國家表演藝術中心資通安全維護計畫

108年6月17日文資字第1083017331號函核備
109年7月22日文資字第1093034682號函核備
111年6月24日文資字第1111016772號函核備
112年1月16日文資字第1121001168號函核備
112年6月 8日文資字第1123014653號函核備

目　　錄

壹、依據及目的

一、 依據資通安全管理法（以下簡稱本法）第10條及施行細則第6條訂定。
二、 國家表演藝術中心（以下簡稱本中心）由主管機關核定為資通安全責任等級C級公務機關。
三、 本中心為確保所屬單位之地域性、特殊性及獨立運作性，特訂定本資通安全維護計畫（以下簡稱本計畫），以供遵循。
四、 為落實本法資通安全責任等級C級之公務機關應辦事項，本中心所屬單位應導入IEC/ISO/CNS27001（以下簡稱ISMS），依ISMS控制目標及控制措施，訂立程序並確認符合本計畫要求。
五、 本中心所屬單位訂立ISMS控制目標及控制措施四階文件編號，應使用國際標準化組織定義用語及定義，文件編號統一使用ISMS。
六、 「行政院及所屬各機關資訊安全管理要點」已停止適用。本中心所屬單位完成ISMS導入後，亦停止適用電腦作業及資訊安全管理要點，以避免與本計畫競合。
七、 本中心之中心本部及國家交響樂團（以下簡稱樂團）資通業務執行運作，委由國家兩廳院辦理（以下簡稱兩廳院），應確實遵循資通安全法與ISMS各程序要求。

貳、適用範圍

本計畫適用於本中心內部組織、各場館及附設演藝團隊（以下簡稱所屬單位）。

參、核心業務及重要性

一、 核心業務及重要性：

所屬單位核心業務為表演藝術相關藝文活動經營管理與推廣，經營管理、表演藝術文化與活動之策劃、行銷、推廣及交流，以提升國家表演藝術水準及國際競爭力，定義核心系統為公文系統及票務系統。

核心業務	核心資通系統	重要性說明	業務失效影響說明	最大可容忍中斷時間
票務作業	票務系統	為主管機關核定資通安全責任等級C級機關所涉業務	發生資通安全事件致資通系統受影響時，可能造成對資訊、資通系統之存取或使用之中斷，對機關之營運、資產或信譽等方面將產生有限之影響。	72小時
公文作業	公文系統	為主管機關核定資通安全責任等級C級機關所涉業務	發生資通安全事件致資通系統受影響時，可能造成對資訊、資通系統之存取或使用之中斷，對機關之營運、資產或信譽等方面將產生有限之影響。	72小時

註：系統若於假日週間(週五下班後至週一上班前)發生故障，考量場館人員自行修護及合約規範廠商(包含硬體、應用系統及雲端服務等)可修護時程，最大可容忍中斷時間(Maximum Tolerable Period of Disruption, MTPD)訂為72小時。

二、 非核心業務及說明：

所屬單位非核心業務系統，每年應重新盤點乙次，並依照資通系統防護需求分級原則及資通系統防護基準，條列防護分級記錄於資通安全實施計畫實施情形。本中心非核心業務如下表(最大可容忍中斷時間均為72小時)：

1	兩廳院正航 ERP	26	樂團愛樂實驗室
2	兩廳院人事系統	27	樂團會員整合平台管理系統
3	兩廳院客服電話系統	28	衛武營ERP企業資源規劃系統
4	兩廳院場館設施服務系統	29	衛武營人事系統
5	兩廳院發行管理系統	30	衛武營行動支付整合系統
6	兩廳院POS系統	31	衛武營官網
7	兩廳院官網	32	衛武營入館人數統計系統
8	兩廳院表演藝術雜誌社官網	33	衛武營會員中心系統
9	兩廳院好藝網站	34	衛武營場館租借系統
10	兩廳院內部網站	35	衛武營後台空間溫濕度偵測系統
11	兩廳院客服線上系統	36	衛武營活動整合/排班系統

12	國表藝中心數位典藏系統（兩廳院負責管理）	37	衛武營電子郵件系統
13	兩廳院圖書館自動化系統	38	衛武營目錄服務系統
14	兩廳院出勤刷卡	39	臺中國家歌劇院 ERP 系統
15	兩廳院薦購系統	40	臺中國家歌劇院官網
16	兩廳院電力監控系統	41	臺中國家歌劇院 ZDPOS 門店管理系統
17	兩廳院空調監控系統	42	臺中國家歌劇院 UPAS 網路存取控制管理系統
18	兩廳院工務維護管理系統	43	臺中國家歌劇院進出管理系統
19	兩廳院資源探索系統	44	臺中國家歌劇院劇場管理系統
20	兩廳院多視角隨選平台	45	臺中國家歌劇院 CRM 系統
21	兩廳院 AR 眼鏡字幕系統	46	臺中國家歌劇院電子郵件系統
22	兩廳院電子郵件系統	47	臺中國家歌劇院目錄服務系統
23	兩廳院目錄服務系統		
24	樂團人事系統		
25	樂團官網		

肆、資通安全政策及目標

一、 資通安全政策

本中心資通安全政策詳「ISMS-A-01_資通安全政策」，所屬單位應依 ISMS 控制目標與控制措施「A.5 資訊安全政策」規範訂定之。

二、 資通安全目標

本中心資通安全目標詳「ISMS-B-01_資通安全組織與目標管理程序書」，所屬單位應依 ISMS 「6.2 資訊安全目標與達成之規劃」規範訂定之。

三、 資通安全政策及目標之核定程序

本中心資通安全政策依核決權限，由本中心及所屬單位資通安全長核定後落實辦理。

四、 資通安全政策及目標之宣導

(一)資通安全政策及目標每年透過教育訓練、內部會議、張貼公告等方式，向所屬人員進行宣導，並檢視執行成效。

(二)每年向利害關係人(例如 IT 服務供應商、與本中心及所屬單位連線作業有關單位)進行資安政策及目標宣導，得以書面方式辦理，並檢視執行成效。

五、 資通安全政策及目標定期檢討程序

資通安全政策及目標定期於所屬單位資通安全管理相關會議中檢討其適切性。

伍、資通安全推動組織

依本法第11條之規定，本中心及各場館設置資通安全長一名，負責督導場館資通安全相關事項，由所屬單位資通安全長召集各業務部門經理成立場館資通安全推動小組。

單位	資通安全長
國家表演藝術中心	郭主任秘書美娟
國家表演藝術中心國家兩廳院	呂副總監岳霖
國家表演藝術中心臺中國家歌劇院	鄢副總監繼嬪
國家表演藝術中心衛武營國家藝術文化中心	謝副總監瑞香
國家表演藝術中心國家交響樂團	郭執行長玟岑

本中心資通安全推動組織詳如「ISMS-B-01_資通安全組織與目標管理程序書」，所屬單位應依ISMS 控制目標與控制措施「A.6 資訊安全的組織」規範訂定之。

資通安全長，其任務包括：

一、 資通安全管理政策及目標之核定、核轉及督導。
二、 資通安全責任之分配及協調。
三、 資通安全資源分配。
四、 資通安全防護措施 之監督。
五、 資通安全事件之檢討及監督。
六、 資通安全相關規章與程序、制度文件核定。
七、 資通安全管理年度工作計畫之核定
八、 資通安全相關工作事項督導及績效管理。
九、 其他資通安全事項之核定。

陸、專職人力

一、 專職人力及資源之配置

(一)所屬單位依資通安全責任等級分級辦法之規定，屬資通安全責任等級Ｃ級，所屬單位最低設置資通安全專職人員１人。

(二)所屬單位由所設之資通安全推動小組，負責督導所屬人員之資通安全作業，

防範不法及不當行為。

(三)資訊相關專業人力資源之配置情形每年定期檢討，並納入資通安全維護計畫持續改善機制之管理審查。

二、 經費之配置

(一)所屬單位規劃配置相關經費及資源時，應考量資通安全政策及目標，並提供建立、實行、維持及持續改善資通安全維護計畫所需之資源。

(二)所屬單位於規劃建置資通系統建置時，一併規劃資通系統之資安防護需求，並於整體預算中合理分配資通安全預算所佔之比例。

(三)所屬單位如有資通安全資源之需求，應配合預算規劃期程，由資通安全專職人員提出，以視整體資通安全資源進行分配，並進行相關建置。

(四)資通安全經費、資源之配置情形每年定期檢討，並納入資通安全維護計畫持續改善機制之管理審查。

柒、資通系統及資訊之盤點

一、 資通系統及資訊盤點

(一) 本中心每年辦理資通系統及資訊資產盤點，詳「ISMS-B-04_資訊資產管理程序書」，所屬單位應依 ISMS 控制目標與控制措施「A.8 資產管理」規範訂定之。

(二)本中心每年應依資通系統及資訊盤點結果，製作「資通系統及資訊資產清冊」，並依行政院國家資通安全會報資通安全作業管考系統所需欄位製作格式，所屬單位依期限填覆中心本部據以辦理回報作業。

(三)資通系統及資訊資產應以標籤標示於設備明顯處。

(四)所屬單位之管理資訊或資通系統如有異動，各單位應即時通知資通安全推動小組更新資產清冊。

捌、資通安全風險評估

一、 資通安全風險評估

(一)所屬單位每年針對資通系統及資訊資產進行風險評估。

(二)風險評估方法詳「ISMS-B-05_資通安全風險評鑑管理程序書」，所屬單位應依 ISMS 本文「6.1 風險與機會的應對措施」規範訂定之。

(三)所屬單位每年依據資通安全責任等級分級辦法之規定，分別就機密性、完整性、可用性、法律遵循性等構面評估自行或委外開發之資通系統防護需求分級。

玖、資通安全防護及控制措施

所屬單位依據前章資通安全風險評估結果、自身資通安全責任等級之應辦事項及核心資通系統之防護基準，採行相關之防護及控制措施，由於本中心核心資通系統已通過ISMS驗證，本中心之防護及控制措施詳如ISMS資通安全管理系統文件。所屬單位應依ISMS導入之各項控制領域、目標及措施，確實的執行資訊安全準則。

壹拾、資通安全事件通報、應變及演練相關機制

為即時掌控資通安全事件，並有效降低其所造成之損害，本中心應訂定資通安全事件通報、應變及演練相關機制，詳「資通安全事件通報及應變管理程序」與「ISMS-B-13_資通安全事件管理程序書」，所屬單位應依ISMS 控制目標與控制措施「A.16 資訊安全事故管理」規範訂定之。

壹拾壹、資通安全情資之評估及因應

所屬單位接獲資通安全情資，評估該情資之內容，並視其影響、可接受之風險及資源，決定最適當之因應方式，必要時得調整資通安全維護計畫之控制措施，並做成紀錄。

一、 資通安全情資之分類評估

所屬單位接受資通安全情資後，指定資通安全專職人員進行情資分析，並依據情資之性質進行分類及評估，情資分類評估如下：

（一）資通安全相關之訊息情資

資通安全情資之內容如包括重大威脅指標情資、資安威脅漏洞與攻擊手法情資、重大資安事件分析報告、資安相關技術或議題之經驗分享疑似存在系統弱點或可疑程式等內容，屬資通安全相關之訊息情資。

（二）入侵攻擊情資

資通安全情資之內容如包含特定網頁遭受攻擊且證據明確、特定網頁內容不當且證據明確、特定網頁發生個資外洩且證據明確、特定系統遭受入侵且證據明確、特定系統進行網路攻擊活動且證據明確等內容，屬入侵攻擊情資。

（三）機敏性之情資

資通安全情資之內容如包含姓名、出生年月日、國民身份證統一編號、護照號碼、特徵、指紋、婚姻、家庭、教育、職業、病例、醫療、基因、性生活、健康檢查、犯罪前科、聯絡方式、財務情況、社會活動及其他得以直接或間接識別之個人資料，或涉及個人、法人或團體營業上秘密或經營事業有關之資訊，或情資之公開或提供有侵害公務機關、個人、法人或團體之權利或其他正當利益，或涉及一般公務機密、敏感資訊或國家機密等內容，屬機敏性之情資。

二、 資通安全情資之因應措施

所屬單位於進行資通安全情資分類評估後，針對情資之性質進行相應之措施，必要時得調整資通安全維護計畫之控制措施。

（一）資通安全相關之訊息情資

由資通安全專職人員彙整情資後進行風險評估，並依據資通安全維護計畫之控制措施採行相應之風險預防機制。

（二）入侵攻擊情資

由資通安全專職人員判斷有無立即之危險，必要時採取立即之通報應變措施，並依據資通安全維護計畫採行相應之風險防護措施，另通知各單位進行相關之預防。

（三）機敏性之情資

涉及個人資料、營業秘密、一般公務機密、敏感資訊或國家機密之內容，採取遮蔽或刪除之方式排除，例如個人資料及營業秘密，以遮蔽或刪除該特定區段或文字，或採取去識別化之方式排除之。

壹拾貳、資通系統或服務委外辦理之管理

本中心委外辦理資通系統之建置、維運或資通服務之提供時，應考量受託者之專業能力與經驗、委外項目之性質及資通安全需求，選任適當之受託者，並監督其資通安全維護情形。詳如「ISMS-B-12_委外管理程序書」，所屬單位應依 ISMS 控制目標與控制措施「A.15 供應商關係」規範訂定之。

一、 選任受託者注意事項

(一)受託者辦理受託業務之相關程序及環境，具備完善之資通安全管理措施或通過第三方驗證。

(二)受託者配置充足且經適當之資格訓練、擁有資通安全專業證照或具有類似業務經驗之資通安全專業人員。

(三)受託者辦理受託業務得否複委託、得複委託之範圍與對象，及複委託之受託者具備之資通安全維護措施。

二、 監督受託者資通安全維護情形注意事項

(一)受託業務包括客製化資通系統開發者，受託者提供該資通系統之第三方安全性檢測證明；涉及利用非自行開發之系統或資源者，並標示非自行開發之內容與其來源及提供授權證明。

(二)受託者執行受託業務，違反資通安全相關法令或知悉資通安全事件時，立即通知所屬單位及採行之補救措施。

(三)委託關係終止或解除時，確認受託者返還、移交、刪除或銷毀履行委託契約而持有之資料。

(四)受託者採取之其他資通安全相關維護措施。

(五)所屬單位定期或於知悉受託者發生可能影響受託業務之資通安全事件時，以稽核或其他適當方式確認受託業務之執行情形。

壹拾參、資通安全教育訓練

一、 資通安全教育訓練要求

(一)本中心資通安全責任等級分級屬Ｃ級，資通安全專職人員每人每年至少接受十二小時以上之資通安全專業課程訓練或資通安全職能訓練。資訊人員每人每二年至少接受三小時以上之資通安全專業課程訓練或資通安全職能訓練，且每年接受三小時以上之資通安全通識教育訓練。相關訓練情形，所屬單位應陳核其資通安全長，記錄於資通安全實施情形。

(二)一般使用者與主管，每人每年接受三小時以上之資通安全通識教育訓練。

二、 資通安全教育訓練辦理方式

(一)所屬單位之承辦單位於每年年初，考量管理、業務及資訊等不同工作類別之需求，擬定資通安全認知宣導及教育訓練計畫，以建立員工資通安全認知，提升資通安全水準，並保存相關之資通安全認知宣導及教育訓練紀錄。

(二)資通安全認知宣導及教育訓練之內容得包含：

1. 資通安全政策(含資通安全維護計畫之內容、管理程序、流程、要求事項及人員責任、資通安全事件通報程序等)。

2. 資通安全法令規定。

3. 資通安全作業內容。

4. 資通安全技術訓練。

(三)員工報到時，使其充分瞭解資通安全相關作業規範及其重要性。

(四)資通安全教育及訓練之政策，除適用所屬員工外，對外部的使用者，亦一體適用。

壹拾肆、所屬人員辦理業務涉及資通安全事項之考核機制

所屬單位人員之平時考核或聘用，依據本中心內控制度薪工循環及所屬單位人事單位各相關規定辦理之。

壹拾伍、資通安全維護計畫及實施情形之持續精進及績效管理機制

一、 資通安全維護計畫之實施

為落實本資通安全維護計畫，使本中心之資通安全管理有效運作，所屬單位於訂定各階文件、流程、程序或控制措施時，應與本中心資通安全政策、目標及本資通安全維護計畫之內容相符，並應保存相關之執行成果紀錄。

二、 資通安全維護計畫實施情形之稽核機制

（一）稽核機制之實施

1. 所屬單位之資通安全推動小組應定期(至少每年一次)或於系統重大變更或組織改造後執行一次內部稽核作業，以確認人員是否遵循本規範與機關之管理程序要求，並有效實作及維持管理制度。

2. 辦理稽核前，資通安全推動小組應擬定資通安全稽核計畫並安排稽核成員，稽核計畫應包括稽核之依據與目的、期間、重點領域、稽核小組組成方式、保密義務 、稽核方式、基準與項目及受稽單位協助事項，並應將前次稽核之結果納入稽核範圍。

3. 辦理稽核時，資通安全推動小組應於執行稽核前 14 日，通知受稽核單位，並將稽核期程、稽核項目紀錄表及稽核流程等相關資訊提供受稽單位。

4. 本中心之稽核人員應受適當培訓並具備稽核能力，且不得稽核自身經辦業務，以確保稽核過程之客觀性及公平性；另，於執行稽核時，應填具稽核項目紀錄表，待稽核結束後，應將稽核項目紀錄表內容彙整，並提供給受稽單位填寫辦理情形。

5. 稽核結果應對所屬單位相關管理階層(含資通安全長)報告，並留存稽核

過程之相關紀錄以作為資通安全稽核計畫及稽核事件之證據。

6. 稽核人員於執行稽核時，應至少執行一項特定之稽核項目（如是否瞭解資通安全政策及應負之資安責任、是否訂定人員之資通安全作業程序與權責、是否定期更改密碼）。

（二）稽核改善報告

1. 受稽單位於稽核實施後發現有缺失或待改善項目者，應對缺失或待改善之項目研議改善措施、改善進度規劃，並落實執行。

2. 受稽單位於稽核實施後發現有缺失或待改善者，應判定其發生之原因，並評估是否有其類似之缺失或待改善之項目存在。

3. 受稽單位於判定缺失或待改善之原因後，應據此提出並執行相關之改善措施及改善進度規劃，必要時得考量對現行資通安全管理制度或相關文件進行變更。

4. 所屬單位應定期審查受稽單位缺失或待改善項目所採取之改善措施、改善進度規劃及佐證資料之有效性。

5. 受稽單位於執行改善措施時，應留存相關之執行紀錄，並填寫稽核結果及改善報告。

三、 資通安全維護計畫之持續精進及績效管理

（一）所屬單位之資通安全推動小組應於每年第四季(每年至少一次)召開資通安全管理審查會議，確認資通安全維護計畫之實施情形，確保其持續適切性、合宜性及有效性。相關審查會議紀錄除函知資通安全長、小組成員及場館藝術總監或樂團執行長外，並副知中心本部。

（二）管理審查議題應包含下列討論事項：

1. 過往管理審查議案之處理狀態。

2. 與資通安全管理系統有關之內部及外部議題的變更，如法令變更、上級機關要求、資通安全推動小組決議事項等。

3. 資通安全維護計畫內容之適切性。

4. 資通安全績效之回饋，包括：

(1) 資通安全政策及目標之實施情形。

(2) 資通安全人力及資源之配置之實施情形。

(3) 資通安全防護及控制措施之實施情形。

(4) 內外部稽核結果。

(5) 不符合項目及矯正措施。

5. 風險評鑑結果及風險處理計畫執行進度。

6. 重大資通安全事件之處理及改善情形。

7. 利害關係人之回饋。

8. 持續改善之機會。

（三）持續改善機制之管理審查應做成改善績效追蹤報告，相關紀錄並應予保存，以作為管理審查執行之證據。

壹拾陸、資通安全維護計畫實施情形之提出

本中心依據本法第 12 條之規定，所屬單位應配合行政院管考系統要求時間，回報資通安全維護計畫實施情形，由中心本部資安專職人員彙整後，填報行政院國家資通安全會報資通安全作業管考系統，使文化部瞭解本中心年度資通安全計畫實施情形。依照行政院或文化部之指示應修正本計畫時，得經本中心資通安全長同意後，依行政院及文化部之指示修正本計畫，並於修正後之最近一次董事會報告及追認。

壹拾柒、相關法規、程序及表單

一、 相關法規及參考文件

(一)資通安全管理法

(二)資通安全管理法施行細則

(三)資通安全責任等級分級辦法

(四)資通安全事件通報及應變辦法

(五)資通安全情資分享辦法

(六)資訊系統風險評鑑參考指引

(七)風險類型暨風險對策參考表

(八)政府資訊作業委外安全參考指引

(九)無線網路安全參考指引

(十)網路架構規劃參考指引

(十一) 行政裝置資安防護參考指引

(十二) 政府行動化安全防護規劃報告

(十三) 安全軟體發展流程指引

（十四） 安全軟體設計指引

（十五） 安全軟體測試指引

（十六） 資訊作業委外安全參考指引

（十七） 本中心及所屬單位資通安全事件通報及應變程序

（十八） 場館電腦作業及資訊安全管理要點

二、 附件表單

(一)資通安全保密同意書

(二)資通安全需求申請單

(三)資通系統及資訊資產清冊

(四)風險評估表

(五)管制區域人員進出登記表

(六)委外廠商執行人員保密切結書、保密同意書

(七)委外廠商查核項目表

(八)年度資通安全教育訓練計畫

(九)資通安全認知宣導及教育訓練簽到表

(十)資通安全維護計畫實施情形