華梵大學

圖書資訊處

資訊安全政策

機密等級：一般

文件編號：**HFU-ISMS-A-001**

版　　次：**1.1**

發行日期：**100.12.15**

修　訂　紀　錄				
版次	修訂日期	修訂頁次	修訂者	修訂內容摘要
1.0				初版
1.1	100.12.13	P3	張維世	6.1 增加「驗證範圍內」 7.1 修正為「切結書」

資訊安全政策					
文件編號	HFU-ISMS-A-001	機密等級	一般	版次	1.1

目錄

資訊安全政策					
文件編號	HFU-ISMS-A-001	機密等級	一般	版次	1.1

1 目的

為確保華梵大學圖書資訊處（以下簡稱「本處」）所屬之資訊資產的機密性、完整性及可用性，避免或減低遭受內、外部蓄意或意外之安全事件損害，並遵循相關法令、法規之要求，特訂定本政策。

2 適用範圍

2.1 本政策適用範圍涵蓋本處之各項資訊安全管理作業。

2.2 資訊安全管理範疇涵蓋 11 項領域，各領域分述如下：

2.2.1 資訊安全政策訂定與評估。

2.2.2 資訊安全組織。

2.2.3 資訊資產分類與管制。

2.2.4 人員安全管理與教育訓練。

2.2.5 實體與環境安全。

2.2.6 通訊與作業安全管理。

2.2.7 存取控制安全。

2.2.8 系統開發與維護之安全。

2.2.9 資訊安全事件之反應及處理。

2.2.10 業務永續運作管理。

2.2.11 相關法規與施行單位政策之符合性。

3 責任

3.1 本處應成立資訊安全組織統籌資訊安全事項推動。

3.2 管理階層應積極參與及支持資訊安全管理制度，並透過適當的標準和程序以實施本政策。

3.3 本處全體人員、委外服務廠商與訪客等皆應遵守本政策。

3.4 本處全體人員及委外服務廠商均有責任透過適當通報機制，通報資訊安

全事件或弱點。

3.5 任何危及資訊安全之行為，將視情節輕重追究其民事、刑事及行政責任或依本處之相關規定進行議處。

4 定義

4.1 資訊安全之本質大致可歸為以下 3 類：

4.1.1 機密性－Confidentiality：確保只有經授權的人才可以存取資訊。

4.1.2 完整性－Integrity：確保資訊與處理方法的正確性與完整性。

4.1.3 可用性－Availability：確保經授權的使用者在需要時可以取得資訊及相關服務。

4.2 除了以上 3 項基本性質外尚可依業務狀況考量驗證性 (authenticity)、可歸責性 (accountability)、不可否認性 (non-repudiation) 或可靠性 (reliability)，其說明如下：

4.2.1 驗證性－Authenticity：確保使用者登入時有適當的驗證程序。

4.2.2 可歸責性－Accountability：確保使用者執行任何動作均有適當的軌跡可追蹤至執行者。

4.2.3 不可否認性－Non-repudiation：確保使用者無法否認於系統上完成的作業。

4.2.4 可靠性－Reliability：確保作業執行皆有一致結果。

5 資訊安全管理目標

為維護本處資訊資產之機密性、完整性與可用性，並保障使用者資料隱私之安全。期藉由本處全體同仁共同努力以達成下列目標：

5.1 保護本處業務服務之安全，確保資訊需經授權人員才可存取資訊，以確保其機密性。

5.2 保護本處業務服務之安全，避免未經授權的修改，以確保其正確性與完

整性。

5.3 建立本處業務永續運作計畫，以確保本處業務服務之持續運作。

5.4 確保本處各項業務服務之執行須符合相關法令或法規之要求。

5.5 以上目標應建立「ISMS 有效性量測表」由資訊安全管理組織審核與確認。

6 資產管理

6.1 網路系統組、系統開發組應明確識別驗證範圍內，所管理之資產、並製作與維護重要資產清冊。

6.2 資訊形式之資產應以其對本校的價值、法律要求、敏感性及重要性加以分類。

7 人員安全管理

7.1 凡同仁工作職責需使用或處理資訊者，應簽署「保密切結書」課予機密維護責任。

7.2 人員離(調)職時，應取消或變更各項資訊資源之所有權限。

8 資訊安全訓練

8.1 本處應每年至少辦理乙次資訊安全教育訓練及宣導，以提高同仁資訊安全意識，促其遵守資訊安全規定。

8.2 資訊安全教育及訓練內容宜包括防毒、資料備份、法令法規等。

9 電腦系統作業程序及責任

9.1 對外開放網路服務應訂定作業程序。

9.2 應將測試與正式作業系統分開處理，並避免作業軟體或資料遭意外竄

改，或不當使用。

9.3 資訊業務委外時，應於事前審慎評估可能的潛在安全風險並與廠商簽訂適當的資訊安全協定，將相關的安全管理責任納入契約條款。

9.4 委外人員電腦通行使用權利應經適當控管；委外期間結束後，應立即收回該項權利。

10 日常作業之安全管理

10.1 對於電腦系統作業中斷（測試機除外）及更正等異常事項，應詳實記錄。

10.2 應監測電腦作業環境狀況。

10.3 營運(正式運作)中之程式需要維護時，應經過正式核准之程序辦理。

11 電腦病毒及駭客防範

11.1 電腦應設密碼、安裝防毒軟體，並即時更新系統漏洞修補。

12 網路安全管理

12.1 學校與外界網路連接網點應加裝防火牆，網路設備架構應定期檢討，得視需要建置入侵偵測系統，以因應各種網路攻擊。

12.2 本處應訂定網路被入侵時之處理程序及必要採取的行動。

13 全球資訊網之安全管理

13.1 對外開放網站不得透露任何含有敏感、個人隱私之資料。

14 系統存取控制規定

14.1 各單位應將其存取控制需求，明確告知本處，以利執行及維持有效之存

取控制機制。

15 系統存取管理

15.1 本處應建立系統使用者註冊管理制度。

15.2 系統存取權限之配賦，應以執行業務及職務所需者為限。

15.3 應以安全有效的使用者通行碼管理系統鑑別使用者身份。

15.4 對於使用者忘記密碼之處理，應有身分確認程序，方可再次使用系統。

15.4.1 身分確認程序如：檢查身分證件、電話回撥、詢問該單位主管等

16 系統安全需求規劃：

16.1 新發展或現有資訊系統功能之強化，應在系統規劃之需求階段，即將安全需求納入系統功能。

17 系統變更及維護環境安全

17.1 營運系統變更作業，皆應獲得權責主管人員同意。

17.2 應用系統變更應有備份處理措施。

17.3 委外建置或維護軟硬體設施時，應有相關人員監督及陪同下為之。

18 機房管理：

18.1 電腦機房應有門禁管制，並設置防火設施及緊急照明設備。

19 設備安全管理

19.1 設備應安置在適當地點予以保護。

19.2 對外提供網路服務設備應使用不斷電系統。

19.3 含有儲存媒體的設備，應在異動前詳加檢查，並確保任何機密性資料及版權軟體已被移除。

20 備份

20.1 重要主機系統應定期備份，包括完整系統備份、系統架構設定備份。

20.2 系統開發組所開發之原始程式碼應定期備份，並定期進行還原測試，以確保備份資料之可用性。

21 災害復原

21.1 關鍵業務應訂災害復原緊急處理作業說明，以減少負面衝擊。

22 政策審查

本政策應每年至少審查乙次，以反映政府法令、技術及業務等最新發展現況，並確保本處業務永續運作之能力。

23 實施與修訂

本政策經「資訊安全委員會」核定後實施，修訂時亦同。