萬能科技大學

資訊安全政策

機密等級：一般

文件編號：IS-A-001

版　　次：2.8

發行日期：114 年 12 月 2 日

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	97 年 9 月 9 日		邱泰毅	初版
1.1	99 年 11 月 30 日	2	邱泰毅	修改 3.目標，維護本校資訊資產之機密性、完整性與可用性，並依據個人資料保護法保障個人資料隱私。
1.2	101 年 7 月 10 日	2	邱泰毅	修改: 1. 目的，為維護萬能科技大學(以下簡稱本校)所屬之核心業務相關資訊資產... 2. 適用範圍，本政策適用於電子計算機中心之機房維運管理及師生教學活動資訊系統之維護管理，資訊安全管理涵蓋 11 項管理事項，以避免因人為疏失... 3. 目標，維護本校電子計算機中心之機房維運管理及師生教學活動資訊系統之維護管理相關資訊資產之機密性、完整性與可用性，並依據「教育體系資訊安全管理規範」、「個人資料保護法」等相關法令與規定，保障個人資料隱私。... 3.3 建立資訊業務永續運作計畫，每年至少測試一次以確保業務永續經營計畫之可行性。 3.4 電子計算機中心之機房維運之核心業務全年達99%以上之可用性。 3.5 資安事件每年發生率低於10 次。

1.3	102 年 3 月 1 日	2	邱泰毅	3.4 電子計算機中心之機房維運之核心業務全年達 99.5%以上之可用性。
1.4	102 年 6 月 4 日	2	邱泰毅	3.4 電子計算機中心之機房維運之核心業務全年達 99%以上之可用性。
1.5	102 年 12 月 31 日	1,2	邱泰毅	單位名稱電子計算機中心變更為圖書資訊中心
1.6	103 年 12 月 30 日	1,2	邱泰毅	施作範圍「機房維運管理及師生教學活動資訊系統之維護管理」變更為「中心機房及個人入口網系統維運管理」 3.4 圖書資訊中心之機房維運之核心業務全年達 99.5%以上之可用性。 3.5 資安事件每年發生率低於 5 次。
1.7	104 年 12 月 13 日	2	邱泰毅	3.4 圖書資訊中心之機房維運之核心業務全年達 99.6%以上之可用性
2.0	106 年 10 月 3 日	1,2,3	邱泰毅	配合新版教育體系資通安全暨個人資料管理規範修訂相關條文、適用範圍與政策審查單位。

新版資安規範(14 控制領域)	原有資安規範(11 控制領域)
A.5 資訊安全政策訂定與評估	A.5 資訊安全政策訂定與評估
A.6 資訊安全組織	A.6 資訊安全組織
A.7 人力資源安全	A.8 人員安全管理與教育訓練
A.8 資產管理	A.7 資訊資產分類與管制
A.9 存取控制	A.11 存取控制安全
A.10 密碼學(加密控制)	
A.11 實體及環境安全	A.9 實體與環境安全
A.12 運作安全	A.10 通訊與作業安全管理
A.13 通訊安全	A.10 通訊與作業安全管理
A.14 系統獲取、開發及維護	A.12 系統開發與維護之安全
A.15 供應者關係	
A.16 資訊安全事件管理	A.13 資訊安全事件之反應及處理
A.17 業務永續運作管理	A.14 業務永續運作管理

		A.18 遵循性	A.15 相關法規與施行單位政策之符合性	
2.1	107 年 3 月 6 日	1	邱泰毅	調整 2.12
2.2	110 年 1 月 27 日	1、3	劉珊妤	調整 2 及 5
2.3	110 年 3 月 23 日	1、2	劉珊妤	調整 2 及 3
2.4	110 年 10 年 19 日	1、2	劉珊妤	調整 2 及 3
2.5	111 年 12 年 20 日	1、2	資訊安全暨個人資料保護推動委員會	調整 2 及 3
2.6	112 年 12 月 5 日	1~4	資訊安全暨個人資料保護推動委員會	配合全校導入資訊安全進行修訂
2.7	113 年 12 月 3 日	2	資訊安全暨個人資料保護推動委員會	調整 5.1
2.8	114 年 12 月 2 日	2	資訊安全暨個人資料保護推動委員會	調整 5.1

資訊安全政策					
文件編號	IS-A-001	機密等級	一般	版次	2.8

目錄

1 目的 1

2 適用範圍 1

3 名詞定義 1

4 權責 1

5 要求事項 1

6 修訂 3

7 實施 3

資訊安全政策					
文件編號	IS-A-001	機密等級	一般	版次	2.8

1 目的

本政策規範萬能科技大學（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

2 適用範圍

本校員工、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推動委員會」，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 資訊安全目標

維護本校使用核心業務的各單位相關資訊資產之機密性、完整性與可用性，並依據教育體系資通安全暨個人資料管理規範等相關法令及契約對

施行單位資訊安全的要求與規定，保障個人資料隱私。藉由全體同仁共同努力來達成下列目標：

5.1.1保護本校業務活動資訊，避免未經授權的存取。

5.1.2保護本校業務活動資訊，避免未經授權的修改，確保其正確完整。

5.1.3建立資訊業務永續運作計畫，每二年測試一次以確保業務永續經營計畫之可行性。

5.1.4圖書資訊中心之機房維運之核心業務全年達 99.96 以上之可用性。

5.1.5資安事件每年發生率低於 2 次。

5.2 資訊安全管理事項

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。資訊安全管理應涵蓋 14 項管理事項：

1.資訊安全政策。

2. 資訊安全組織。

3. 人力資源安全。

4. 資產管理。

5. 存取控制。

6. 密碼學(加密控制)。

7. 實體與環境安全。

8. 運作安全

9.通訊安全

10.資訊系統取得、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。

5.3 資訊安全管理原則

5.3.1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。

5.3.2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。

5.3.3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。

5.3.4應訂定營運持續計畫並定期演練，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。

5.3.5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。

5.3.6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。

5.3.7違反本政策與資訊安全相關規範，依相關法規或本校懲戒規定辦理。

5.3.8本政策每年至少評估一次，依業務變動、技術發展及風險評鑑的結果修訂。

6 修訂

6.1 管理階層審查

6.1.1確保「資訊安全管理系統」實務運作之可用性、安全性及有效性。本政策每年依業務變動、技術發展及風險評鑑的結果或配合政府資訊安全管理要求、法令、技術及最新業務發展現況至少評估或修訂一次。

7 實施

7.1 資訊安全政策配合管理審查會議進行資訊安全政策審核。

7.2 本政策經資訊安全暨個人資料保護推動委員會核定後公告實施，修訂時亦同。