國立臺灣師範大學

資訊安全政策

文件編號：NTNU-ISMS-A-001

機密等級：一般

版　　次：3.1

發行日期：113.12.30

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	99.10.07		柯文傑	初版發行
1.1	103.09.23	1,2	柯文傑	因應 ISO 27001:2013 新版標準進行調整，刪除管理指標無法量測部分
1.2	103.12.29	2	柯文傑	因應內部稽核發現調整 4.2、修改 5.1.1.1
1.3	104.12.21	2	柯文傑	修改 5.1.1.2
1.4	110.12.28	2	柯文傑	5.1.1.1 由 98%修改成 99% 5.1.1.2 由 98%修改成 99% 5.1.2.1 由 3 次修改成 2 次 5.1.2.2 由 3 次修改成 2 次
3.0	112.06.28	全	柯文傑	本版次於112年6月28日111學年度第一次資訊安全暨個人資料保護委員會修正通過。 修正摘要如下： 1. ISMS 範圍擴大到全校 2. 核定組織變更成「資訊安全暨個人資料保護委員會」
3.1	113.12.30	1、2	柯文傑	配合 ISO27001:2022 及教育部資通安全稽核建議事項修訂

`目　錄

1 目的

國立臺灣師範大學（以下簡稱「本校」）為確保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、委外服務廠商與訪客等。

2.2 資訊安全管理範疇涵蓋 4 大控制主題，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，各控制主題分述如下：

2.2.1 組織控制

2.2.2 人力控制

2.2.3 實體控制

2.2.4 技術控制

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，期藉由本政策之實施以達成下列目標：

3.1 保護本校業務服務之安全，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 建立本校業務永續運作計畫，以確保本校業務服務之持續運作。

3.4 確保本校各項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 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、支持及承諾持續改善資訊安全管理制度，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，通報資訊安全事件或弱點。

4.5 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

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服務時間 99%以上。

5.1.1.2 關鍵業務系統服務達全年服務時間 99%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，每次最長不得超過工作小時要求如下：

5.1.2.1 資訊機房維運服務中斷，每次最長不得超過 4 工作小時。

5.1.2.2 關鍵業務系統服務中斷，每次最長不得超過 4 工作小時。

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情況，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」核定後實施，修訂時亦同。