淡江大學108年度

高階主管
個資管理教育訓練

資訊處專案發展組

徐翔龍組長

2019/12/06

大綱

- 保護自己的個資安全
- 認識個資法
- BS10012:2017簡介
- 本校個資管理制度簡介

保護自己的個資安全

詐騙信件範例

"寄件者"跟"收件者"都是自己

From: Beitris Englert <hbeleonoretvi@outlook.com>
Date: July 12, 2018

Subject:

It seems that, xxxxxxxxx is your password. You may not know me and you are probably wondering why you are getting this e mail, right?

actually, I setup a malware on the adult vids (porno) web-site and guess what, you visited this site to have fun (you know what I mean). While you were watching videos, your internet browser started out functioning as a RDP (Remote Desktop) having a keylogger which gave me accessibility to your screen and web cam. after that, my software program obtained all of your contacts from your Messenger, FB, as well as email.

What did I do?

I created a double-screen video. 1st part shows the video you were watching (you've got a good taste haha . . .), and 2nd part shows the recording of your web cam.

exactly what should you do?

Well, in my opinion, $2900 is a fair price for our little secret. You'll make the payment by Bitcoin (if you do not know this, search "how to buy bitcoin" in Google).

BTC Address: 1KiCTVUq5A9BPwoFC8S965tsbtqcWr8bty
(It is cAsE sensitive, so copy and paste it)

Important:
You have one day in order to make the payment. (I've a unique pixel in this e mail, and at this moment I know that you have read through this email message). If I do not get the BitCoins, I will certainly send out your video recording to all of your contacts including relatives, coworkers, and so on. Having said that, if I receive the payment, I'll destroy the video immidiately. If you need evidence, reply with "Yes!" and I will certainly send out your video recording to your 6 contacts. It is a non-negotiable offer, that being said don't waste my personal time and yours by responding to this message.

說您的信箱、電腦、雲端帳戶…等已被駭或是宣稱手中握有您的照片、影片、隱私…等資料

威脅匯款至他的比特幣帳戶(BTC Wallet)

詐騙信件範例

From: mail [mailto:anenigma@xtra.co.nz]
Sent: Wednesday, July 26, 2017 1:02 PM
To: [redacted]@mail.tku.edu.tw
Subject: 提醒：郵件中心警告終止

電子郵件安全警報

此消息是為: [redacted]@mail.tku.edu.tw

這是通知你，有人試圖登錄到 您的電子郵件從無法識別的位置。
你知道關於此操作?

為您的帳戶安全，我們 強烈建議您現在驗證您 的電子郵件帳戶, 如果你不會驗證您的電 子郵件，您的帳戶將被 阻止而不必另行通知。

按一下此處驗證及保 護您的電子郵件帳戶現在

驗證後，我們將向您的電 子郵件中添加額外的保 ;護，讓它更安全的使用。

訊息源: 電子郵件安全團隊

http://www.hororatanurseries.co.nz/chinese_dco/crypt/connect.php?email=romeman@mail.tku.edu.tw

勒索信件範例


Arlie Wilson <Wilson.Arlie@biz.rr.com>
Important Information
收件人: dragon@tku.edu.tw
Dear dragon, your payment was not processed due to the problem with credentials.
Payment details are in the attached document.
Please check it out as soon as possible.
payment_dragon.zip
2.8K

個人電腦端點防護

安裝防護軟體

校園電腦：Symantec SEP

校園授權軟體

家中電腦：SecureAPlus (申請中)

資工系 **高浩傑校友 讚助**

楷巨國際科技有限公司 總經理

手　　機：McAfee Mobile Security Apps

Trend Micro Apps

Google隱私權與條款-服務條款

2017年10月25日更新

當您將內容上載、提交、儲存或傳送到「服務」，或在「服務」接收內容，或透過「服務」進行以上操作時，即表示您**授予 Google** (及我們的**合作夥伴**) **全球通用的授權，可使用、代管、儲存、重製、修改、製作衍生作品** (例如翻譯、改編或變更您的內容，使其更加配合我們的「服務」)、**傳播、發佈、公開操作、公開展示與散佈**這類內容。.....

即使您**停止使用**「服務」，本項授權仍**持續具有效力** .....

- **不放私密資料、照片**
- **含個資檔案要加密**

社群軟體LINE最新版APP將「設定」「隱私設定」之「外部應用程式存取」預設值，從「拒絕」更改為「**一律允許**」

➢ **請改為「拒絕」**

請三思而行

將個人**旅遊行程**或**機票**照片放在社群 (如acebook)

- 偷竊
- 護照資料、eMail、個人資訊→申請假銀行帳號

IBM安全專家表示，網路罪犯會利用機場、火車站和其它**公共場所的USB插槽來竊取你的個人資料**。他們可以輕易地修改USB插座，安裝可以竊取用戶包含銀行資訊等個人資料的特殊軟體。

- **使用自已的電源插頭**
- **使用自已的手機線**

個資事件

- 2018/8 台北市政府衛生局發生駭客入侵事件
  298萬餘筆就醫市民個資外洩

- 2019/6 銓敘部59萬筆公務員個資外洩
  包括國安局、軍情局、調查局、警政署、檢察、
  海巡、政風及憲兵等8大情治系統個資
  實際影響人數為24萬3376筆，
  含身分證字號、姓名、服務機關、職務編號、職稱

個資事件

- 2019/7 1111人力銀行20萬筆求職者個資個資外洩
  包括身分證字號、中文姓名、生日、電子信箱、
  電話號碼、地址、畢業學校等

- 2019/9 Facebook 高達4.19億筆個資外洩
  含手機號碼、帳戶位置等

個資事件

- 2019/9 EZ（EZding）訂購票平臺個資外洩
  一審判定，業者需依個資法賠償民眾2萬元，
  二審最終裁定**賠償18萬3,274元**
  法院發現：
  - 有多項Log記錄不完整，
  - 伺服器的Audit Log 無記錄，
  - SSH登入權限未限縮並稽核，
  - 內部機敏資料上傳到外部雲端硬碟

個資事件

- 2019/10 雄獅旅行社2017年36萬筆旅客個資外洩

  消基會提起團體訴訟，求償450萬餘元，

  首宗個資法團訟案件，一審判免賠。

  法院認為雄獅案發後：

  - 隨即報警並發布重大訊息，
  - 且已採行**符合個資法規定的安全措施**，
  - 因第三人入侵所致，難以認定雄獅有過失，
  - **判決免賠**，可上訴

認識

個人資料保護法

個人資料保護法(56) 105/3/15施行

- 公務機關及
- 非公務機關(指前款以外之自然人、法人或其他團體)

資通安全管理法(23) 108/1/1施行

- 公務機關及
- 特定非公務機關(指關鍵基礎設施提供者、公營事業及政府捐助之財團法人)

個資定義(第2條)

個人資料(自然人)

- 姓名
- 出生年月日
- 國民身分證統一編號
- 護照號碼
- 特徵
- 指紋
- 婚姻
- 家庭
- 教育
- 職業
- **病歷**
- **醫療**
- **基因**
- **性生活**
- **健康檢查**
- **犯罪前科**

特種個資

- 聯絡方式
- 財務情況
- 社會活動
- 其他得以**直接**或**間接方式識別**該個人之資料)

第5條

- 個人資料之蒐集、處理或利用，
  應尊重當事人之權益，
  依誠實及信用方法為之，
  不得逾越**特定目的**之必要範圍，
  並應與蒐集之目的具有正當合理之關聯。

個人資料安全
(細則第12條)

- **安全維護措施、安全維護事項、適當之安全措施：**

  指公務機關或非公務機關為防止個人資料被竊取、竄改、毀損、滅失或洩漏，**採取技術上及組織上之措施**。

技術上及組織上之措施

(細則第12條)

- 一、配置管理之人員及相當資源。
- 二、界定個人資料之範圍。
- 三、個人資料之風險評估及管理機制。
- 四、事故之預防、通報及應變機制。
- 五、個人資料蒐集、處理及利用之內部管理程序。
- 六、資料安全管理及人員管理。
- 七、認知宣導及**教育訓練**。
- 八、設備安全管理。
- 九、資料安全**稽核機制**。
- 十、使用紀錄、軌跡資料及**證據保存**。
- 十一、個人資料安全維護之整體持續改善。

賠償、罰責

有法律就有罰則

第四章 損害賠償及團體訴訟

第五章 罰則

第29條

- 非公務機關違反本法規定，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。但能**證明其無故意或過失者，不在此限**。

第28、29條

- $500~$20,000 (每人每一事件)
- 最高總額以**新臺幣二億元**為限
- 因事實所涉利益超過新臺幣二億元者，以該**所涉利益為限**。

第50條

- 非公務機關之**代表人**、**管理人**或其他有**代表權人**，因該非公務機關依前三條規定受罰鍰處罰時，**除能證明已盡防止義務者外**，應並受同一額度罰鍰之處罰。
  - 第47條 5萬-50萬元
  - 第48條 2萬-20萬元
  - 第49條 2萬-20萬元

PIMS
BS10012:2017
個人資訊管理系統

BS 10012:2017管理摘要

1.法源依據 (6.1.3)
2.合法、公平且透明的處理 (8.2.6)
3.善盡告知義務 (隱私權資訊 (8.2.6.1)
4.僅基於特定合法目的取得(8.2.7)
5.適當、相關及限於資料侷限原則(資料最小化 8.2.8)
6.正確並及時更新 (正確性 8.2.9)
7.資料的儲存不得超過許可的必要 (保管期限 8.2.10)
8.適當確保個人資料安全 (完整性及機密性 8.2.11)
9.確保資料傳輸之安全 (8.2.11.4)
10.落實委外安全管理 (8.2.11.10)
11.自然人權利 (8.2.12)
12.妥善處理訴怨程序 (8.2.12.9)

BS 10012:2017管理摘要

根據《ISO/IEC 指南 51》

「**安全**」的定義為**免於無法承受的風險**。

換句話說，

將**風險降低到可承受的等級**，就能達到安全。

淡江大學
個資管理制度

全校導入 BS10012 (國際標準)

103年1月29起取得
BSI 英國標準協會認證

http://pims.tku.edu.tw/

PIMS實作

- **P 規劃**

  範圍及目標、管理政策、職責與當責性、資源提供、落實組織文化

- **D執行**

  管控機制、認知與教育訓練、辨識及記錄個資、風險評鑑；公正與合法、基於特定目的、適當且不過度處理個資、正確性、保存、個人權利；安全議題、揭露給第三方、委外處理

- **C稽核**

  內部稽核、外部稽核(第三公正方)

- **A改善**

  預防措施、矯正措施

PIMS教育訓練

教育體系資通安全暨個人資料管理規範

附錄B 個人資料管理規範 B.3.1.1

對**全體教職員工**進行**每年至少三小時的教育訓練或宣導**，來提高、強化與維持對個人資料管理政策的認知

PIMS稽核

教育體系資通安全暨個人資料管理規範 六、(二)內部稽核

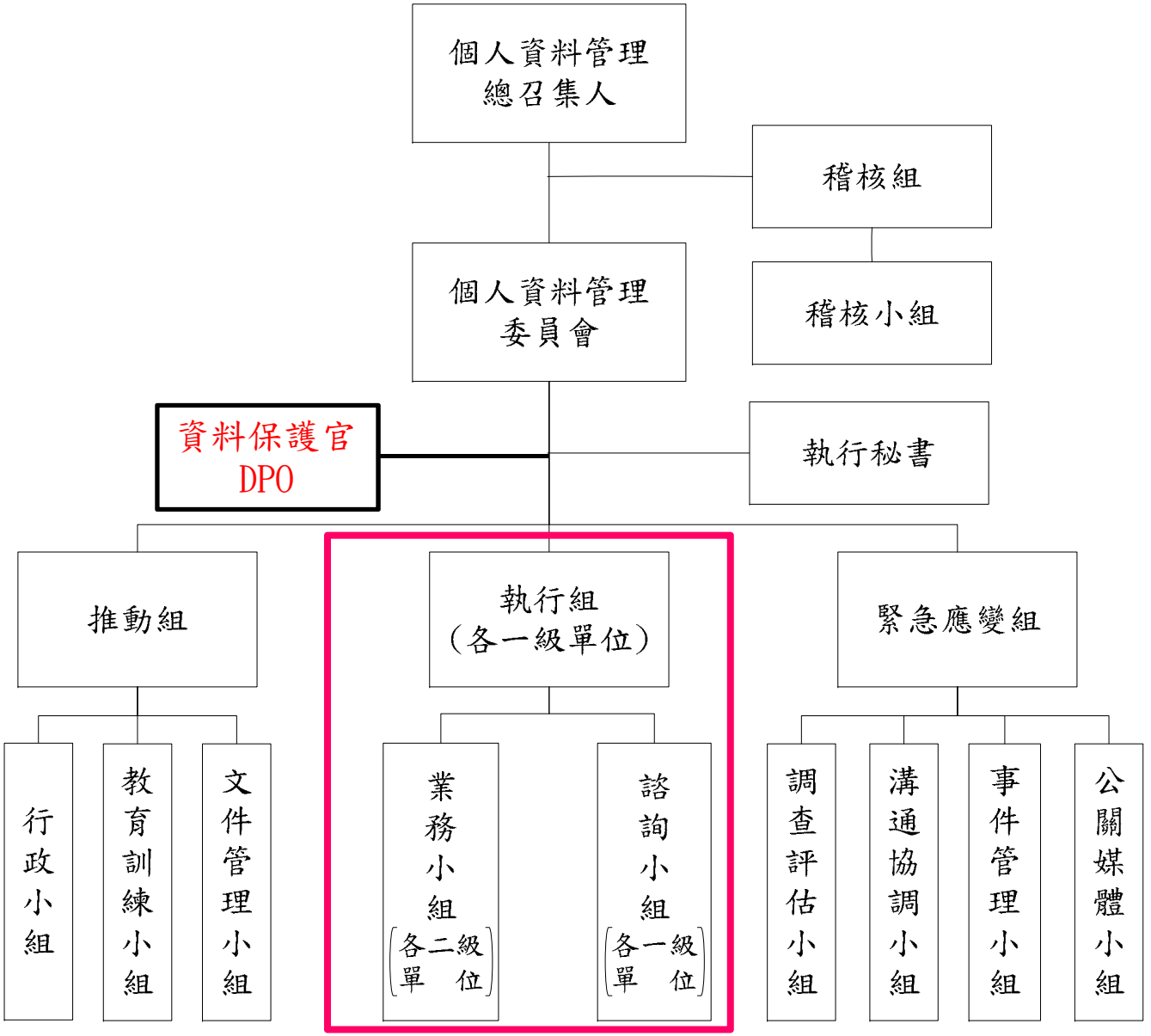
學校應定期（至少**每年一次**）或於重大變更後執行一次內部稽核，以確認機關（構）或學校與人員是否遵循本規範與機關（構）或學校管理程序要求，並**有效實作及維持管理制度**。

BS10012:2017 9.2內部稽核

稽核計畫應明確包含任何高風險個人資料之處理。
且應包含委外廠商（資料處理者）所處理的個人資料。

本校現有38位BSI主導稽核員 (領先全國)

淡江大學個人資料管理組織架構



淡江個資制度執行摘要

- 法規遵循、法源依據
- 蒐集最小化原則
- 盤點清冊 (V3.0)
- 風險評估表(V3.0)
- 軌跡紀錄(傳遞)
- 保存方式(安全)
- 保存期限
- 銷毀紀錄 (Log)
- 權利 (行使窗口)

風險

威脅、弱點

→控制措施

→風險等級

(極高、高、中、低)

「低或中」者為本校風險可接受水準

注意事項

- **法源依據、稽核準則**
  - ✓政府相關法律、規定、國際標準
  - ✓ 校規作業準則、合約、**合理自訂(會議決議)**
- **資料保存期限**
  - ✓主管機關法規
  - ✓機關共通性檔案保存年限基準 (20 大專校院類)

    106年5月17日國家發展委員會檔案管理局

    (檔徵字第1060009095號函訂頒)
  - ✓分層負責明細表
  - ✓業務主管部門公告 (OA)

外部單位調用個資

- 主管機關要求師生資料？
- 派出所來文要求師生資料?
- 警察局來文要求師生資料？
- 校友會要求新生資料?
- 校友會要求校友資料?

外部單位調用個資

- 個資法第8條：(得免告知)

  個人資料之蒐集係公務機關執行法定職務或非公務機關履行法定義務所必要。

- 刑事訴訟法第228、229、230條 (105/6/22)

  檢察官、司法警察官

  警政署署長、**警察局局長**或警察總隊總隊長、憲兵隊長官

  警察官長、憲兵隊官長、士官

- 調度司法警察條例第2、3條 (69/7/4)

  司法警察官

  市長、縣長

  警察廳長、警保處長、**警察局長**或警察大隊長以上長官、憲兵隊營長以上長官

  警察分局長、憲兵隊連長

外部單位調用個資

- 正式來文(函-公文交換)
- 長官署名、理由、個人資料範圍
- 是否為合理事項
- 最小化提供
- 至少須經一級主管核准 (執行組)

外部單位調用個資

- 蒐集個資時事先告知 (特定目的)
- 個資當事人同意 (目的外利用)

- 校友會要求新生資料?
- 校友會要求校友資料?

個資保護、資訊安全

人人有責

簡報結束