國家表演藝術中心資通安全事件通報及應變管理程序

111年5月25日第三屆第2次董事會通過

目　　錄

壹、　目的

國家表演藝術中心及所屬單位(以下簡稱所屬單位)為遵照資通安全管理法第14條暨本中心資通安全維護計畫(以下簡稱資安維護計畫)之規定，建立資通安全事件之通報及應變機制，以迅速有效獲知並處理事件，特訂定本管理程序。

貳、　適用範圍

發生於所屬單位之事件，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、所屬單位所屬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、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、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、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。

肆、　事件通報窗口及緊急處理小組

一、所屬單位之資通安全事件通報窗口與聯繫專線，詳如附件一。人員進行異動時，應函知資安長、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、所屬單位每年以公告方式，使所屬人員明確知悉事件通報窗口及聯絡方式。

三、發現資通安全事件後，應立即向所屬單位資安長及通報窗口進行通報。

四、各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。

五、負責事件處理之單位(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。

六、事件經初步判斷認為可能屬重大資安事件或事態嚴重時，應即向資安長報告，由資安長成立緊急處理小組，立即協助進行處理；接獲受託廠商所通報之資通安全事件時，亦同。

七、資安長成立緊急處理小組時，應指派場館之資通安全相關技術人員擔任小組成員，必要時並得聘外部專家擔任之。

八、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。

伍、 通報程序

一、通報作業程序

(一)判定事件等級之流程及權責

權責人員或緊急處理小組依以下事項，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，權責人員或緊急處理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)權責人員或緊急處理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)資通安全事件等級如有變更，權責人員或緊急應變小組告知通報窗口，使其續行通報作業。

(七)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，即向權責人員或窗口，以指定之方式進行通報。

(八)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，權責人員或緊急處理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。

二、接獲自身、監督單位通報之評估作業程序

(一)權責人員或緊急處理小組，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)權責人員或緊急處理小組進行本條第一項之審核過程中，得請求通報之公務或特定非公務機關提供級別判斷所需之資料或紀錄。

(三)權責人員或緊急處理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) 負責應變之權責人員或緊急處理小組，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。

(二)對於第一級、第二級資通安全事件，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，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。

(三)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。

(四) 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、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、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。

三、應向文化部及行政院提出前項之報告，以供監督與檢討。

捌、 紀錄留存及管理程序之調整

一、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、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。

玖、 演練作業

各館團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。

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	莊岳儒	(07)262-6851 0939-701-369	yuehju.chuang@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。