# 輔仁大學資訊安全政策實施要點

97.05.21 第一次資安會議修正通過

## 一、 目的

輔仁大學（以下簡稱本校）爲維護整體資訊安全，強化各項資訊資產之安全管理，確保其具機密性、完整性、可用性、鑑別性與不可否認性，以因應業務運作需要，妥善支援教師教學研究、職員工作及學生學習，特訂定本要點。

- 機密性(Confidentiality)：確保只有經過授權的人才能存取資訊資產。
- 完整性(Integrity)：確保資訊資產其處理方法的準確性及完整性。
- 可用性(Availability)：確保授權的使用者在需要時，可以使用資訊資產。
- 鑑別性(Authentication)：確保網路中之個體（Entity）的身分確實如他所表明，或由網路所接收的資料確實爲該傳送者（ Sender ）所傳送。
- 不可否認性(Non-repudiation)：發送端不可否認其所同意傳送出的資料或他所完成的交易行爲。

## 二、 名詞定義

本要點所稱資訊安全係保護資訊資產避免遭受各種不當使用、洩漏、竄改、竊取、破壞等事故威脅，並降低可能影響及危害本校業務運作之損害程度。

本要點所稱資訊資產係本校所收集、產生、運用之資料，以及爲完成以上工作所需使用之相關設備。

## 三、 適用範圍

本要點適用於本校各項資訊資產及其資訊使用者。

- 資訊使用者係包含專兼任教師、專兼任職員(聘僱人員)、工友、學生(含推廣部)、建置維護廠商及其他經授權使用資訊資產之人員。

## 四、 法令依據

本要點及依據本要點所訂定之各項附屬規定 (以下簡稱資訊安全管理制度)，係參考電腦處理個人資料保護法、著作權法、國家機密保護法、電

子簽章法等法規及其他相關標準所訂定，資訊使用者應確實遵守，如有違反者，依相關法令辦理。

- 除本條所述法令外，以下各項爲訂定本校資訊安全管理制度的重要參考標準。
  - 國際標準組織的資訊安全標準(ISO27001：2005；資訊安全管理系統要求)。
  - 國際標準組織的資訊安全標準(ISO27002：2005；資訊安全管理作業要點)。
- 依據本要點所訂定之各項附屬規定-憑證政策、資訊安全組織作業原則、資訊安全文件管理、資訊資產分類分級、網路安全管理、主機安全管理、資訊應用系統安全管理、一般資訊設備管理、PKI 資訊安全管理、電腦機房管理、資訊安全通報處理、資訊安全稽核、資訊存取控制、辦公區域管理、委外管理、資訊安全風險評鑑與管理等作業原則。

## 五、 組織

本校爲落實資訊安全管理，成立資訊安全委員會，負責本要點之審核及資訊安全管理制度之推動事宜，其設置辦法另訂之。

- 成立以下必要組織推動資訊安全管理制度。
- 資訊安全長一人，由校長指派之副校長兼任之。
- 資訊安全委員會委員若干人，由主管中若干人兼任之。
- 顧問若干人，由資訊安全專長教師及具有資安證照之人員擔任之。
- 技術小組，由資訊中心及所屬組別組成。
- 訂定資訊安全組織作業原則，說明以下事項：
  - 資訊安全組織架構、工作職掌及運作方式。
  - 資訊安全會議及資訊安全小組會議召開頻率及討論事項。
  - 資訊安全組織人員資格及教育訓練。

## 六、 資訊資產安全

爲保護本校資訊資產安全，應建立資訊資產清冊加以分類分級，並訂定相對應之管制措施。

- 本校之資訊資產分爲資訊類資產(如檔案資料、系統文件、資料庫、教學教材及研究報告等)、實體類資產(如電腦硬體、通訊設備等)、軟體類資產(如作業系統、應用軟體、系統軟體等)、服務類資產（如電源、空調等）。
- 資訊資產清冊內容應註明資訊資產類別、擁有者、使用者及機密等級。
- 訂定資訊資產分類分級作業原則，說明以下事項：
  - 資訊資產分類原則。
  - 資訊資產分級原則。
  - 資訊資產管控措施。

## 七、 人事安全

爲降低內部人爲因素對本校資訊安全之影響，本校各單位應考量人力與工作職掌，實行分工及輪調措施。

本校應視需要實施資訊安全教育訓練及宣導，以提高人員對資訊安全之認知。

## 八、 委外管理

爲提高委外作業之安全，本校應要求廠商簽署保密協議書，並管理專案人員及駐點人員之各項資訊資產存取權限。

- 訂定委外管理作業原則，說明以下事項：
  - 規範保密協議。
  - 委外績效評鑑。
  - 委外廠商駐點人員管理。
  - 委外人員存取規範。

## 九、 風險管理

爲有效管理本校各項資訊資產所面臨之威脅、弱點及其衝擊程度，本校應辦理風險評鑑並進行必要之風險管理。

- 威脅指資訊資產遭受外來安全衝擊的影響，如火災、水災及駭客入侵。
- 弱點指資訊資產的安全控制不足所帶來的影響，如人爲疏失、網路漏洞。
- 風險評鑑指資訊安全確認的過程，藉由評估各個資訊資產的威脅與弱點以產出風險值，並確認其控制適足性。
- 風險管理指在可接受的成本內，對可能影響資訊安全之因素進行確認、控管，以降低其影響程度。
- 訂定風險評鑑暨管理作業原則，說明以下事項：
  - 資訊安全風險評鑑步驟。
  - 資訊安全風險管理步驟。
  - 資訊安全風險評鑑時機。

## 十、 實體安全

爲確保電腦機房維運及資訊資產使用區域之安全，應訂定安全管理規範。

- 訂定電腦機房管理作業原則，說明以下事項：
  - 機房內設備例行性檢查。
  - 機房內資訊設備及資訊媒體使用管理注意事項。
  - 門禁管理。
- 訂定辦公區域管理作業原則，說明以下事項：
  - 桌面淨空管理。
  - 螢幕保護程式設定。

- 傳真(機)資料管理注意事項。
- 設備安全管理。

- 訂定一般資訊設備管理作業原則，說明以下事項：
  - 個人電腦管理及使用規範。
  - 個人電腦報廢。

## 十一、主機系統安全

為確保主機作業平台及資料庫之安全，使操作程序標準化，應訂定安全技術規範。

- 主機系統係指大型電腦、伺服器、資料庫等。作業平台係指 Windows Server、Unix、其它及網站伺服器等。
- 訂定主機系統安全管理作業原則，說明以下事項：
  - 作業平台建置標準。
  - 日常操作管理。
  - 異常狀況排除。
  - 各項日誌記錄管理及保護措施。

## 十二、應用系統安全

為確保應用系統開發、測試、上線及維護之安全，應訂定標準管制及驗收程序。

- 應用系統指管理資訊系統及應用服務系統。
- 訂定應用系統安全管理作業原則，說明以下事項：
  - 應用系統開發管理。
  - 應用系統驗收測試。
  - 應用系統上線作業。
  - 應用系統維護。

## 十三、網路安全

為確保網路服務及使用之安全，應訂定管理規範。

- 訂定網路安全管理作業原則，說明以下事項：
  - 網路設備安裝維護事宜。
  - 防火牆建置與管理注意事項。
  - 網路安全監控檢核注意事項。
  - 網路流量監控統計注意事項。
  - 電腦病毒及惡意程式防治注意事項。
  - 入侵偵測系統(IDS)注意事項。

## 十四、憑證安全

為使憑證申請及應用有所依據，應制定憑證政策、憑證實務作業基準，並定期進行評估及修訂。

- 訂定憑證政策，說明以下事項：
  - 憑證申請及簽發。
  - 憑證下載事宜。
  - 憑證管理單位責任。
  - 憑證註銷事宜。
- 制定憑證實務作業基準，針對憑證政策內容，說明憑證實務作業的必要管理程序，並依據憑證標準之變異執行修訂。

## 十五、存取安全

為避免資訊資產因未授權之存取而使機密性或敏感性資料遭不當使用，應考量人員職務授予相關權限，必要時得採行加解密及身份鑑別機制，以加強資料之安全。

- 本校現行可採行加解密技術使用公開金鑰基礎建設（Public Key Infrastructure，PKI）。PKI 指運用公開金鑰，確保電子資料交換的安全性。
- 本校現行網頁加密採用 SSL (Secure Socket Layer) 技術以確保資料於網路上傳輸具有加密安全性。
- 本校現行身份辨識使用 LDAP 技術或電子憑證確認對方身分之機制。
- 訂定資訊存取控制作業原則，說明以下事項：
  - 使用者存取權限區分與管理。
  - 主機平台使用者帳號密碼管理。
  - 網路設備系統管理員帳號管理機制。
  - 筆記型電腦連線管理機制。
  - 無線裝置、攜帶式行動設備等使用管理機制。
  - E 化教室有線網路連線管理機制。
- 訂定 PKI 資訊安全管理作業原則，說明以下事項：
  - 晶片卡(CA)空白卡之使用管理注意事項。
  - PKI 憑證應用管理注意事項。

## 十六、資訊安全事件管理

為降低資訊安全事件造成之損害，應建立資通安全通報及處理程序，並加以記錄。

- 資訊安全事件指：
  - 內部危安事件─發現(或疑似)遭人為惡意破壞、毀損、作業不慎、資料遭竊等。
  - 外部攻擊事件─病毒感染事件、駭客攻擊(或非法入侵)事件。
  - 天然災害事件─颱風、水災、地震、雷擊。
  - 重大突發事件─火災、爆炸、戰爭等。
- 依據國家資通安全應變中心之通報規範，訂定資訊安全通報處理作業原則，說明以下內容：
  - 建立資訊安全事件通報程序。

- 建立資訊安全事件分析及處理程序。
- 資訊系統、資料之備份作業。
- 災害復原計畫。

## 十七、業務永續運作管理

爲避免資訊資產遭受災害而影響業務永續運作，應訂定應變及復原計畫，並定期測試演練。

- 災害指因資訊安全事件的發生，所造成之損失。
- 訂定業務永續運作管理作業原則，說明以下內容：
  - 災害處理程序。
  - 備援系統啓用處理程序。
  - 異地備援機房災害處理程序。
  - 應用系統回復處理程序。
  - 關鍵業務之復原優先順序。
  - 分析業務停頓的損失和備援措施。
  - 在地備援管理規範。

## 十八、資訊安全稽核管理

爲落實資訊安全管理制度，資安稽核小組應訂定稽核計畫，並定期執行。

- 資訊安全稽核工作可由內部或外部具備國際資安證照專業人員進行，並秉持獨立性及客觀性。
- 資訊安全內部稽核計畫之擬訂應參考過去稽核結果以決定稽核範圍及查核重點。
- 訂定資訊安全稽核管理作業原則，說明以下內容：
  - 稽核計畫之訂定。
  - 稽核範圍、頻率、方法。
  - 稽核紀錄與報告。
  - 改善行動與跟催。

## 十九、修訂

本要點應每年檢討，以反映最新標準規範、技術及業務現況，各項附屬規定由資訊安全委員會視需要修訂。

- 訂定資訊安全文件管理作業原則，說明以下內容：
  - 文件內容綱要。
  - 文件變更管理。
  - 文件編號編制方式。
- 本要點之版本變更應依據資訊安全文件管理作業原則。

## 二十、宣導

本要點應定期宣導，並依據 ISO27001、ISO27002 資訊安全管理要求本校各單位及所屬教職員工生共同遵守。

## 二十一、施行

本要點經資訊安全委員會通過，報請校長核定後施行。