

國立臺灣戲曲學院

「資訊安全管理系統」

資訊安全政策

機密等級：一般

文件編號：TCPA-ISMS-A-001

版本編號：1.0

制訂日期：2022年5月 日

使用本文件前，如對版本有疑問，請與修訂者確認最新版次。

本文件歷次變更紀錄：

版次	修訂日	修訂者	說明	核准者
1.0	2022年 5月 日	資訊安全執行小組	初版發行	召集人

本聲明書由資訊安全執行小組負責維護。

目錄：

1	目的	3
2	適用範圍	3
3	目標	3
4	責任	4
5	審查	4
6	實施	5

1 目的

- 1.1 為確保國立臺灣戲曲學院（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和遵循本校資訊安全政策，訂定本中心資訊安全政策。

2 適用範圍

- 2.1 本政策適用範圍為本校之內部人員、委外服務廠商與訪客等相關人員。
- 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，藉由本校全體人員共同努力達成下列目標：

3.1 定性化目標

3.1.1 保護業務服務之安全，確保資訊經授權人員才可存取，以確保其機密性。

3.1.2 保護業務服務之安全，避免未經授權的修改，以確保其正確性與完整性。

3.1.3 建立業務永續運作計畫，以確保業務服務之持續運作。

3.1.4 確保各項業務服務之執行符合相關法令或法規之要求。

3.1.5 確保所有資安事件、意外事件或可疑之安全弱點，都應依循適當通報機制向上反應，予以適當調查及處理。

3.2 定量化目標

3.2.1 確保機房內核心系統電力、空調服務達到全年 90% 以上之可用性。

3.2.2 確保機房內核心系統業務服務達到全年 90% 以上之可用性。

3.2.3 核心系統服務中斷（3 級（含）以上）每年發生次數低於 10 次。

4 責任

4.1 本校「資通安全暨個人資料保護推動委員會」設立「資通安全執行小組」統籌本中心資訊安全事項推動。

4.2 本校各級主管應積極參與及支持資訊安全管理制度，並透過所制訂的相關標準和程序來達成本政策。

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 審查

5.1 本政策每年至少應審查一次，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。

6 實施

- 6.1 本政策經「資通安全暨個人資料保護推動委員會管理審查會議」核定後實施，修訂時亦同。