)，請查照並轉知所屬。

說明：

一、鑒於學校使用雲端資通服務(如Google表單等)蒐集個人資料時，可能因設定不當而增加個資外洩及資安風險，請各校使用資通系統或雲端資通服務蒐集教職員、學生及家長個人資料者，應注意旨揭事項，以「最小化」為原則，降低風險，並請各校主管機關加強宣導並督導所轄學校。

二、另提醒教職員工在處理個人資料時，應注意以下法規：

(一)個人資料保護法第28條第1項「公務機關違反個人資料保護法規定，致個人資料遭不法蒐集、處理、利用或其他侵害當事人權利者，負損害賠償責任。」

(二)個人資料保護法第41條第1項「違反個人資料保護法有關特種資料的蒐集、處理或利用規定，足生損害於他人者，處二年以下有期徒刑、拘役或科或併科新臺幣二十萬元以下罰金。」

密碼原則管理

- **使用預設密碼登入資通系統時，須立即變更密碼，不得使用弱密碼！並遵守下列事項：**
  - **管理者**至少每**3個月**更換密碼一次，**使用者**至少每**6個月**更換密碼一次，並禁止重複使用相同的密碼。
  - **密碼的長度最少8碼，混合大小寫、數字或特殊符號。**
  - 應避免將密碼記錄在書面上，或張貼於個人電腦、螢幕或其它容易洩漏之場所。

5

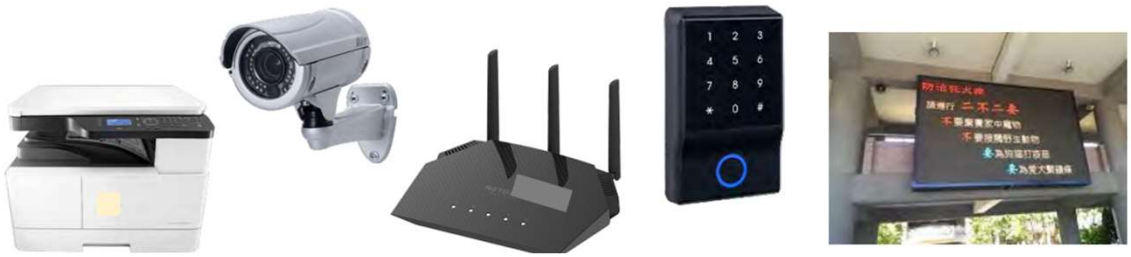
物聯網設備使用安全守則

- **物聯網(Internet of Things，IoT)，是指各種可透過連接網路提供服務的裝置**
- **設備類型包含但不限於：網路印表機/多功能事務機、網路攝影機、自設門禁設備、環控系統、自設無線網路基地台(AP)/路由器、連網電子看板、能源管理系統(EMS)...等。**
- **應遵守下列事項：**
  - **變更設備預設帳密。**
  - **進行安全性更新。**
  - **禁止使用大陸品牌之產品。**

6

物聯網設備安全風險

- 學校可能面臨的安全風險
  - 無法掌握**全校物聯網設備清單**及管理情形。
  - 設備**曝露於外網**，增加被外界發動攻擊的風險。
  - 設備**管理失當**，如使用**廠商預設帳密**、**未修補重大安全漏洞**等。

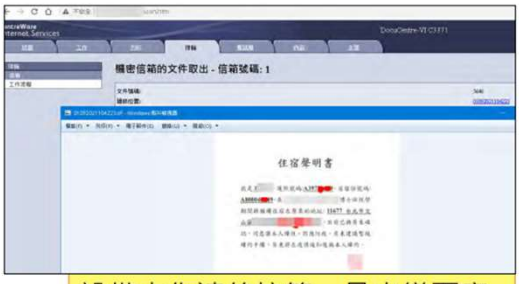


物聯網設備管理原則(1/2)

- **清查全校**物聯網設備
  - **盤點範圍**包含學校**採購**、**公務使用**之物聯網設備。
  - **設備類型**包含但不限於：**網路印表機**/**多功能事務機**、**網路攝影機**、門禁設備、環控系統、無線網路基地台(AP)/路由器、**連網電子看板**、能源管理系統(EMS)等。
  - 建立物聯網設備**管理清冊**(至少包含設備類型、廠牌型號、IP、存放地點、管理單位及用途等欄位)並**定期更新**(至少每年1次)。未納管設備建議斷網。
  - 逐步汰換老舊且無安全更新支援的設備。

物聯網設備管理原則(2/2)

- 加強設備連線控管
  - 依業務需求設定適當網路存取限制。
  - 無需對外開放連線者，得以防火牆限制僅供內部連線。
- 變更設備預設帳密。
  - 不得使用廠商預設帳密及弱密碼。
  - 符合機關規範之密碼複雜度要求。
- 修補設備重大安全漏洞。
  - 依公告漏洞情資即時進行安全性更新。



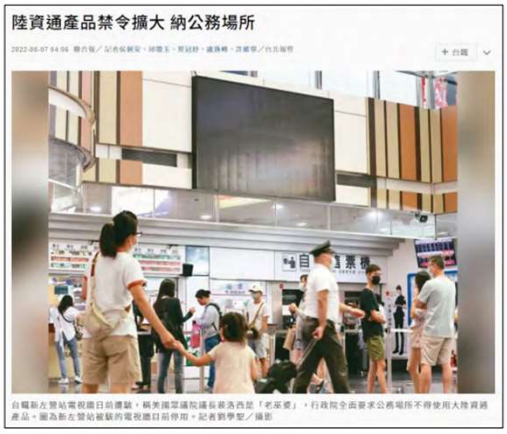
設備未作連線控管，且未變更廠商預設帳密，可能導致嚴重後果，如教職員生敏感個資外洩。

大專校院應辦事項(物聯網設備入侵)

- 依物聯網設備管理原則，落實設備安全防護。
  - 清查全校物聯網設備，定期更新清冊，並確認管理權責單位。
  - 加強設備連線控管，不得使用廠商預設帳密及弱密碼。
  - 即時修補設備重大安全漏洞。
- 不得使用大陸廠牌資通訊產品，如有應立即停止與公務環境介接，並盡速完成汰換。

大陸廠牌資通訊產品禁令擴大至對外出租場域

- 行政院111年8月資安警戒專案相關會議指示：
  - 針對傳播影像或聲音，供不特定人士直接收視或收聽之情形，皆不可使用危害國家資安產品(如大陸廠牌軟體、硬體及服務)。
  - 非屬前述傳播類型之危害國家資安產品，亦須列冊管理，控管資安風險，請各機關透過委外契約及場地租借使用規定來推動辦理。



資料來源: 聯合新聞網 111/8/7 報導，
https://udn.com/news/story/122988/6518330

大專校院應辦事項(對外出租場域)

- 限制出租場域使用大陸廠牌資通訊產品
  - 於學校委外契約或場地租借使用規定，明訂不得使用危害國家資安之產品（如大陸廠牌軟體、硬體及服務）。
  - 針對現有委外契約，協調廠商配合辦理或修正契約規定。
  - 備妥應變機制，如遇駭入侵，能緊急斷電下架。

工作區域實體管控(1/3)

1. 資訊資產分級：機密等級為**一般(1)**、**限閱(2)**標示成**綠色**、機密等級為**敏感(3)**標示成**黃色**，機密等級為**機密(4)**標示成**藍色**。
2. **螢幕保護程式應設定10分鐘啟動，並設定密碼保護。**
3. 電腦應安裝防毒軟體並即時更新病毒碼。
4. **電腦之作業系統及使用之軟體(如MS Office、Adobe PDF Reader等)應即時更新修補程式。**
5. 應定期將重要資料備份存放。
6. **清理資源回收筒。**
7. 時間同步設定(ntp.nttu.edu.tw) 已打勾同步且也更新。
8. **使用之電腦軟體均須具有合法版權。**

13

工作區域實體管控(2/3)

9. 禁止將「敏感」及「機密」等級資料存放於私人行動裝置中。
10. **禁止使用私人行動裝置翻拍校內「敏感」及「機密」等級資料。**
11. 免費軟體應於軟體開發原始網站進行下載使用。
12. **共享軟體授權規則為於試用期滿後須進行採購，若不進行採購，應於試用期滿前，將該軟體移除。**
13. 原版軟體除合法備份外，不得再有任何型式之備份，亦不得體安裝至其他電腦使用。
14. **IE 安全性政策為中高等級。**
15. 檢查桌面及工作場域。
16. **是否整齊清潔。**
17. 多功能事務機是否有未取走之文件。

14

工作區域實體管控(3/3)

18.紙張回收處是否已清理所有廢紙。

19.是否貼有帳號密碼。

21.是否有紀錄帳號密碼的筆記本。

22.是否有公文夾，尤其是有註明機密等級的文件。

23.是否有非正在使用中的可攜式儲存媒介(NB、USB)。

24.其他未使用但有可能暴露業務或工作資訊的通訊錄、帳密本、USB、NB等，請鎖到櫃子裡。

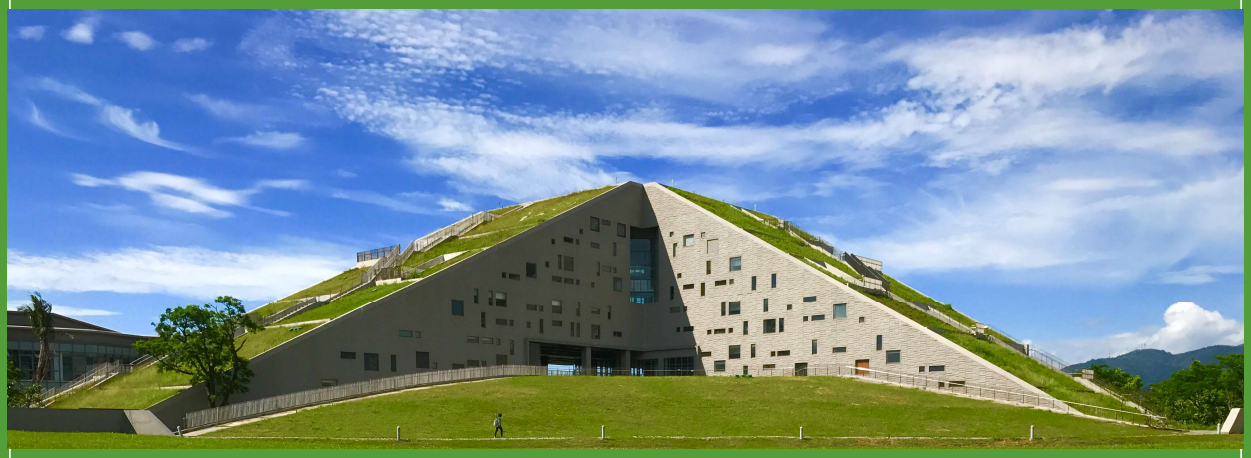
15

網頁遭竄改緊急應變原則

- 參考行政院111年8月資安警戒專案相關會議指示，如發現所轄管系統網站內容遭竄改，應依下列原則辦理**緊急應變**：
  1. 原網站**立刻下架**。(注意亦須完成跡證保全及留存)
  2. **維護公告**網頁：**10分鐘內上架**。
  3. **靜態資訊**網頁：網站功能**無安全疑慮**的部分可先上架**恢復服務**，如純資訊公告、媒體播放等。
  4. 逐步**功能恢復**：網站每次**版更上線前弱點掃描**，確認**無重大安全性弱點**。(必要時加入人工測試)
  5. 全面修復上架。

大專校院應辦事項(網頁遭竄改)

- 依資安法及「臺灣學術網路各級學校資通安全通報應變作業程序」規定，落實**資安事件通報**及**應變**作業(於**知悉1小時內完成通報**)。
  - 訂定內部作業規範且**適用範圍為全校**(含各行政單位、系所)。
  - 實施**教育訓練**或辦理演練，使相關人員確實熟悉作業程序。
- 針對網頁**遭竄改**事件：
  - **備妥應變機制**。請各行政單位、系所**盤點所管網站**，**事先建立維護公告**頁面及**切換機制**，以利及時應變。(發現網站內容遭竄改後10分鐘內切換為維護公告頁面)
  - **「行政單位、系所網頁遭竄改」**應納入學校**業務持續運作演練(BCP)**演練情境，並請相關單位**實際演練緊急應變**作業程序。



敬請指教