國立臺灣戲曲學院

「資訊安全管理系統」
適用性聲明書

機密等級：一般

文件編號：TCPA-ISMS-A-002

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

1.1 適用性聲明 （Statement of Applicability, SOA）明列國立臺灣戲曲學院（以下簡稱本校）資訊安全管理制度之管理架構的目標、控制及對策。

2 範圍

2.1 適用於本校核心業務資訊系統全球資訊網及機房維運管理。

3 名詞定義

3.1 無。

4 權責

4.1 本校人員：遵守適用性聲明之要求。

4.2 「資通安全暨個人資料保護推動委員會」：覆核適用性聲明書。

5 作業說明

5.1 適用性聲明的內容來自於風險評鑑程序辨認出來的控制。

5.2 以風險評鑑及風險管理程序結果，選擇適用的控制措施、制定資訊安全管理制度文件詳「TCPA-ISMS-B-002_文件管理程序書」之「TCPA-ISMS-D-007_資訊安全管理文件列表」，完成適用性聲明（SOA）的訂定。

5.3 列出沒有被選擇的控制措施，並說明其不適用或未被選擇的原因。

6 作業流程

6.1 無。

7 參考文件

7.1 文件管理程序書。

ISO 27001 標準要求	適用性	對應文件	理由及補充說明（註）
附錄 A：控制目標及控制項			
A.5 資訊安全政策			
A.5.1 資訊安全政策			
A.5.1.1 資訊安全政策文件	適用	TCPA-ISMS-A-001_資訊安全政策	1
A.5.1.2 資訊安全政策的審查	適用	TCPA-ISMS-A-001_資訊安全政策	1
A.6 資訊安全之組織			
A.6.1 內部組織			
A.6.1.1 資訊安全之角色與職責	適用	TCPA-ISMS-B-001_資訊安全組織程序書	3
A.6.1.2 職務的區隔	適用	TCPA-ISMS-B-007_通訊與作業管理程序書	2
A.6.1.3 與權責機關之聯繫	適用	TCPA-ISMS-B-001_資訊安全組織程序書	3
A.6.1.4 與特殊利害相關團體之聯繫	適用	TCPA-ISMS-B-001_資訊安全組織程序書	3
A.6.1.5 專案管理之資訊安全	適用	TCPA-ISMS-B-010_委外管理程序書	3
A.6.2 行動裝置與遠距工作			
A.6.2.1 行動裝置政策	適用	TCPA-ISMS-B-007_通訊與作業管理程序書	1
A.6.2.2 遠距工作	適用	TCPA-ISMS-B-007_通訊與作業管理程序書 TCPA-ISMS-C-002_網路及系統安全管理說明書	3
A.7 人力資源安全			
A.7.1 聘雇之前			
A.7.1.1 篩選	適用	TCPA-ISMS-B-005_人員安全與教育訓練程序書	3
A.7.1.2 聘僱條款與條件	適用	TCPA-ISMS-B-005_人員安全與教育訓練程序書 TCPA-ISMS-B-010_委外管理程序書	3
A.7.2 聘僱期間			
A.7.2.1 管理階層責任	適用	TCPA-ISMS-B-001_資訊安全組織程序書 TCPA-ISMS-B-005_人員安全與教育訓練程序書	3
A.7.2.2 資訊安全認知、教育及訓	適用	TCPA-ISMS-B-005_人員安	3

練		全與教育訓練程序書	
A.7.2.3 懲處過程	適用	TCPA-ISMS-B-005_人員安全與教育訓練程序書	3
A.7.3 聘雇終止或變更			
A.7.3.1 聘僱責任之終止或變更	適用	TCPA-ISMS-B-005_人員安全與教育訓練程序書	2、3
A.8 資產管理			
A.8.1 資產責任			
A.8.1.1 資產清冊	適用	TCPA-ISMS-B-003_資訊資產管理程序書	3
A.8.1.2 資產之擁有權	適用	TCPA-ISMS-B-003_資訊資產管理程序書	3
A.8.1.3 資產的可接受使用	適用	TCPA-ISMS-C-001_資訊資產管理說明書	3
A.8.1.4 資產之歸還	適用	TCPA-ISMS-C-001_資訊資產管理說明書	3
A.8.2 資訊分類			
A.8.2.1 資訊之分類	適用	TCPA-ISMS-B-003_資訊資產管理程序書	3
A.8.2.2 資訊之標示	適用	TCPA-ISMS-B-003_資訊資產管理程序書	3
A.8.2.3 資產之處置	適用	TCPA-ISMS-B-003_資訊資產管理程序書	3
A.8.3 媒體處置			
A.8.3.1 可移除式媒體之管理	適用	TCPA-ISMS-C-001_資訊資產管理說明書	3
A.8.3.2 媒體之汰除	適用	TCPA-ISMS-C-001_資訊資產管理說明書	3
A.8.3.3 實體媒體傳送	適用	TCPA-ISMS-C-001_資訊資產管理說明書	3
A.9 存取控制			
A.9.1 存取控制的營運要求			
A.9.1.1 存取控制政策	適用	TCPA-ISMS-B-008_存取控制管理程序書	1
A.9.1.2 網路與網路服務之存取	適用	TCPA-ISMS-B-008_存取控制管理程序書 TCPA-ISMS-B-007_通訊與作業管理程序書 TCPA-ISMS-C-002_網路及系統安全管理說明書	2、3
A.9.2 使用者存取管理			

A.9.2.1 使用者註冊與註銷	適用	TCPA-ISMS-B-008_存取控制管理程序書 TCPA-ISMS-C-004_帳號及通行密碼管理說明書	2、3
A.9.2.2 使用者之存取配置	適用	TCPA-ISMS-B-008_存取控制管理程序書 TCPA-ISMS-C-004_帳號及通行密碼管理說明書	2、3
A.9.2.3 存取之特權管理	適用	TCPA-ISMS-B-008_存取控制管理程序書 TCPA-ISMS-C-004_帳號及通行密碼管理說明書	2、3
A.9.2.4 使用者之機密鑑別資訊的管理	適用	TCPA-ISMS-B-008_存取控制管理程序書 TCPA-ISMS-C-004_帳號及通行密碼管理說明書	2、3
A.9.2.5 使用者存取權限之審查	適用	TCPA-ISMS-B-008_存取控制管理程序書 TCPA-ISMS-C-004_帳號及通行密碼管理說明書	2、3
A.9.2.6 存取權限之移除或調整	適用	TCPA-ISMS-B-008_存取控制管理程序書 TCPA-ISMS-C-004_帳號及通行密碼管理說明書	2、3
A.9.3 使用者責任			
A.9.3.1 機密鑑別資訊之使用	適用	TCPA-ISMS-B-008_存取控制管理程序書 TCPA-ISMS-C-004_帳號及通行密碼管理說明書	2、3
A.9.4 系統與應用存取控制			
A.9.4.1 資訊存取限制	適用	TCPA-ISMS-B-009_系統開發與維護程序書	2、3
A.9.4.2 保全登入程序	適用	TCPA-ISMS-B-009_系統開發與維護程序書	2、3
A.9.4.3 通行碼管理系統	適用	TCPA-ISMS-B-009_系統開發與維護程序書	2、3
A.9.4.4 特許系統公用程式之使用	適用	TCPA-ISMS-B-009_系統開發與維護程序書	2、3
A.9.4.5 程式原碼之存取控制	適用	TCPA-ISMS-B-009_系統開發與維護程序書	2、3

A.10 密碼			
A.10.1 密碼控制措施			
A.10.1.1 使用密碼控制措施的政策	適用	TCPA-ISMS-B-009_系統開發與維護程序書	2、3
A.10.1.2 金鑰管理	適用	TCPA-ISMS-B-009_系統開發與維護程序書	3
A.11 實體與環境安全			
A.11.1 安全區域			
A.11.1.1 實體安全周界	適用	TCPA-ISMS-B-006_實體安全管理程序書	3
A.11.1.2 實體進入控制措施	適用	TCPA-ISMS-B-006_實體安全管理程序書	3
A.11.1.3 保護辦公處所及設施	適用	TCPA-ISMS-B-006_實體安全管理程序書	3
A.11.1.4 不受外在及環境的威脅	適用	TCPA-ISMS-B-006_實體安全管理程序書	3
A.11.1.5 在安全區域內工作	適用	TCPA-ISMS-B-006_實體安全管理程序書	3
A.11.1.6 公共存取、收發、及裝卸區	適用	TCPA-ISMS-B-006_實體安全管理程序書	3
A.11.2 設備安全			
A.11.2.1 設備安置與保護	適用	TCPA-ISMS-B-006_實體安全管理程序書	3
A.11.2.2 支援之共用設備	適用	TCPA-ISMS-B-006_實體安全管理程序書	3
A.11.2.3 佈纜之安全	適用	TCPA-ISMS-B-006_實體安全管理程序書	3
A.11.2.4 設備維護	適用	TCPA-ISMS-B-006_實體安全管理程序書	3
A.11.2.5 資產之攜出	適用	TCPA-ISMS-B-006_實體安全管理程序書	3
A.11.2.6 場外設備及資產之安全	適用	TCPA-ISMS-B-006_實體安全管理程序書	3
A.11.2.7 設備之安全汰除或再使用	適用	TCPA-ISMS-C-001_資訊資產管理說明書	3
A.11.2.8 無人看管之使用者設備	適用	TCPA-ISMS-B-008_存取控制管理程序書	3
A.11.2.9 桌面淨空與螢幕淨空政策	適用	TCPA-ISMS-B-008_存取控制管理程序書	3
A.12 運作管理			

A.12.1 運作程序與職責			
A.12.1.1 文件化運作程序	適用	TCPA-ISMS-B-007_通訊與作業管理程序書	3
A.12.1.2 變更管理	適用	TCPA-ISMS-B-007_通訊與作業管理程序書	3
A.12.1.3 容量管理	適用	TCPA-ISMS-B-007_通訊與作業管理程序書	3
A.12.1.4 開發、測試與運作環境之分隔	適用	TCPA-ISMS-B-007_通訊與作業管理程序書	3
A.12.2 防範惡意軟體			
A.12.2.1 對抗惡意軟體之控制措施	適用	TCPA-ISMS-C-003_惡意軟體防護管理說明書	3
A.12.3 備份			
A.12.3.1 資訊備份	適用	TCPA-ISMS-B-007_通訊與作業管理程序書 TCPA-ISMS-C-005_資訊備份管理說明書	3
A.12.4 存錄與監控			
A.12.4.1 事件存錄	適用	TCPA-ISMS-B-007_通訊與作業管理程序書	3
A.12.4.2 日誌資訊之保護	適用	TCPA-ISMS-B-007_通訊與作業管理程序書	3
A.12.4.3 管理者與操作者日誌存取控制	適用	TCPA-ISMS-B-007_通訊與作業管理程序書	3
A.12.4.4 鐘訊同步	適用	TCPA-ISMS-B-007_通訊與作業管理程序書	3
A.12.5 運作中軟體之控制			
A.12.5.1 運作中系統之軟體的安裝	適用	TCPA-ISMS-B-007_通訊與作業管理程序書	3
A.12.6 技術性弱點的管理			
A.12.6.1 技術性弱點的管理	適用	TCPA-ISMS-B-007_通訊與作業管理程序書	3
A.12.6.2 軟體安裝之限制	適用	TCPA-ISMS-B-007_通訊與作業管理程序書	3
A.12.7 資訊系統稽核考量			
A.12.7.1 資訊系統稽核控制	適用	TCPA-ISMS-B-007_通訊與作業管理程序書	3
A.13 通訊管理			
A.13.1 網路安全管理			
A.13.1.1 網路控制措施	適用	TCPA-ISMS-B-007_通訊與	3

		作業管理程序書	
A.13.1.2 網路服務之安全	適用	TCPA-ISMS-B-007_通訊與作業管理程序書 TCPA-ISMS-C-002_網路及系統安全管理說明書	3
A.13.1.3 網路區隔	適用	TCPA-ISMS-B-007_通訊與作業管理程序書 TCPA-ISMS-C-002_網路及系統安全管理說明書	3
A.13.2 資訊傳送			
A.13.2.1 資訊傳送政策與程序	適用	TCPA-ISMS-B-007_通訊與作業管理程序書 TCPA-ISMS-C-002_網路及系統安全管理說明書	3
A.13.2.2 資訊傳送協議	適用	TCPA-ISMS-B-007_通訊與作業管理程序書 TCPA-ISMS-C-002_網路及系統安全管理說明書	3
A.13.2.3 電子傳訊	適用	TCPA-ISMS-B-007_通訊與作業管理程序書 TCPA-ISMS-C-002_網路及系統安全管理說明書	3
A.13.2.4 機密性或保密協議	適用	TCPA-ISMS-B-007_通訊與作業管理程序書 TCPA-ISMS-C-002_網路及系統安全管理說明書 TCPA-ISMS-B-010_委外管理程序書	3
A.14 系統獲取、開發及維護			
A.14.1 資訊系統之安全要求			
A.14.1.1 安全要求分析與規格	適用	TCPA-ISMS-B-009_系統開發與維護程序書	3
A.14.1.2 公共網路之安全的應用服務	適用	TCPA-ISMS-C-002_網路及系統安全管理說明書	3
A.14.1.3 應用服務交易之保護	不適用	TCPA-ISMS-C-002_網路及系統安全管理說明書	3
A.14.2 開發與支援過程的安全			
A.14.2.1 安全開發政策	適用	TCPA-ISMS-B-009_系統開發與維護程序書	3
A.14.2.2 系統變更控制程序	適用	TCPA-ISMS-B-009_系統開	3

		發與維護程序書	
A.14.2.3 作業系統變更後的應用系統技術審查	適用	TCPA-ISMS-B-009_系統開發與維護程序書	3
A.14.2.4 套裝軟體變更之限制	適用	TCPA-ISMS-B-009_系統開發與維護程序書	3
A.14.2.5 安全系統工程原則	適用	TCPA-ISMS-B-009_系統開發與維護程序書	3
A.14.2.6 開發環境之安全	適用	TCPA-ISMS-B-009_系統開發與維護程序書	3
A.14.2.7 委外之開發	適用	TCPA-ISMS-B-009_系統開發與維護程序書	3
A.14.2.8 系統安全測試	適用	TCPA-ISMS-B-009_系統開發與維護程序書 TCPA-ISMS-C-006_系統開發與維護作業說明書	3
A.14.2.9 系統驗收測試	適用	TCPA-ISMS-B-009_系統開發與維護程序書 TCPA-ISMS-C-006_系統開發與維護作業說明書	3
A.14.3 測試資料			
A.14.3.1 測試資料的保護	適用	TCPA-ISMS-B-009_系統開發與維護程序書 TCPA-ISMS-C-006_系統開發與維護作業說明書	3
A.15 供應者關係			
A.15.1 供應者關係之資訊安全			
A.15.1.1 供應者安全之資訊安全政策	適用	TCPA-ISMS-B-010_委外管理程序書	3
A.15.1.2 供應者協議中之安全的說明	適用	TCPA-ISMS-B-010_委外管理程序書	3
A.15.1.3 資訊與通訊技術供應鏈	適用	TCPA-ISMS-B-010_委外管理程序書	3
A.15.2 供應者服務之交付管理			
A.15.2.1 供應者服務之監視與審查	適用	TCPA-ISMS-B-010_委外管理程序書	3
A.15.2.2 供應者服務變更之管理	適用	TCPA-ISMS-B-010_委外管理程序書	3
A.16 資訊安全事故管理			
A.16.1 資訊安全事故管理與改進			
A.16.1.1 職責與程序	適用	TCPA-ISMS-B-011_安全事件管理程序書	3
A.16.1.2 通報資訊安全事件	適用	TCPA-ISMS-B-011_安全事	3

		件管理程序書	
A.16.1.3 通報資訊安全弱點	適用	TCPA-ISMS-B-011_安全事件管理程序書	3
A.16.1.4 資訊安全事件之評鑑與決策	適用	TCPA-ISMS-B-011_安全事件管理程序書	3
A.16.1.5 資訊安全事故之回應	適用	TCPA-ISMS-B-011_安全事件管理程序書	3
A.16.1.6 從資訊安全事故中學習	適用	TCPA-ISMS-B-011_安全事件管理程序書	3
A.16.1.7 證據之收集	適用	TCPA-ISMS-B-011_安全事件管理程序書	3
A.17 營運持續管理之資訊安全層面			
A.17.1 資訊安全持續			
A.17.1.1 資訊安全持續之規劃	適用	TCPA-ISMS-B-012_營運持續運作管理程序書	3
A.17.1.2 資訊安全持續之實作	適用	TCPA-ISMS-B-012_營運持續運作管理程序書	3
A.17.1.3 資訊安全持續之查證、審查與評估	適用	TCPA-ISMS-B-012_營運持續運作管理程序書	3
A.17.2 備援措施			
A.17.2.1 資訊處理設施之可用性	適用	TCPA-ISMS-B-012_營運持續運作管理程序書	3
A.18 遵循性			
A.18.1 法律與契約要求事項之遵循性			
A.18.1.1 識別適用之法律與契約的要求	適用	TCPA-ISMS-B-002_文件管理程序書 TCPA-ISMS-B-005_人員安全與教育訓練程序書 TCPA-ISMS-B-013_資訊安全稽核作業程序書	3
A.18.1.2 智慧財產權	適用	TCPA-ISMS-C-001_資訊資產管理說明書 TCPA-ISMS-B-013_資訊安全稽核作業程序書	3
A.18.1.3 紀錄之保護	適用	TCPA-ISMS-B-002_文件管理程序書 TCPA-ISMS-B-013_資訊安全稽核作業程序書	3
A.18.1.4 個人可識別資訊之保護與隱私	適用	TCPA-ISMS-B-002_文件管理程序書 TCPA-ISMS-B-013_資訊安全稽核作業程序書	3
A.18.1.5 密碼控制措施之法規	適用	TCPA-ISMS-B-002_文件管	3

		理程序書 TCPA-ISMS-B-009_系統開發與維護程序書	
A.18.2 資訊安全審查			
A.18.2.1 資訊安全之獨立審查	適用	TCPA-ISMS-B-001_資訊安全組織程序書 TCPA-ISMS-B-013_資訊安全稽核作業程序書	3
A.18.2.2 安全政策與標準之遵循性	適用	TCPA-ISMS-B-001_資訊安全組織程序書 TCPA-ISMS-B-013_資訊安全稽核作業程序書	3
A.18.2.3 技術遵循性審查	適用	TCPA-ISMS-B-001_資訊安全組織程序書 TCPA-ISMS-B-013_資訊安全稽核作業程序書	3

註：適用性理由及補充說明：
（1）政策要求
（2）風險評估的結果或降低風險所採取之措施
（3）運作需求或程序規範
（4）不適用理由如後