國家表演藝術中心資通安全事件通報及應變管理程序

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、目的

國家表演藝術中心（下稱本中心）及所屬單位(以下稱本中心及所屬單位)為遵照資通安全管理法(以下簡稱資通法)暨本中心資通安全維護計畫之規定，於發生資通安全事件時，迅速完成損害控制或復原作業，降低資通安全事件對本中心業務之衝擊影響，並確保資通安全事件發生時之跡證保存，特訂定國家表演藝術中心資通安全事件通報及應變管理程序（下稱本管理程序）。

貳、適用範圍

發生於本中心及所屬單位之事件，系統、服務或網路狀態經鑑別而顯示可能有違反資通安全政策或保護措施失效之狀態發生，影響資通系統機能運作，構成資通安全政策之威脅者。

參、責任

一、 本中心及所屬單位之人員於發現資通安全事件時，應依本管理程序或資通安全長(以下簡稱資安長)之指示，執行通報及應變事務。

二、 本中心及所屬單位應於資通安全事件發生前，確保同仁及權責人員熟悉資通安全事件之通報，落實資通安全事件通報及應變管理程序，並依規定指定其知悉資通安全事件之通報以及完成應變作業後之結案登錄方式。

三、 本中心及所屬單位應確實執行本管理程序，並於知悉資通安全事件後依相關規定進行通報，於完成事件之通報及應變程序後，提供相關紀錄或資料。

四、 本中心及所屬單位於知悉資通安全事件後，依本管理程序之規定，儘速完成損害控制、復原與事件之調查及處理作業，並於完成後，依文化部及行政院指定之方式進行結案登錄作業，以及送交調查、處理及改善報告。

五、 依據資安維護計畫、所屬單位「資訊及資通系統資產清冊」所訂之清冊負責人及場館核決權限表簽核人員為本管理程序所稱之權責人員。

六、 所屬單位應依本管理程序及 ISMS 控制目標與控制措施「A.16 資訊安全事故管理」規範訂定「資通安全事件管理程序」。

肆、事件通報窗口及通報應變小組

一、 依行政院修正「各機關資通安全事件通報及應變處理作業程序」，成立國家表演藝術中心資通安全事件通報及應變小組(以下簡稱通報應變小組)，於

平時進行演練，並於發生資通安全事件時，依事件需要進行通報、應變及緊急處理作業。

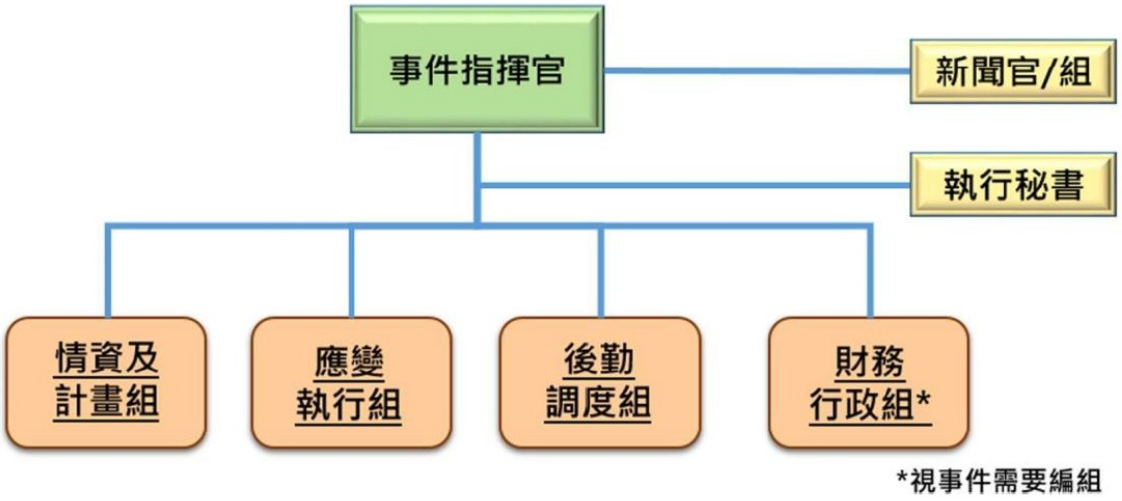
二、 本中心及所屬單位資通安全長得以現有組織分組為基礎，依單位編制及業務分工，參考下圖一經資通安全長同意後調整通報應變小組組成及選派各分組代表，另得視資通安全事件或資通環境需要調整各分組任務。

(一) 第一、二級資通安全事件：事件指揮官為本中心所屬單位資通安全長。

(二) 第三、四級資通安全事件：事件指揮官為本中心資通安全長。

三、 各相關權責人員應記錄事件處理過程，並檢討事件發生原因，著手進行改善，並留存必要之證據。

四、 通報應變小組組成建議如圖一，各分組代表如表一，各分組代表及任務如下：



圖一、資通安全事件通報及應變小組組成

表一、資通安全事件通報及應變小組各分組名單

	第一級、第二級資通安全事件		第三級、第四級資通安全事件	
	中心	場館	中心	場館
事件指揮官		資通安全長	資通安全長	
執行秘書		資訊主管		資通安全長
新聞官/組		公共溝通/行	行政管理部	

		銷公關/行銷主管	經理	
情資及計畫組組長	中心資安窗口	資訊組人員	中心資安窗口	資訊主管
應變執行組組長		資訊組人員/委外廠商	行政管理部經理	資訊主管
後勤調度組組長		資訊主管	行政管理部經理	資訊主管
財務行政組組長		財務單位主管	財務單位主管	財務單位主管

(一) 事件指揮官：為通報應變小組總召集人，綜理全般業務，直接督導各單位聯絡人員及新聞官/組。

(二) 新聞官/組：視事件需要由事件指揮官或其授權人員擔任新聞官或分組代表，資通安全事件對外發布新聞或說明之單一窗口，綜整與定期更新訊息及擬定溝通計畫。

(三) 執行秘書：為事件指揮官幕僚，負責督辦通報應變小組各項業務。

(四) 情資及計畫組：本分組由資通安全專責人員、資訊人員及委外廠商或外部專家組成。其任務如下：

1. 資通安全事件通報及情資分享：透過資通安全監控中心(SOC)、防毒軟體及系統釐清事件影響，並清查各單位受影響情形，據以完成資通安全事件各階段通報，分享惡意程式 IoC 等。
2. 應變策略及計畫研擬：於發生重大資通安全事件時，依據事件情況研擬損害控制、復原作業及跡證保存計畫。
3. 設立情資及計畫組資安通報窗口(以下簡稱通報窗口)：確保即時接獲資安情資反映，儘速啟動資安應變措施，有效控制災害範圍。

(五) 應變執行組：本分組由資通安全專責人員、資訊人員、業務單位及委外廠商組成。其任務如下：

1. 執行損害控制：依據情資及計畫組研擬之應變策略及計畫，調度資訊及資通安全人員執行災害搶救及損害管制，防止次波攻擊及損害擴散。
2. 復原作業：依據情資及計畫組研擬之復原作業，完成系統重建、弱點掃描或漏洞修補等事宜。
3. 跡證保全及留存：確保受害系統與相關系統及網路設備事件日誌之保存及管理。

(六) 後勤調度組：本分組由資通安全專責人員、資訊人員及委外廠商或外部專家組成。其任務如下：

1. 事件根因查找：依據系統保存跡證，完成鑑識分析，並追查防堵惡意中繼站。
2. 提出改善建議：依據事件調查根因，提出短、中、長期改善建議。
3. 彙整改善報告。
4. 撰寫調查、處理及改善報告。
5. 追蹤管考：針對已結案或未結案事項，如有未盡改善事宜，將另案追蹤管考。

(七) 財務行政組：本分組視事件需要由財務或秘書單位組成，負責辦理預算調撥及提供行政支援事宜。

五、 資通安全事件通報及應變程序，應包含通報資通安全事件、組成通報應變小組與召開事件應變會議、損害控制或復原作業、事件根因分析及改善追蹤等項目，並依資通法施行細則第六條第一項第九款規定納入資通安全維護計畫中，各項程序如下：

(一) 本中心及所屬單位應依資通法及資通安全事件通報及應變辦法規定，由情資及計畫組依主管機關或中央目的事業主管機關指定方式完成事件通報。

(二) 資通安全事件通報窗口與聯繫專線，詳如附件一。

(三) 每年以公告方式使相關人員明確知悉事件通報窗口及聯絡方式。

(四) 發現資通安全事件後，應立即向所屬單位資通安全長及通報窗口進行通報。

(五) 通報窗口應確保聯絡管道全天維持暢通，若因設備故障或其他情形導致通報窗口聯絡管道中斷，該中斷情況若持續達一小時以上者，立即將該情況進行周知，同時提供其他有效之臨時聯絡管道。

(六) 負責事件處理之小組、該事件發生之單位權責人員與相關單位密切合作，以進行事件處理，並使通報窗口適時掌握事件處理之進度及其他相關資訊。

(七) 上級機關、中央目的事業主管機關或相關機關支援派員參與時，依派員支援屬性由各組負責彙整報告，使上級機關、中央目的事業主管機關或相關機關支援派員充分掌握事件狀況與進度。

(八) 事件經初步判斷認為可能屬重大資安事件或事態嚴重時，應即向本中心資通安全長報告，由本中心資通安全長成立通報應變小組著手處理；接獲本中心或受託廠商所通報之資通安全事件時，亦同。

(九) 組成通報應變小組與召開事件應變會議：本中心於完成第三級或第四級資通安全事件之初步損害控制後應召開事件應變會議，會議形式不拘，由事件指揮官主持討論下列事項，並得視情況邀請上級機關、中央目的事業主管機關或主管機關出席：

1. 資通安全事件概況。
2. 評估受影響範圍。

3. 其他必要之討論事項。

伍、通報程序

一、 通報資通安全事件

（一） 本中心及所屬單位應依資通法及本管理程序規定，由情資及計畫組依主管機關或中央目的事業主管機關指定方式完成事件通報。

（二） 第三級或第四級資通安全事件，本中心除依前目規定通報外，應另以電話或其他適當方式通知上級機關或中央目的事業主管機關，無上級機關者，應通知主管機關；數位發展部資通安全署就第三級或第四級資通安全事件，依國土安全緊急通報作業規定轉報行政院國土安全辦公室。

二、 通報作業程序

（一） 判定事件等級之流程及權責：本中心及所屬單位通報應變小組依以下事項，於知悉資通安全事件後，依行政院所頒之「資通安全事件通報及應變辦法」，進行資通安全事件等級判斷：

1. 事件涉及核心業務或關鍵基礎設施業務之資訊與否。
2. 事件導致業務之資訊或資通系統遭竄改之影響程度，屬嚴重或輕微。
3. 事件所涉資訊是否屬於國家機密、敏感資訊或一般公務機密。
4. 業務運作若遭影響或資通系統停頓，是否可容忍中斷時間內能回復正常運作。
5. 事件其他足以影響資通安全事件等級之因素。

（二） 除事件之等級外，本中心及所屬單位通報應變小組亦應對資通安全事件之影響範圍、損害程度及因應之能力進行評估。

（三） 本中心及所屬單位通報應變小組於完成資通安全事件等級之判斷及相關評估後，應盡速報本中心或所屬單位資安長核准。

（四） 除因網路或電力中斷等事由，致無法依本中心或文化部及行政院所指定或認可之方式通報外，於知悉資通安全事件後一小時內向本中心、文化部及行政院所指定或認可之方式，進行事件通報。

（五） 因網路或電力中斷等事由，致無法依前項規定方式為通報者，於知悉資通安全事件後一小時內以電話或其他適當方式，將該次資安事件通報之內容及無法依規定方式通報之事由，分別告知本中心、文化部及行政院，並於事由解除後，依原方式續行通報。

（六） 本中心及所屬單位委外辦理資通系統之建置、維運或提供資通服務之情形時，於合約中訂定委外廠商於知悉資通安全事件時，即向通報窗口，以指定之方式進行通報。

（七） 知悉資通安全事件後，如認該事件之影響涉及其他機關或應由其他機關依其法定職權處理時，本中心及所屬單位通報應變小組應於知悉資

通安全事件後一小時內，將該事件依文化部或行政院所指訂或認可之方式，通知該機關。

三、 接獲自身、監督單位通報之評估作業程序

（一） 本中心及所屬單位通報應變小組，於接獲所屬單位之資通安全事件通報後，應於以下時限內，完成資通安全事件通報等級及相關事項之審核：

1. 通報為第一級或第二級之資通安全事件，於接獲通報後八小時內。
2. 通報為第三級或第四級之資通安全事件，於接獲通報後二小時內。

（二） 本中心及所屬單位通報應變小組進行本條第一項之審核過程中，得請求通報之公務機關提供級別判斷所需之資料或紀錄。

（三） 本中心及所屬單位通報應變小組於必要時得依據審核之結果，逕行變更資通安全事件之等級，並應於決定變更後一小時內，將審核結果及級別變更之決定通知行政院，並提供做成決定所依據之相關資訊。

陸、應變程序

一、 事件發生前之防護措施規劃

所屬單位應於平時妥善實施資安維護計畫，並以組織營運目標與策略為基準，透過整體之營運衝擊分析，規劃業務持續運作計畫並實施演練，以預防資安事件之發生。

二、 損害控制機制

（一） 由應變執行組執行損害控制或復原作業，並辦理下列事項：

1. 確認具體受害範圍，並優先恢復對外服務及核心資通系統運作，防止次波攻擊及擴散情形。
2. 評估各系統是否於可容忍中斷時間內恢復服務及對利害關係人之影響，決定是否對外公告事件之相關內容。
3. 於完成損害控制或復原作業後，依主管機關或中央目的事業主管機關指定之方式完成通知作業。

（二） 第三級或第四級資通安全事件，除依前目規定辦理外，並應辦理下列事項：

1. 定時向事件指揮官、通報應變小組成員、上級機關或中央目的事業主管機關回報控制措施成效。
2. 倘涉及個人資料外洩，應評估通知當事人之適當方式，依個人資料保護法第十二條規定辦理。

（三） 本中心及所屬單位通報應變小組，應完成以下應變事務之辦理，並留存應變之紀錄。：

1. 資安事件之衝擊及損害控制作業。

2. 資安事件所造成損害之復原作業。
3. 資安事件相關鑑識及其他調查作業。
4. 資安事件之調查與處理及改善報告之方式。
5. 資安事件後續發展及與其他事件關聯性之監控。
6. 資訊系統、網路、機房等安全區域發生重大事故或災難，致使業務中斷時，依據所屬單位事前擬定之緊急計畫，進行應變措施，以恢復業務持續運作之狀態。
7. 其他資通安全事件應變之相關事項。

（四） 對於第一級、第二級資通安全事件，本中心及所屬單位於知悉事件後七十二小時內完成前項事務之辦理，並留存紀錄；於第三級、第四級資通安全事件，本中心及所屬單位於知悉事件後三十六小時內完成損害控制或復原作業，並執行上述事項及留存相關紀錄。

（五） 完成通報及應變程序之辦理後，依文化部或行政院所指定或認可之方式進行結案登錄。

（六） 本中心及所屬單位於知悉受託廠商發生與受託業務相關之資通安全事件時，於知悉委外廠商發生第一、二級資通安全事件後七十二小時內，確認委外廠商已完成損害控制或復原事項之辦理；於知悉委外廠商發生第三、四級資通安全事件後三十六小時內，確認委外廠商完成損害控制或復原事項之辦理。

柒、資安事件後之復原、鑑識、調查及改善機制

一、 本中心及所屬單位完成資通安全事件之通報及應變程序後，針對事件所造成之衝擊、損害及影響進行調查與改善，並於事件發生後一個月內完成事件調查、處理及改善報告。

二、 事件根因分析，由本中心及所屬單位通報應變小組後勤調度組執行，依資通安全事件等級，建議辦理事項如下：

（一） 依「捌、紀錄留存及管理程序之調整」跡證保存之規定保存相關跡證，惡意程式建議得請防毒軟體或資安服務公司檢測，並上傳至 Virus Check 網站(https://viruscheck.tw/)分析，以更新或強化相關偵測及聯防機制，不宜上傳至其他平臺。

（二） 除設備故障外，後勤調度組應依據前目保存跡證，由組長督導委外廠商或外部專家進行根因調查，並提出紀錄分析；如發現惡意程式，應提出惡意程式分析。

（三） 依據事件調查根因分析結果，應評估短、中、長期資安管理改善策略，其內容如下：

1. 短期：完成可立即性修補項目之調整，例如更換密碼或修補程式弱點等。
2. 中期：依據事件根因提出三至六個月內完成之強化作為，例如盤點老舊設備，並訂定汰換期程。
3. 長期：依據事件受害情形，視需要提出二年內完成之管理改善建議，例如培養資安人員能力。

（四） 由執行秘書將事件調查根因及改善策略提報事件指揮官裁處，並由情資及計畫組彙整送交上級機關或中央目的事業主管機關。

三、 資通安全事件調查、處理及改善報告，應包括以下項目：

（一） 事件發生、完成損害控制或復原作業之時間。

（二） 事件影響之範圍及損害評估。

（三） 損害控制及復原作業之歷程。

（四） 事件調查及處理作業之歷程。

（五） 為防範類似事件再次發生所採取之管理、技術、人力或資源等層面之措施。

（六） 前款措施之預定完成時程及成效追蹤機制。

四、 本中心通報應變小組應向文化部及行政院提出前項之報告，以供監督與檢討。

五、 改善追蹤：本中心及所屬單位通報應變小組進行事件改善追蹤時，應視需要召開會議，並據以辦理下列事項：

（一） 評估改善作為期程。

（二） 評估執行成效，並據以調整改善策略。

（三） 配合上級機關、中央目的事業主管機關或主管機關辦理相關改善作為。

（四） 第三級或第四級資通安全事件，應由本中心通報應變小組執行秘書將各階段改善措施執行成效定期回報事件指揮官至完成各項改善措施為止，並由情資及計畫組彙整送交上級機關或中央目的事業主管機關。

（五） 本中心及所屬單位通報應變小組依主管機關或中央目的事業主管機關指定之方式，送交調查、處理及改善報告；第三級或第四級資通安全事件，應另以密件公文將該報告送交主管機關及上級或監督機關。

（六） 本中心及所屬單位通報應變小組送交調查、處理及改善報告後，相關改善事項應納入現行定期追蹤管考機制。

捌、紀錄留存及管理程序之調整

一、 本中心及所屬單位應將資通安全事件之通報與應變作業之執行、事件影響範圍與損害程度，以及其他通報應變執行情形，於「資安事件通報紀錄單」上留存完整之紀錄，該文件並經權責人員、資安長簽核。

二、 本中心及所屬單位完成資通安全事件之通報及應變程序後，依據「資安事件通報紀錄單」之內容及實際處理情形，於必要時對本管理程序、人力配置或其他相關事項進行修正或調整。

三、 本中心及所屬單位完成資通安全事件之通報及應變程序後，依據「資安事件通報紀錄單」之內容及實際處理情形，於必要時對本管理程序、人力配置或其他相關事項進行修正或調整：

(一) 於日常維運資通系統時，應依自身資通安全責任等級保存日誌(log)，並建議定期備份至與原稽核系統不同之實體系統，其保存範圍及項目如：

1. 應保存全部核心資通系統最近六個月之日誌紀錄。
2. 作業系統日誌(OS event log)
3. 網站日誌(web log)
4. 應用程式日誌(AP log)
5. 登入日誌(logon log)

(二) 發生資通安全事件時，應依下列原則進行跡證保存：

1. 進行跡證保存時，應優先採取隔離機制，包含設備關機、網路連線中斷或隔離、關閉服務、限制連線、限制權限、有限度修補漏洞等方式，以降低攻擊擴散。
2. 若系統無備援機制，應備份受害系統儲存媒介(例如硬碟、虛擬機映像檔)後，以乾淨儲存媒介重建系統，於完成系統測試後提供服務。
3. 若系統有備援機制，應將服務切換至備援系統提供服務，並保留受害系統及設備，於完成事件根因分析或完整備份後重建系統，經系統測試後切換至原系統提供服務。
4. 若備援設備亦為受害範圍，於重建受害系統時應以維持最低限度對外運作為原則，保存受害跡證。

(三) 本中心及所屬單位於簽訂資通系統或服務之委外契約時，應依前二款規定於契約中明定紀錄保存及備份規定。

玖、演練作業

本中心及所屬單位應配合行政院依資通安全事件通報應變辦法之規定辦理下列資通安全演練作業：

一、　社交工程演練。
二、　資通安全事件通報及應變演練。
三、　網路攻防演練。
四、　情境演練。
五、　其他必要之演練。

壹拾、本程序之實施及修正

本管理程序經董事會通過後實施，修正時亦同。如依照行政院或文化部之指示應即時修正本管理程序時，得經本中心資安長同意後，依行政院及文化部之指示修正本管理程序，並於修正後之最近一次董事會報告及追認。

附件一

資通安全事件通報窗口與聯繫專線

所屬單位	通報窗口	聯繫專線	電子信箱
國家表演藝術中心	吳佳芸	(02)3393-9967 0983-326-112	wgujane@mail.npac-ntch.org
國家兩廳院	陳冠廷	(02)3393-9938 0975-344-879	tin_chen@mail.npac-ntch.org
臺中國家歌劇院	莊富凱	(04)22512333#5789 0919-677-395	jeff@npac-ntt.org
衛武營國家藝術文化中心	林明勳	(07)262-6850 0919-537-888	stan.lin@npac-weiwuying.org
國家交響樂團	吳佳芸	(02)3393-9967 0983-326-112	wgujane@mail.npac-ntch.org

注意事項:

一、 知悉資通安全事件後一小時內，向所屬單位通報窗口進行事件通報。

二、 評估作業程序:

(一) 第一級或第二級資通安全事件，於知悉事件後八小時內完成評估。

(二) 第三級或第四級資通安全事件，於知悉事件後二小時內完成評估。

三、 損害控制:

(一) 第一級或第二級資通安全事件，於知悉事件後七十二小時內完成損害控制。

(二) 第三級或第四級資通安全事件，於知悉事件後三十六小時內完成損害控制或復原作業。

(三) 執行上述事項及留存相關紀錄。

四、通報窗口因職務異動變更時，授權由權責主管修正本附件，並依本管理程序規定通知相關人員。