仁德醫護管理專科學校

資訊安全政策

文件編號：JENTE-IS-A-001
機密等級：一般

版　　次：1.0

發行日期：112.12.19

修　訂　紀　錄				
版次	修訂日期	修訂頁次	修訂者	修訂內容摘要

目　錄

1 目的

為確保仁德醫護管理專科學校（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，並衡酌本校之業務需求，訂定本政策。

2 適用範圍

2.1 本政策適用範圍為本校之全體人員、委外服務廠商、工讀生與訪客等。

2.2 資訊安全管理範疇涵蓋 11 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，對本校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 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 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 確保本校業務資訊需經權責單位授權才可存取，以維護其機密性。

3.2 確保本校業務資訊之正確與完整，避免被竄改或損壞。

3.3 確保本校各項業務之執行須符合相關法令或法規之要求。

4 責任

4.1 本校應成立資訊安全組織統籌資訊安全事項推動。

4.2 管理階層應積極參與並支持資訊安全管理制度，並透過適當標準及程序實施本政策。

4.3 本校全體人員、委外服務廠商、工讀生與訪客等皆應遵守本政策。

4.4 本校全體人員均有責任透過適當通報機制，通報資訊安全事件或弱點。

4.5 任何危及資訊安全之行為，將視情節輕重依本校相關規定進行議處。

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

5.1.1 確保資訊機房維運服務達全年上班時間 97%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，每季不得超過 3 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，每次最長不得每次最長不得超過 4 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 為確保本校資訊安全措施或規範符合現行法令、法規之要求，每兩年至少需執行乙次內部稽核。

5.1.6 維護及演練業務永續運作計畫每兩年至少需進行乙次，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。

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，並定期稽核系統安全弱點。

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。

6 審查

本政策應每兩年至少審查乙次，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

本政策經仁德醫護管理專科學校行政會議通過後實施，修改時亦同。