

宏國學校財團法人宏國德霖科技大學 資訊安全政策

民國104年6月15日103學年度第2學期第1次資訊安全暨個人資料保護委員會會議通過

民國106年7月25日105學年度第2學期第3次校務會議修正通過

1. 目的

規範宏國學校財團法人宏國德霖科技大學(以下簡稱本校) 資訊安全管理制度，以確保本校管轄資訊資產之機密性、完整性、可用性及符合相關法規之要求，進而保障全校教職員工生之權益。

2. 適用範圍

本校教職員工、接觸本校業務資料之外機關人員、委外服務提供廠商人員及訪客。

3. 名詞定義

- 3.1. 機密性 (Confidentiality)：使資訊不可用或不揭露給未經授權之個人、個體或過程的性質。
- 3.2. 完整性(Integrity)：保護資產的準確度(Accuracy)和完全性(Completeness)的性質。
- 3.3. 可用性 (Availability)；經授權個體因應需求之可存取及可使用的性質。
- 3.4. 資訊安全：係避免因人為疏失、蓄意或自然災害等風險，運用系統化之控制措施，包含政策、實施、稽核、組織結構和軟硬體功能等，以確保本校資訊資產受到妥善保護。
- 3.5. 資訊資產：凡本校作業流程中使用之資訊資產，如內部人員、外部人員、紙本文件、電子文件、網路服務、電腦應軟體、應用系統、電腦硬體、網路設備、環控系統、建築保護設施與便利設施等皆屬之。

4. 權責

設置本校「資訊安全暨個人資料保護委員會」，負責政策之核定及監督、資訊安全預防及危機處理。

5. 要求事項

5.1. 資訊安全管理涵蓋 14 項管理事項

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，對本校帶來各種可能之風險及危害。管理事項如下：

- (1) 安全政策。
- (2) 資訊安全之組織。
- (3) 人力資源安全。
- (4) 資產管理。
- (5) 存取控制。
- (6) 密碼學。

- (7) 實體及環境安全。
- (8) 運作安全。
- (9) 通訊安全。
- (10) 系統獲取、開發及維護。
- (11) 供應者關係。
- (12) 資訊安全事故管理
- (13) 營運持續管理之資訊安全層面
- (14) 遵循性

5.2. 管理階層承諾

- 5.2.1. 重要之資訊資產應定期清查、分類分級與進行風險評鑑，並據以實施適當的防護措施。
- 5.2.2. 重要資訊資產存取權限應予以區分，考量人員職務授予相關權限，必要時得採行加解密及身分鑑別機制，以加強資訊資產之安全。
- 5.2.3. 對於資訊安全事件須有完整的通報及應變措施，以確保資訊系統、業務的持續運作。
- 5.2.4. 應訂定營運持續計畫並不定期演練，以確保重要系統、業務於資安事故發生時能於預定時間內恢復作業。
- 5.2.5. 相關人員應依規定接受資訊安全教育訓練與宣導，以加強資訊安全認知。
- 5.2.6. 定期執行資訊安全稽核作業，檢視存取權限及資訊安全管理制度之落實。

6. 施行

- 6.1. 本政策須經「資訊安全暨個人資料保護委員會」進行審議後公告使用，修訂時亦同。