2019年
個資保護及資訊安全教育訓練

主講:陳寶惠

2019/6/11

我們公司的 ISO認證

- BS10012:2009 個人資訊管理系統
- 有效期限：2017-01-08~2020-01-07
- 預計2019年導入BS10012 : 2017改版事宜

個人資料保護要求

- 對於資訊安全及個人資料蒐集、處理及利用，因執行業務所持有之任何個人資料，負有保密義務，非經公司同意，不得以任何方式，直接或間接向第三人透露或使其知悉。

個人資料生命週期

- **蒐集：依法進行告知義務 / 取得同意。**
- 處理：採取適當的保護措施，避免個人資料被竊取、竄改或毀損。
- 利用：應於蒐集之特定目的內使用，特定目的外之使用應另外取得書面同意。
- 傳遞：傳遞及交換分享中採取適當的保護措施，避免個人資料被竊取、竄改或毀損。
- 銷毀：特定目的消失 / 期限屆滿 / 當事人要求。

資訊安全控管

- 檔案軌跡 LOG 紀錄 (檔案傳輸、刪除)
- 電腦、系統帳號權限（檔案存取）
- 個人電腦與文件（密碼鎖定、桌面清空）
- 門禁權限與管制（設備維護、進出貨、訪客）
- 物料銷毀（待銷毀品管控）
- 管理作業程序 (管理、更新與執行)

資訊安全風險

- 離開工作崗位時，請將電腦鎖定或登出。
- 下班後請將電腦關機，並遵守桌面淨空政策，文件紙本放置抽屜上鎖。
- 帳號及密碼僅供個人使用，不得告知其他人。
- 帳號密碼不慎遺失外洩，請立即通報資安單位。
- 請勿下載來路不明的檔案。

何謂加密勒索軟體

- 勒索軟體 Ransomware是一種特殊的惡意軟體，會將你電腦上的硬碟、檔案加密，使你無法讀取電腦上任何資料檔案，如果不付錢給這攻擊的背後黑手也就無法解開密碼。基本上，你的系統或資料成為了人質，讓你被迫去支付贖金。這也就是它被稱為「勒索軟體」的原因。

加密勒索軟體如何感染電腦

- 網路廣告。
- 被駭客入侵的網站。
- 電子郵件。

加密勒索軟體如何感染電腦

- 一旦感染加密勒索軟體，請依下列步驟迅速處理：

1. 先**拔除**插在電腦主機背後的**網路線**，避免災情可能擴大。
2. 若是使用者能夠即時發現，自己電腦中的檔案正在被惡意程式加密中，立刻**持續按壓電源鍵**，強迫電腦進行關機動作。
3. 立即連絡MIS人員，協助支援處理。
4. 將被感染的電腦**硬碟格式化**，**重灌系統**，讓電腦回復成乾淨的原始狀態。**切勿自行嘗試將檔案複製到其他電腦讀取**。

如何避免成為勒索程式的受害者

- 勿任意開啟不明來源電子郵件及郵件附加檔案(尤其是.zip壓縮檔)。
- 勿任意點選不明來源電子郵件中的超連結(如：http://www.xxx.idv/)
- 勿任意點選網站上不明的超連結。(如：http://www.xxx.idv/)
- 勿隨意將私人隨意碟或移動式硬碟接到公司電腦。
- 平時備份您的重要檔案或避免將業務機密資料儲存在個人電腦。
- 隨時更新作業系統(Window update)、防毒及應用軟體(如:Adobe)。

簡報結束