

# 數據分類及處理

## 你的數據在哪裏？

數據正以指數級的速度增長，我們分分秒秒都會接觸到數據。我們經常製造、處理或儲存各樣數據，如紙張文件、數碼照片、或是在大學校園電腦系統中數以TB計的研究數據。正因為不同的資訊載有在各種各樣的設備上，作為個人用戶應如何在大學環境中配合不斷增長的數據管理需求？



電腦實驗室



手提電腦



圖書館



外置硬盤



紙張



打印機



USB記憶棒

## 誰負責處理數據？

### 管理層

- 提供管理框架
- 制定數據分類

你

### 數據擁有者

- 標識和分類數據
- 實行監控程序

### 資訊科技部門

- 提供適當的基礎設施和培訓

## 為什麼要把數據分類？

1. 集中資源保護敏感資料以管理資料洩露的風險。
2. 幫助學生和教職員明白各類日常處理的數據的重要性和機密性。
3. 有效地實施各種監控措施來保護不同分類的數據。
4. 確保學生和教職員清楚怎樣根據數據分類來保護數據。

# 數據分類框架

數據分類 是一種為各式數據提供有效分類等級的工具。它使你明白：

- 不同類型數據的重要性
- 當你遺失這些數據時對你和這所大學所造成的影響
- 處理各類資訊的適當方式
- 各類型數據的存取權限
- 各類型數據的擁有者和使用者

People | Process | Technology  
人物 | 流程 | 科技

## IPPTI

當你實施數據安全管理框架時，往往需要顧及不同的方面考慮。PPT是一個讓你能對資訊安全作全面考慮的框架。當實施一個有效的數據分類時，我們需要知道 -

誰將會負責處理有關數據

將會運用甚麼技術

經過怎樣的處理過程

我們也需要知道如何分辨種種不同的數據，以及它們如何相互作用及聯繫。

### 人物

例如：

- 數據擁有者
- 數據保管者
- 數據使用者

### 流程

例如：

- 資訊分類政策
- 數據處理守則
- 第三方數據處理要求

### 科技

例如：

- 數據加密技術
- 數據保護技術
- 文件管理系統

## 數據標籤

數據分類標籤的例子

### Public 公開資料

可能或必須提供給公眾的資料。  
一些沒有本地、國家或國際法律存取限制的資訊。

### Sensitive 敏感資料

基於擁有權、道德或隱私的考慮而必須加以保護的資訊。  
這種分類亦適用於民事法規沒有要求保護的資訊。

### Restricted 限制資料

因數據保護守則、政策或法規要求而保障的數據。  
數據的擁有者行使他們的權利以限制存取的數據。



# 如何處理及保護數據

作為數據使用者，根據數據的分類來處理有關資訊是極為重要。根據數據的分類，數據處理可能要求不同級別的保護或預防措施。

## 建立

### DO'S

- 於數據建立時確定資訊的分類
- 當建立敏感資訊時選擇合適的加密機制
- 當建立沒有加密的敏感數據，應確保該設備有適當的實體保護以防止未經授權的存取
- 對敏感數據實施足☒的用戶認證

### DON'TS

- 別在公用電腦上建立未經加密的敏感數據

## 使用

### DO'S

- 確保在存取敏感資訊時輸入的用戶名稱和密碼沒有被他人看見
- 遠端存取於完成使用後應被立即終止
- 盡快取回於打印输出的敏感資訊

### DON'TS

- 敏感的資訊不應被他人看見
- 除非以安全形式建立遠端存取，否則不要存取敏感資訊
- 不要使用公用電腦存取敏感資訊
- 避免下載或列印敏感數據
- 瀏覽敏感資訊時不要離開你的電腦
- 千萬不要把 自己的帳戶名和密碼與他人分享

## 刪除

### DO'S

- 刪除所有不必要的敏感資訊
- 利用數據刪除工具來徹底刪除於存儲設備上的敏感數據
- 碎掉載有敏感資訊的紙張
- 防止被人翻找垃圾，例如不要讓任何人於被丟棄的文件中找到了有價值的資訊

### DON'TS

- 不要使用基本的系統檔案刪除指令，因為一般操作下刪除的數據可以被取回
- 不要將敏感資訊丟進一般的垃圾桶

## 轉移

### DO'S

- 在轉移敏感數據的過程中考慮額外的加密程序
- 只複製最少量的敏感資訊作已允許用途
- 轉移數據前，應先通知收件人有關資訊的分類

### DON'TS

- 不要複製過多的敏感數據
- 除非你是數據的擁有者，不要降低數據的分類級別



## 存檔

### DO'S

- 敏感資料的存檔應使用加密的檔案格式或媒體
- 把存檔用的密碼分成多部分，並交由不同員工保存。只有數據擁有者知道完整密碼
- 存檔資訊應保存於適當的實體和環境安全中
- 注意存儲媒體的運輸安全

### DON'TS

- 不要複製過多敏感資訊作存檔用

## 變換

### DO'S

- 只向有需要進行相關工作的人員披露變換後的敏感資訊
- 留意數據分類和變換數據時所需的保安控制
- 變換敏感資料時應使用適當的安全存取控制

### DON'TS

- 除非雙方有保密協議，否則不應向任何第三方提供變換的機密數據

## 存儲

### DO'S

- 限制敏感數據的存取
- 以實體監控保護存儲設備
- 對敏感數據進行加密
- 實施用戶驗證機制
- 在災難恢復計劃中，應保障敏感數據的備份媒體的實體安全

### DON'TS

- 不應儲存敏感數據於不設加密存儲設備上
- 使用後不要保留敏感數據

# 別忘記基本保護資料安全

數據處理程序的制定是為了保護敏感數據。然而，安全數據處理程序的效果仍然依賴基本的資訊安全知識。數據會因不同的原因受到破壞或外洩；以下一些基本方法能有效地保護您的敏感資料。

## 電腦

- 當離開電腦時，將電腦屏幕上鎖
- 每天晚上把電腦關閉
- 將辦公室的出入口鎖上



## 密碼

- 使用保安效能較強的密碼（如足夠的長度及複雜性），並將它們保密
- 不要使用您的帳戶為其他人登入系統
- 不要將密碼保存於電腦檔案或外置儲存裝置上
- 不要把密碼寫在紙上
- 定期更改密碼



## 電郵

- 每天檢查你電郵帳戶的“已發送郵件”和“已刪除郵件”，以確保敏感資訊不會被儲存到未知的位置。
- 不要開啟可疑電子郵件或其附件
- 避免以電子郵件發送敏感數據。並於發送前仔細檢查該收件人的名稱
- 除非你主動提出，否則從不要跟從電子郵件上對個人資料的要求
- 驗證在電子郵件上的網站鏈結並注意網站是否釣魚（虛假）網站



## 互聯網

- 不要從未經驗證的來源下載軟件
- 於瀏覽器上刪除臨時網頁檔案
- 關閉網上表格的自動填寫功能，因為它會存儲你的資訊，例如用戶名和密碼



## 實體保安

- 敏感數據應存放在安全地方
- 儲存敏感數據的地方限指定授權人員進入



## 人 PEOPLE

你於數據分類和處理中的角色

縱使有清晰的數據分類和處理政策以及昂貴的檔案管理技術，資訊安全仍然依靠人們：

- 識別資訊及為資訊分類
- 處理數據
- 應用已有的科技

用戶應明白數據的重要性，並時刻注意對數據的分類和處理。



# 資訊安全中的人為因素



## 「您」作為系統的一部分

資訊安全不僅關係到電腦系統本身。但為什麼資訊安全不能只談科技？

- 科技可能有漏洞
- 機構可能無法充分解決所有的技術安全問題
- 科技的成本高昂
- 設定及使用科技的都是人

人始終是資訊保安中最弱的一環

## 資訊安全的基本原則

- 保密性- 即是對敏感資訊的保護
- 完整性- 即是保存完整及有效的資訊
- 可用性- 即是讓資訊能被及時提供



## 人為因數怎樣破壞資訊安全

### 場景一

#### 電腦系統登入 - 安全vs 一時方便

- 密碼政策規定密碼長度、複雜性和有效期限
- 密碼政策落實到一般使用者的應用程式上
- 設有密碼到期提示措施，以幫助用戶遵守密碼政策的要求
- 但是...由於需要頻密地更改密碼，用戶將密碼寫在便條上，並貼在屏幕旁！

你會否將你的鑰匙掛在大門的旁邊嗎？

#### 犯錯

輸入錯誤數值

製造不正確電腦程式

#### 大意

忘記登出系統

把密碼與他人分享

#### 欺詐

發放電腦病毒

在程式中隱藏漏洞

#### 好奇

開啟可疑電郵的鏈接

安裝不明開發商的軟件

#### 大意

#### 犯錯



#### 欺詐



#### 好奇



# 資訊安全中的人為因素

## 系統安全修補程式 - 安全vs專業知識

- 系統供應商確定了系統漏洞
- 系統安全修補程式以及對漏洞的概念驗證均已由供應商發佈
- 由於更新數量龐大，系統管理員未有安裝新的安全修補程式
- 有人針對已發佈的漏洞製造電腦病毒
- 發生校園網絡病毒爆發！

## 惡意電子郵件 - 安全意識 vs 好奇心

- 已進行安全意識培訓，並提醒學生員工不可開啟可疑電郵的附件
- 病毒開發者設法找出辦法，利用了一般用戶的好奇心，例如有趣的電郵主題，內文和附件檔案名稱

場景二

場景三

## 資訊安全的角色及職責

- 了解資訊安全的重要性
- 制定資訊安全方向，並撥出足夠的資金用於資訊安全管理
- 跟進安全事故
- 讓資訊安全團隊參與管理層的會議



管理層

- 了解最新的安全趨勢、保安威脅及漏洞
- 認識最新的科技資訊及了解系統相關的安全更新
- 及時安裝系統安全更新，並定期向安全管理小組報告



操作團隊

- 了解最新的安全趨勢、保安威脅及漏洞
- 為用戶提供足夠的安全意識培訓
- 審查和更新資訊保安政策以及將有關更新通知用戶
- 向管理層報告資訊安全事故
- 建立系統操作團隊的技術能力
- 了解校園的資訊安全趨勢，並找出潛在的弱點



資訊安全團隊

- 了解自己在資訊安全中的角色
- 參與資訊安全意識培訓
- 小心處理可疑的電子郵件及互聯網內容
- 使用保安效能較強的密碼，並將密碼保密
- 向資訊安全團隊報告資訊安全事故



用戶