

玄奘大學

資訊安全政策

機密等級：一般

文件編號：HCU-ISMS-A-001

版次：2.2

發行日期：112.11.07

資訊安全政策					
文件編號	HCU-ISMS-A-001	機密等級	一般	版次	2.2

目錄

1	目的	1
2	適用範圍	1
3	目標	2
4	責任	2
5	管理指標	2
6	審查	4
7	實施	4

資訊安全政策					
文件編號	HCU-ISMS-A-001	機密等級	一般	版次	2.2

1 目的

為確保玄奘大學(以下簡稱本校)所屬之資訊資產的機密性、完整性及可用性，以符合相關法令、法規之要求，使其免於遭受內、外部蓄意或意外之威脅，並衡酌本中心之業務需求，訂定本政策。

2 適用範圍

2.1 本政策適用範圍為本校員工、接觸本校業務資料之外機關人員、委外服務廠商與訪客等。

2.2 資訊安全管理範疇涵蓋 14 項領域，避免因人為疏失、蓄意或天然災害等因素，導致資料不當使用、洩漏、竄改、破壞等情事發生，對本中心造成各種可能之風險及危害，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 人力資源安全。

2.2.4 資產管理。

2.2.5 存取控制。

2.2.6 密碼學(加密控制)。

2.2.7 實體及環境安全。

2.2.8 運作安全。

2.2.9 通訊安全。

2.2.10 系統獲取、開發及維護。

2.2.11 供應者關係。

2.2.12 資訊安全事故管理。

2.2.13 營運持續管理之資訊安全層面。

2.2.14 遵循性。

資訊安全政策					
文件編號	HCU-ISMS-A-001	機密等級	一般	版次	2.2

3 目標

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

- 3.1 保護本校資訊業務服務之安全，確保資訊需經授權人員才可存取資訊，以確保其機密性。
- 3.2 保護本校資訊業務服務之安全，避免未經授權的修改，以確保其正確性與完整性。
- 3.3 建立本校資訊業務永續運作計畫，以確保本校資訊業務服務之持續運作，確保經授權個體因應需求之可存取及可使用。
- 3.4 確保本校各項資訊業務服務之執行須符合相關法令或法規之要求。

4 責任

- 4.1 成立資訊安全暨個人資料保護委員會統籌相關業務推動，政策之核定及監督，資訊安全事件預防及危機處理。
- 4.2 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。
- 4.3 本校全體人員、委外服務廠商與訪客等皆應遵守本政策。
- 4.4 本校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、個資事件或弱點。
- 4.5 任何危及資訊安全或個人資料隱私之行為，將視情節輕重追究其民事、刑事及行政責任或依本校之相關規定進行議處。

5 管理指標

為評量資訊安全管理目標達成情形，特訂定資訊安全管理指標如下：

5.1 定量化指標

資訊安全政策					
文件編號	HCU-ISMS-A-001	機密等級	一般	版次	2.2

5.1.1 確保本校資訊服務可用性之要求如下：

5.1.1.1 資訊機房維運服務達全年上班時間 96%以上。

5.1.1.2 關鍵業務系統服務達全年上班時間 94%以上。

5.1.2 確保因資通安全事件、異常事件、其他安全事故所造成系統、主機異常而中斷營運服務之情事，每年不得超過次數如下：

5.1.2.1 資訊機房維運服務中斷，每季不得超過 3 次。

5.1.2.2 關鍵業務系統服務中斷，每季不得超過 4 次。

5.1.3 確保因資通安全事件、異常事件、其他安全事故所造成系統、主機異常而中斷營運服務之情事，每次最長不得超過工作小時要求如下：

5.1.3.1 資訊機房維運服務中斷，每次最長不得超過 8 工作小時。

5.1.3.2 關鍵業務系統服務中斷，每次最長不得超過 8 工作小時。

5.1.4 應適當保護本校資訊資產之機密性與完整性，每年至少需進行乙次風險評鑑及風險管理。

5.1.5 為確保資訊需經權責單位授權才可存取，以確保其機密性，每年發生機密等級資訊外洩之事件不得超過乙次。

5.1.6 為確保本校教職員生資料(如：學籍系統資料庫)之正確性與完整性，每年應無發生資料遭未經授權竄改之事件。

5.1.7 為確保本校資訊安全措施或規範符合現行法令、法規之要求，每年至少需稽核乙次。

5.1.8 維護及演練業務永續運作計畫每年至少需進行乙次，以確保本校資訊業務服務得以持續運作。

5.2 定性化指標

5.2.1 應定期審查本校資訊安全組織人員執掌，以確保資訊安全工作之推展。

資訊安全政策					
文件編號	HCU-ISMS-A-001	機密等級	一般	版次	2.2

- 5.2.2 應符合主管機關之要求，依員工職務及責任提供適當之資訊安全相關訓練。
- 5.2.3 應加強本校資訊機房設施之環境安全，採取適當之保護及權限控管機制。
- 5.2.4 應確保資訊不因傳遞過程，或無意間之行為，透漏給未經授權之第三者。
- 5.2.5 應加強存取控制，防止未經授權之不當存取，以確保本校資訊資產已受適當之保護。
- 5.2.6 本校資訊系統開發應考量安全需求，並定期稽核安全弱點。
- 5.2.7 應確保所有資訊安全事件或可疑之安全弱點，均依循適當之通報機制向上反應，並予以適當調查及處理。
- 5.2.8 進行資訊處理時，若含有個人資料，應依據「個人資料保護法」及相關規定審慎處理，不私自蒐集或洩漏業務資訊，非公務用途嚴禁調閱使用。

6 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，並確保本校業務永續運作之能力。

7 實施

本政策經「資訊安全暨個人資料保護委員會」核定後公告實施，修訂時亦同。