淡江大學資訊處

員工資訊安全認知手冊

編號：FK-ISMS-03002

版本 4.0

機密等級：一般資訊

生效日期：107.09.20

版本變更紀錄：

變更日期	文件版本	編訂者	變更紀要說明
93.11.05	1.1	蔡春枝	文件負責人由張慧君改為蔡春枝
97.11.04	2.0	姜美文	配合重審作業及資訊安全之演進，增加資安認知內容
100.11.24	3.0	蔡春枝	配合學校組織名稱更改修訂(資訊中心改為資訊處，主任改為資訊長)
102.07.29	3.1	張碧君	文件負責人蔡春枝改為蕭明清
103.01.15	3.2	張碧君	文件封面文件負責人欄位取消
103.09.09	3.3	張碧君	1.文件封面簽核欄及修訂日期移除 2.文件編號 FIHX 改為 FKHX 3.新增手冊適用範圍
107.09.17	4.0	姜美文	配合擴大驗證範圍修改內容

員工資訊安全認知手冊

員工資訊安全認知手冊適用於淡江大學資訊處 IDC 機房(T105、T104)及異地備份機房之實體維運與骨幹網路、TSM 資料備份及回復及財務與學務系統開發及維運等相關作業之所有正式員工、臨時及約聘人員、工讀生、維護與服務廠商人員及非本處之機房作業人員。本手冊：

一、每年一次透過辦公室自動化系統，向資訊處各單位公告；E-mail 學校外單位及廠商等之業務相關人員。

二、手冊有增修更新時，除以辦公室自動化系統公告本處各單位、E-mail 學校外單位及廠商等之業務相關人員，並將最新版本之電子檔張貼於資訊處網頁之資訊處人員專區。

資訊安全基本觀念

1. 什麼是資訊?

「資訊」存在於任何形式，如磁帶、磁片、報表、通話內容、傳真等，不論有形或無形，使企業可以永續經營的資訊資產。

2. 什麼是資訊安全?

資訊安全就是對這些資訊資產加以保護，達到：

機密性(Confidentiality)：保護資訊不被非法存取或揭露。

完整性(Integrity)：確保資訊在任何階段沒有不適當的修改或損毀。

可用性(Availability)：經授權的使用者能適時的存取所需資訊。

3. 為什麼需要資訊安全?

資訊安全在保護資訊資產，避免遭受各種威脅，確保永續經營，降低傷害，提昇投資報酬率及信譽。

4. 資訊安全的範圍為：資訊使用之『環境』、『技術』、『規定』、『人員』。

資訊安全絕不是僅僅是資訊人員之責任；絕對是組織全體之責任。

資訊安全絕對需要長官的大力支持；資訊安全之推動絕對不是專案形式。

組織每位成員都可能成為資安漏洞。

5. 什麼是資訊安全事件?

資訊安全事件是指任何違反常軌的異常行為，可能造成資訊系統及網路的安全威脅，經證明可能導致資訊系統運作錯誤事件或事故之情形及其後續所產生之故障效應等。

例如：√ 竊盜

√ 來自周遭環境的潛在危險

√ 系統當機

√ 天然災害(地震、水災、颱風等)

√ 未經授權進入或使用電腦系統的資源
√ 未經授權使用他人帳戶
√ 電腦病毒
√ 駭客入侵
√ 人員差錯：錯誤或不良的維護、錯誤設定和操作員的其他錯誤行為等。

6. 據統計有 80%的資料遺失，是因為內部人員有意或無意之下所造成的結果。
例如：將重要的資料寄給非授權的人、備忘錄放至網路留言板、將資料、文件燒錄至光碟、關鍵文件透過印表機列印出等。
7. 資訊安全威脅與來源
- 好奇人士：可能剛學會入侵電腦的方法，就應用書本上寫的方法當起駭客。
- 內部員工：也有可能是潛在的威脅，尤其對單位有不滿情緒及抱怨的人。
- 預謀犯罪的歹徒：透過各種方式竊取單位機密、牟取暴利，如販賣個人資料。
- 間諜：因商業上或政治上的因素，以各種滲透入侵技術，取得企業機密文件。
- 組織型駭客：主要以竊取或破壞單位內部電腦機敏檔案資料為主，以刺探、竊取為目的。

8. 來自內部粗心員工的威脅
- 不規避旁人，如重要資料或密碼輸入。
- 不隨手關機。
- 隨時討論業務機密。
- 使用者帳號隨便借給他人。
- 印出的報表隨手亂放。
- 檔案資料未事先分類
- 硬碟存放私人資料。

9. 常見的錯誤觀念：
- 沒人會知道我曾經上過那些網站，所以.....
正確觀念：你所瀏覽過的網頁都會在系統內留下紀錄，稽核人員會不定期抽查。
- 網路上的免費程式可以隨意下載使用
正確觀念:某些免費軟體可能含病毒或後門程式，會破獲電腦的運作或竊取密碼及資料。
- 公文或重要文件下班了就放在桌面上也沒關係
正確觀念:公文和機密資料應於下班前收好並鎖入櫃子，以防止遺失或遭竊。

資訊設備使用

- 安裝在公共區域的設備（如公用主機、印表機或伺服器），應有具體的保護：
  - 在活動完成時應終止對話，結束畫面。
  - 螢幕保護程式需設定密碼保護。
  - 活動結果時登出系統或主機，再關閉電腦。

- PC 或設備不用時，應使用密鎖或其他安全控制措施，以防止他人非法使用。

- 桌面淨空
  - 重要、機密文件不置於桌上。
  - 重要、機密文件下班或離開辦公室前應鎖入安全空間。
- 螢幕淨空
  - 設定螢幕保護程式
  - 設定保護密碼。
  - 離開座位或暫時不使用時鎖定螢幕。

電腦軟體及網路使用

- 不得將授權軟體轉借或給予未經授權人員使用。
- 不得任意更改個人電腦 IP 位址與網路卡。
- 個人電腦不得安裝數據機或架設無線網路等相關對外連線設備。
- 個人電腦(筆記型電腦、伺服器)應關閉 USB 儲存裝置自動執行設定(Auto Run)，以防駭客藉由 USB 儲存裝置植入後門程式。
- 機密檔案不得在網路上傳送。

密碼管理

- **不當的密碼設定-懶人密碼**
  - 空白密碼
  - 密碼與帳號相同
  - 密碼與電腦名稱相同
  - 使用自己或親朋好友的生日、電話等資料
  - 常見的英文姓名，像是：John、Jack、Mary
  - 使用 1111、1234、aaaa 等簡單的組合
  - 鍵盤上連續位置的字元組合，如 asdf…等
- **正確的密碼設定技巧**
  - 英文大小寫字母及特殊符號(如標點符號或是@#|><)，混合使用(若系統允許)。
  - 至少 8 個字元。
  - 沒有任何意義的組成。
  - 避免使用懶人密碼。
  - 不使用有意義的單字，以避免字典攻擊。
  - 使用不同的符號替換原來的數字或字母，或以輸入法代替。

    例：數字“0”→ 替代字母 “O”、 數字“1”→ 替代字母 “l”

    ″ 你好美″ 以注音輸入法之 su3cl3ao3 來代替。
  - 變動英文或數字既有排列順序，包含鍵盤按鍵的相對次序

    例：12345 以 54321 反序來對應。

➢ 創建獨一無二的首字母縮寫詞， 例如用 “蘿莉就是我” 的諧音 “loli945”。

- **不得將識別碼或密碼張貼在個人電腦或終端機螢幕或其他容易洩漏秘密之場所。**
- **定期更換。**
- **懷疑密碼外洩時立即更新。**

即時通訊軟體使用安全

- **登入密碼最好不要用「儲存密碼」記錄於系統內。**
- **不任意傳遞與分享公司重要資訊或檔案。**
- **不任意接收來路不明之分享檔案。**
- **使用者必須秉持以公事使用之目的使用企業即時訊息。**
- **隨時更新使用端程式。**

網路釣魚

網路釣魚是利用垃圾郵件的管道發送仿效知名網站的電子郵件，引誘無知的使用者進入偽裝的知名網站，藉此騙取使用者帳號、密碼或姓名、地址、電話及信用卡資料，然後再利用這些資料獲取不當利益。

遠離網路釣魚犯罪陷阱與騙局：

- **不回應不明公司、技術部門要求提供個人隱私或安全資訊。**
- **不點選來路不明郵件的網頁連結，如無法辨別真偽，不要點信件上的連結，而是自己輸入網址，減少被騙的機會。**
- **不利**用企業網路轉寄垃圾郵件。

郵件安全

可疑電子郵件之自我保護措施

- 安裝防毒軟體過濾郵件。
- 非必要閱讀之郵件逕行刪除。
- 確任發信者電子郵件帳號，惟發信者電子郵件帳號仍有被偽冒的機率，必要時直接與寄信者連絡確認是否來信。
- 設定為純文字讀取模式再開啟郵件閱讀。
- 開啟郵件內含之超連結時先確認連線網址之網域名稱(Domain Name)是否足以識別？若為數字 IP 之網址勿輕易開啟。
- 不隨意輸入資料送出，傳送私密資料時確認是否有啟動加密機制。
- 取消郵件預覽，不明來路之電子郵件不宜打開，不隨意開啟或下載附件，以避免木馬或病毒植入。

防堵垃圾郵件

- 絕對不回覆垃圾電子郵件訊息。
- 不購買垃圾電子郵件的廣告商品。
- 不轉寄串接式的電子郵件（例如聲稱不轉寄給 10 個人就會倒楣的電子郵件）。

- 要寄送同一訊息給許多收件者時，可採用『密件副本』方式來進行。
- 刪除寄件者為空白的電子郵件。
- 使用垃圾電子郵件過濾軟體。
- 非必要不設定自動傳送電子郵件之讀取回條。
- 注意可疑電子郵件之特徵：過於聳動的主旨與緊急要求、不正常發信時間、陌生人或少往來對象來信、認識的人來信但主旨或內容與其習性不符、要求輸入私密資料等。

社交工程

社交工程(Social Engineering)是利用人對人的信任及互動特性所發展出來的攻擊手法，以取得其所想要的資料。

例：你好，資訊室嗎？我是某某某，我忘記密碼了，可以告訴我的密碼？

防範之道就是不要隨便告訴別人密碼，並加強員工的認知訓練及警覺性。

電腦病毒

徵 兆	電腦系統運行速度異常緩慢。
	上網速度越來越遲緩。
	異常的系統訊息通知。
	螢幕顯示異常，例如畫面突然一片空白。
	來自防毒軟體的警告訊息。
	瀏覽器自動出現產品廣告或色情網頁。
	網路流量異常，例如沒有使用網路服務或收發電子郵件，但網路的連線號卻一直閃爍。
防 範	確認防毒軟體隨時運作。
	勿隨意安裝未經許可的電腦軟體。
	確保軟體在最新更新狀態。
	使用有問題立即反應。

廣告或間諜軟體

症 狀	沒有上網卻還是一直看見廣告視窗。
	網路速度時快時慢。
	首頁被更改成奇怪的網站。
	視窗下方的工具列出現許多原本沒有的工具。
	瀏覽多出沒有安裝過的工具列、搜尋工具，而且無法移除。

	電腦處理速度變慢或當機頻率增加。
防範	使用防火牆阻擋。
	關閉網路瀏覽器的 ActiveX 功能。
	下載免費軟體前仔細閱讀所有相關資訊。
	學習資料備份基本技巧。

駭客入侵

徵兆	檔案及資料庫內容遭到竊取或篡改。
	不知名的 IP 來源與電腦連線。
	系統中異常的服務程式。
	異常通訊埠開啟。
	稽核紀錄及檔案中的異常事件。
	系統帳號的異常增加。
	系統異常的訊息或行為。
簡易處理	定期系統備份。
	針對可能入侵途徑系統作隔離。
	蒐集入侵紀錄、檔案等軌跡。
	追查駭 IP 來源。
	分析資料找出入侵方式並改善。
	報告相關單位。
	適時尋求協助。
防範	即時更新修正檔。
	檢視權限設定。
	日常備份作業。
	紀錄及檢視稽核軌跡。
	設定自動時間校正作業。