財團法人國家文化藝術基金會
委外專案資訊安全規定

專案名稱：財團法人國家文化藝術基金會「公文簽呈系統建置案」

項次	資通安全管控措施項目
1	廠商應遵守資通安全管理法暨其相關子法、行政院頒訂之各項資訊安全規範及本署有關系統開發維護之資訊安全相關規定辦理，以強化資訊系統安全管理，確保資料傳送、儲存及流通之安全。
2	廠商交付之軟硬體及文件，應先行檢查是否內藏惡意程式(如病毒、蠕蟲、特洛伊木馬、間諜軟體等)及隱密通道(covert channel)，並於上線前應清除正式環境之測試資料與帳號及管理資料與帳號。
3	廠商應繳交資安檢測報告書，檢測時須提供掃描軟體系統登入帳密以進行深度檢測，檢測結果不能存在高、中、低風險之弱點。其中低風險弱點若經評估無法修補，須提出說明並經本會同意後方可排除修補。
4	系統需支援跨瀏覽器操作使用及 HTTPS 傳輸協定，SSL 網站之安全性設定檢測(https://www.ssllabs.com/ssltest/index.html)至少須達 B 級以上、SSL 憑證安裝須通過憑證串鍊檢測(https://www.sslshopper.com/ssl-checker.html)
5	契約履約或終止後，廠商應刪除或銷毀執行服務所持有機關之相關資料，或依機關之指示返還之，並保留執行紀錄。
6	廠商所提供之服務，如為軟體或系統發展，須針對各版本進行版本管理，並依照資安管理相關規範提供權限控管與存取紀錄保存。
7	廠商提供服務，如發生資安事件時，必須通報機關，提出緊急應變處置，並配合機關做後續處理。
8	系統如發生資通安全事件（如資料外洩、被竊取、駭客入侵等情事），廠商須於 2 個小時內協助本會辦理資通安全事件狀況處理相關作業程序及查明原因，並於 24 小時內提供改善情形及建議報告書。

財團法人國家文化藝術基金會
委外專案資訊安全規定

9	當系統異常無法正常運作，應配合做緊急處理，應於接獲通知 4 個工作小時內進行處理，並於 1 個工作天內完成。
10	維護期間內如因故終止服務，廠商應於規定期限內，將本會存在於委外廠商處的資料或設備移轉給本會或本會指定委外廠商。
11	廠商參與本專案之成員均需簽署人員保密同意書及切結書。
12	廠商應遵循「個人資料保護法」之相關規定，保留個人資料存取記錄，以利資安稽核。
13	廠商須依「資通安全責任等級分級辦法」附表九「資通系統防護需求分級原則」進行分級，協助鑑別本案資訊系統安全等級及產出評估表經本會確認，並依資訊系統【高】、【中】、【普】等級，執行該法附表十「資通系統防護基準」對應等級之各種資安控制措施。
14	廠商應就本專案之安全需求，填復「資通系統資安防護基準要求與查核表」及「應用系統安全需求查檢表」，並於查檢表上簽名，以示負責。
15	廠商應於專案執行期間負責系統文件最新版本之建立與維護，交付最新版本之系統文件（含光碟），包含完整之系統操作手冊、教育訓練學員簽到簿(如有教育訓練需求)、系統說明書(包含系統架構、功能說明、程式說明清單、資料庫說明)。有關原始程式碼及系統安裝建置，廠商須視本會需求於本會建置所需環境供本會驗證原始程式碼與經編譯後之可執行檔版本是否相符。
16	系統上線前，廠商應將作業系統及發展工具軟體等安裝至最新之修補程式，並針對程式做相關資訊安全檢測（例如 SQL Injection、XSS、惡意程式碼檢測等）。
17	系統上線前，廠商應提供測試計畫及測試報告(含光碟及書面文件)，除功能驗證外，須納入安全需求驗證。各項測試報告應包含測試項目名稱、測試說明、測試條件、事先需成立之條件、測試預期結果、實際測試資料、測試時間、測試人員、測試結果。

財團法人國家文化藝術基金會
委外專案資訊安全規定

18	程式變更須於本會測試環境測試無誤並保留變更前後差異之紀錄，並由本會程式管理人員確認後，於本會指定時間(含下班或例假日)安裝程式變更於正式作業，如程式變更後無法正常運作，則須立即恢復原狀。得標廠商應於更新完成後 10 個工作日內提供相關說明文件，如有必要需安排教育訓練。如程式變更涉及系統文件之修正，應於系統變更完成後一個月內修正完成送交本會。
19	廠商應提供安全完整之系統備份與還原程序（含光碟）及負責設定，並須視本會需要於本會建置所需環境供本會測試驗證。
20	系通應符合資訊安全責任分散之權限控管機制（建議區分申請,覆核,核准,稽核等角色，並加以控制）。
21	配合本會資訊安全風險評估及安全管理需求，對個人資料或機密資料，應妥善保護及加密處理，以確保資料之隱密性。
22	配合本會外部稽核作業之查核，廠商應配合接受本會或委託單位之稽核或查核等業務，其範圍包括本專案開發環境、設備、人員及系統之管理機制等。
23	配合本會實施之弱點掃瞄、滲透測試、內部稽核、外部稽核等作業所提之檢測報告，承包廠商須依檢測報告，提出系統資安問題分析與改善建議，如因特殊原因無法如期完成修正，廠商得敘明理由提交本會進行審查，本會得視情況酌予延長，並於完成改善後交付本會「系統資安問題改善計畫執行報告書」。本會視情況得要求廠商參與相關會議。
24	本會原則禁止承包廠商透過 Internet 遠端維護系統，如有需求須向本會申請。
25	配合本會導入行政院「政府組態基準(GCB)」，廠商應視系統運作狀況配合修正及調整系統，維持系統正常運作。
26	配合本會資訊安全管理系統(ISMS)之導入，協助調整系統相關功能及辦理相關作業。

財團法人國家文化藝術基金會
委外專案資訊安全規定

27	維護期限內，倘維護標的因故搬遷，廠商應免費協助本會辦理系統轉置或重新設定等相關事宜。
28	維護期間內，得標廠商應配合本會主機虛擬化作業時程，將系統原主機資料(包含應用系統、資料庫及檔案等)移轉至 VM 環境，並進行相關網路連線設定，於移機後須進行系統測試，以確保系統運作正常。
29	維護期間內，得標廠商應配合本會要求，對於所維護之應用系統之系統運作環境(如：作業系統版本、資料庫系統版本或軟體版本...等) 之更動，協助進行事前評估及免費協助轉置，且於前述更動後，須進行系統測試，以確保系統運作正常及符合相容性。
30	維護期間內本會因軟硬體設備異動，因而涉及原系統環境變更時(如版本變更或安裝 PATCH)，得標廠商應免費提供技術服務。
31	正式作業及測試系統，應採用不同的登入程序。
32	系統須將存於資料庫內之使用者密碼欄位以加密（不可逆）處理儲存，以防止使用者密碼為使用者以外人員知悉。
33	資料庫連線字串應予加密，密碼避免直接寫於檔案或程式碼中。
34	若應用 ActiveX 與 Java applet，應採取相關防護措施(如:加註警語提醒使用者將下載之相關元件為何)。
35	廠商如違反上述規定，應適用契約之違約責任，並就機關所受損害負賠償之責；如致他人權利受有損害時，廠商亦應負責。

補充說明：依據本規定應交付文件：資安檢測報告書(每期)、保密同意書及切結書、資通系統資安防護基準要求與查核表、應用系統安全需求查檢表、系統操作手冊、教育訓練學員簽到簿(如有教育訓練需求)、系統說明書(包含系統功能架構、功能說明、程式說明清單、資料庫說明)、測試計畫及測試報告(如為開發擴充案)、系統備份與還原程序。