國家電影及視聽文化中心

「114 年網頁應用程式防火牆汰換案」財物採購案（2025-IT028）

需求說明書

一、 採購案號：2025-IT028

二、 採購案名：「114 年網頁應用程式防火牆汰換案」財物採購案（以下稱本案）。

三、 本案說明：

原廠已公告 2026 年 12 月為 WAF X1020 產品生命週期尾聲（EOL），屆期原廠將不再提供更新支援（包括安全修補程式），故更換新式 WAF X2030。

四、 廠商資格：依中華民國法令核准設立之公司、合夥、或獨資之工商行號，且營業項目包含資訊軟體服務業(I301010) 、電腦及事務性機器設備批發業(F113050)、電腦及事務性機器設備零售業(F213030)等其中一項。

五、 履約期限：自決標日次日起至 114 年 12 月 15 日止。

六、 經費預算：新臺幣 348 萬 6,000 元整（含稅）。

七、 履約地點：本中心新莊場館。

八、 採購標的規格、功能、數量：

項目	項目名稱	內容	單位	數量
1	網頁應用程式防火牆 Imperva X2030	**軟體規格：** • 軟體授權 IMPERVA 網頁應用程式防火牆軟體 500M 更新(一年授權) **硬體規格：** **Imperva X2030** • 標準 19 吋機架式尺寸，1U 機架式伺服器，具備 4 個（含）以上 100/1000Mbps 銅纜超高速乙太網路埠。 • 內建硬體式之網路故障自動旁路機制(bypass)且執行 bypass 時不須再手動進行相關設定，以確保設備發生故障時在不需手動設定的情況下仍可維持網路服務不中斷。 • 提供 500Mbps（含）以上的 Throughput of Layer 7 Web Application Firewall 偵測防禦能力。 • 支援 Transparent Inline bridge、Transparent Reverse Proxy、Reverse Proxy、Sniffing Mode 至少兩種以上模式佈署。	套	1

		• 硬碟至少為 480GB 以上，記憶體至少為 16GB 以上。 • 具備 OWASP TOP 10 攻擊事件的資安漏洞防衛功能，提供資料隱碼 (SQL injection)攻擊與防禦、跨網站攻擊 (Cross Site Scripting (XSS))攻擊與防禦、暴力攻擊 (Brute Force login)與防禦、參數值之竄改 (Parameter Tampering)攻擊與防禦、資訊外洩 (Information Leakage)之防範。 • 可過濾 HTTP Session 中的特定字串，並直接拒絕中斷連線。 • 可針對每一個 Session 與來源 IP 進行阻絕，並可以設定「監控」，以利管理者依據不同的攻擊型態或環境等因素調整防禦模式。 • 提供與原廠定時連線更新特徵碼(Signatures)功能，可以自動排程或手動方式進行更新，更新特徵碼時，Web Server 之防禦功能並不會受影響。 • 可檢視原廠預設特徵碼字串內容作為修正誤判特徵碼依據。 • 具備自我學習及調整機制能力可以有效地降低制定策略時之管理負擔。 • 自動學習之 Profile 可由管理者手動調整，管理者可以 URI 為單位手動切換該 URI 為學習模式或防護模式，且也可以目錄為單位鎖定(Lock)該學習功能。 • 內建信用卡敏感資料庫，並可自訂敏感資料規則且可設定遮罩之字元位置，避免機敏資訊以明碼出現於系統管理介面與各式報表。 • 具備對某網段之網站(HTTP、HTTPS)服務掃描功能，並可直接從掃描結果中將欲設定監控保護之網站直接選取納入保護清單中。 • 具備網站弱點掃描結果整合功能，可防止網站弱點被利用攻擊，可整合多家商業弱掃工具，如；WhiteHat Security、HP、IBM、NTO、Qualys 等。 • 內建報表系統，可提供按每日、週或每月排程產生報表並提供符合 ISO27001 之報表範本。 • 報表檔格式支援 PDF 格式及 CSV 格式，並可根據警示內容(來源 IP、目的地 URL、時間、嚴重等級、發生次數、違反的政策規則)自行訂定篩選條件產出報表，報表產出完成可以 Email 寄送給相關管理者。 • 可自訂報表顯示內容資訊並自訂排序欄位，皆可以選單方式點選完成。 • 系統告警功能提供異常行為及完整過程訊息分析功		

		能，包含來源 IP、應用程式主機 IP、使用者帳號、Session Id、HTTP Header、HTTP Content 等，並提供事件收斂(Aggregate)功能。 • 系統告警(Alert)可透過 email、SNMP、OS Command 及 Syslog 等機制通知相關管理者或第三方系統(如 SIEM 等)。 • 提供管理者帳號權限管理，不同帳號登入所能檢視的資料及可執行的操作不同，達到分工分權概念。登入系統之帳號可整合 AD 帳號。 • 具備統一管理系統，能集中控管同廠牌多台網站應用程式防火牆閘道防護設備。可自動派送同步安全政策至所納管的網頁應用程式防火牆設備，並可集中查詢告警事件。 • 至少具備一項安全合規認證：CE、FCC、VCCI。 • 近三年內須至少一次入選 The Forrester Wave WAF 評比為領導(Leaders)。 • 需可匯入現有 WAF 系統之防禦政策、報表、告警、備份等設定。 保固：原廠 1 年保固		
備註： • 上述設備須為 2024 年 1 月 1 日以後（含）製造（需檢附原廠出廠證明及保固書）。				

九、 執行時程及應完成工作

（一）廠商應自決標日次日起至 114 年 12 月 15 日內，將網頁應用程式防火牆送達本中心（指定之場所），廠商以書面向本中心申請驗收。

（二）資安規範

（1）廠商提供服務所使用之資訊通訊軟硬體設備，應遵守本中心「資通訊產品安全規範」（**如附件-資通訊產品安全規範**）。

（三）其他規範

（1）本專案廠商需安排專案負責人負責本專案之執行，且須確實掌握本專案各階段相關進度，並負責與本中心聯繫。

（2）本專案廠商應於本專案執行期間依執行需求與本中心召開工作會議，以就規劃籌辦相關事項進行溝通協調，廠商依協調結果確實執行。

（3）團隊成員不允許為大陸地區廠商及陸籍人士參與本案。

十、 交付項目、安裝與驗收

項次	交付項目	交付期程
1	**資訊安全規範文件** • 委外廠商團隊成員名冊暨保密同意書與切結書 • 未使用大陸廠牌切結書	於契約生效後 10 個工作天內
2	**產品來源證明** • 原廠出廠證明（設備為 2024 年或以後出產製造之原廠出廠）	114 年 12 月 15 日前(含當日)
3	**保固證明文件** • 網頁應用程式防火牆原廠一年保固證明書 • 經銷授權證明書	
4	**其他文件** • 送貨簽收單	應於交貨當天提供
備註：本各項交付文件項目除**未使用大陸廠牌切結書、保固證明文件、委外服務團隊名冊暨保密同意書與切結書**須以正本紙本交付一份，其餘文件以電子檔交付並以電子郵件方式提供本中心，於本中心同意備查後再以 A4 尺寸紙張直式橫書雙面製作印刷並製成紙本一式二份。		

十一、　保固

（一）保固期：本履約標的自全部完成履約經驗收合格日之日起，由廠商保固一年。

（二）廠商於保固期間須提供或配合以下相關工作：

（1）提供免費升級原廠發佈之新版本更新、產品弱點修補並提供技術諮詢服務。

（2）產品硬體保固期間內，提供收送維修品至原廠或原廠授權之維修中心，不得另行收運送費。

（3）每週一至週五正常上班日（工作時間為上午 8 時 30 分至下午 17 時 30 分，中午休息時間為中午 12 時 30 分至下午 13 時 30 分，廠商應於接獲本中心故障通知後 4 小時內處理及回覆）。

（4）技術諮詢服務以電話、電子郵件、遠端支援為主（必要時須到場協助），針對本案所採購之相關軟硬體設備包含下列服務：

(a) 軟硬體設備操作及設定技術諮詢。

(b) 軟硬體設備故障修復之問題排除及設定調整。

十二、　驗收地點：

國家電影及視聽文化中心(新北市新莊區文藝路 2 號)。

十三、　主辦機關

國家電影及視聽文化中心（新北市新莊區文藝路 2 號 4 樓）

聯絡人：資訊室/簡楷峻，電話：02-8522-8000 分機 2305

E-mail：danieljian@tfai.org.tw

國家電影及視聽文化中心

資通訊產品安全規範

114.5.19 版

壹、 適用範圍

本規範適用：

一. 資訊系統之開發、功能擴充、維護與維運。

二. 資通訊設備、資訊軟硬體、資訊服務之提供與使用。

貳、 名詞定義

一、資訊軟體：用來處理、管理和傳輸資訊的軟體工具和應用程式。

二、資訊硬體：指的是在資訊系統中用來處理、存儲、傳輸及展示資訊的設備。

三、資訊系統：涵蓋硬體、軟體、數據、人員和流程等多個方面的軟體系統。資訊系統的目的是支持和改善組織的運作和決策，用於整合和管理組織的各種業務流程，如企業資源規劃（ERP）系統、HRM 人力資源系統、網站、行動應用軟體(APP)、客製化套裝軟體等。

四、資訊服務：指提供與資訊軟硬體有關之服務，包括雲端服務、整體規劃、系統整合、系統稽核、系統管理、網路管理、軟體開發、軟體驗證、軟體維護、硬體維護、硬體操作、機房設施管理、備援服務、網路服務、顧問諮詢、資料庫建置、資料處理、資料登錄或訓練推廣等服務。

五、資通訊產品：參考資通安全管理法第3條用詞定義，包含資訊軟體、資訊硬體及資訊服務等，另具連網能力、資料處理或控制功能者皆屬廣義之資通訊設備，如個人電腦、伺服器、無人機、印表機、網路通訊設備、可攜式設備及物聯網設備（包括監視系統、網路電話、會議系統、電話總機系統、顯示器、影印機、門禁系統、事務機等）等。

六、行動應用軟體：指一種設計給智慧型手機、平板電腦和其他行動裝置使用之應用程式。

參、 資通安全需求

一、資通安全管理法及其相關子法

（一） 應遵守資通安全管理法及其相關子法、行政院所頒訂之各項資通安全規範及標準，並遵守本中心資訊安全管理及保密相關規定。

（二） 本中心為資通安全責任等級C級之公務機關，須遵循資通安全責任等級C級之公務機關應辦事項(**附件一**)，**涉及資通系統開發或維護之廠商**，應鑑別**資通系統防護需求等級**（參考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」與「資通系統安全等級評估表」)，完成資通系統資安防護基準要求與查核表要求(**附件二**)。廠商須配合於系統發展各階段完成與符合資通系統防護基準檢核表要求，並**檢附各項防護措施之佐證資料**。

（三） 本中心委外辦理資訊軟硬體及資訊服務，廠商應接受並配合下列事項：

1. 廠商辦理本中心委託業務之相關程序及環境，應具備完善之資通安全管理措施或通過第三方驗證。
2. 廠商應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。
3. 契約資訊軟硬體及資訊服務部分合計金額如達新臺幣一千萬元以上者，廠商應接受並配合本中心或其所委託之第三方進行資通安全檢測；其範圍包括廠商以及實際提供或使用資訊軟硬體及資訊服務之分包廠商。資通安全檢測項目由本中心視專案性質訂之。
4. 客製化資訊系統開發之廠商，如涉及利用非自行開發之系統或資源者，並應標示非自行開發之內容與其來源及提供授權證明。
5. 廠商執行專案業務，違反資通安全相關法令或知悉資通安全事件時，應立即通知本中心及採行之補救措施。
6. 廠商提供或使用資訊軟硬體或資訊服務，如發生資通安全事件，或有其他重大違反資通安全規定之虞，本中心或其所委託之第三方得對廠商進行資通安全稽核；資通安全稽核範圍應包括廠商以及實際提供或使用資訊軟硬體及資訊服務之分包廠商。資通安全稽核項目，由機關視實際事件狀況訂之。

（四） 應依據資通安全管理法及個人資料保護法，辦理資通安全管理作業，維持本中心委託業務之安全與穩定運作。

（五） 廠商應說明執行本中心委託業務履約之資安作為，並提交「**附件三**：廠商資安管理作業自評表」備查。

（六） 廠商及執行專案之團隊須熟知本中心「**附件四**：資通安全政策」，並簽署「**附件五**：委外服務團隊成員名冊暨保密同意書與切結書」。

二、資訊系統安全設計

（一） 廠商應導入安全軟體發展生命週期(Secure Software Development Life Cycle, SSDLC)，於專案開始各階段(需求、設計、開發、測試、部署維運)進行各項必要的安全防護措施。基本要求須符合「**附件二**：資通系統資安防護基準要求與查核表」之□普□中□高等級（非客製化資訊系統者免填），廠商應依國家資通安全研究院共通規範之資通系統防護基準驗證實務，逐項檢視並執行該等級所要求之防護基準控制措施。

（二） 資訊系統業務衝擊分析（非資訊系統免填）：

可容許的最大資料損失量（RPO）：_____小時。

系統、服務重新上線的時間（RTO）：_____小時。

最大可容忍中斷時間（MTPD）：_____小時。

（三） 保全開發環境：

1. 廠商須自備系統開發環境，禁止於本中心所提供之正式環境進行系統開發與測試。
2. 廠商進行測試時優先使用模擬資料，若因特殊事由需使用真實資料進行測試，亦不得使用原始資料，並對於使用之資料善盡保管及保密之責任。系統應對於異常事件、重要事件或特殊權限帳號儲存保留日誌紀錄。

3. 廠商對資訊系統之異動，應事先作好資料備份工作，並就其實施細節及可能之風險完成規劃及評估，經本中心確認始得實施，如有意外狀況，除應採取還原或其他措施或減少不良影響，並於第一時間通知本中心。
4. 作業系統、資料庫及應用程式之所有密碼資料，皆不得以明碼型態存或傳輸，若有特殊需求須經本中心同意後辦理。
5. 於開發或進行原程式修改之原始碼，須提供未加密完整原始碼於本中心，系統相關軟體如有修改時應配合一併更新（此項視專案屬性擇用，但屬完全為中心客製化開發系統適用）。

（四） 資訊系統防護

1. 資訊系統應依國家資通安全研究院「Web應用程式安全參考指引」設計並進行資安查檢。
2. 資訊系統須具備SQL Injection、XSS、CSRF、File Injection及File Inclusion 等攻擊之防護能力。
3. 資訊系統如為網站系統，傳輸應採用HTTPS協定TLS1.2（含）以上版本，以確保機敏資料以密文方式傳輸。HTTPS連線不得使用遭破解加密演算法，如DES、3DES、RC4等。
4. 資訊系統具備帳號鎖定機制，帳號登入進行身分鑑別失敗達5次後，至少15分鐘內不允許該帳號及來源IP繼續嘗試登入。
5. 資訊系統分級為中、高者，身分驗證機制應防範自動化程式之登入或密碼更換嘗試，登入系統頁面或密碼更換頁面採用圖形驗證碼（CAPTCHA）機制或以其他足以辨識人為動作之方式(如勾選特定選項等)，以防堵自動化程式之嘗試行為。
6. 資訊系統安全機制須整體考慮實體安全、軟體系統壓力及負載測試使用者溝通管道上，規劃適當之安全性協定，以完整地保護各項資料不被盜取、竄改，並杜絕發生系統被入侵之行為。
7. 廠商應配合本中心依國家資通安全研究院公告之政府組態基準(GCB)設定項目需求，辦理資訊系統之伺服器作業系統、瀏覽器等GCB套用。除有套用影響系統及業務運作之情形，應以全部項目套用為原則。
8. 作業系統、資料庫及應用程式層級，除系統作業架構特殊需求外，所有密碼資料，皆不得以明文型態存放。
9. 帳號及密碼管理須遵循本中心制訂之密碼設定原則，密碼輸入時皆以暗碼顯示，帳號或密碼輸入錯誤不直接明示，只顯示「帳號或密碼錯誤」。
10. 須採用無程式碼技術進行系統維護，惟操作畫面等網頁展示部分可採用原始碼技術。
11. 廠商應確保其開發之程式絕無留有任何形式之系統後門，以免危害系統安全。
12. 資訊系統需設置客製化錯誤頁面，當發生錯誤時，使用者頁面僅顯示簡短錯誤訊息與代碼，不包含詳細的錯誤訊息，避免將詳細或除錯用訊息直接顯示於使用者頁面，以防被攻擊者用來刺探系統內部資訊，

或根據錯誤訊息推測出系統可能之弱點。

13. 廠商採用開發架構及系統平台所需使用之相關軟體，應提供最新版本且合理數量之合法授權證明；如為免費工具則應提出本中心可合法使用之佐證資料。

（五） 稽核與可歸責性

1. 資訊系統應有日誌紀錄機制，應保存最近六個月之紀錄，項目如下：
   (1) 作業系統日誌 (OS event log)
   (2) 網站日誌 (web log)
   (3) 應用程式日誌 (AP log)
   (4) 登入日誌 (logon log)，
2. 資訊系統應設計對特定事件「身分驗證失敗」、「帳戶鎖定」、「重要資料異動」、「功能重大錯誤」及「管理者行為」等操作行為之功能。
3. 資訊系統日誌紀錄至少應包含IP、識別使用者之ID(不可為個資類型)、時間戳記、執行的功能或存取的資源、事件類型及事件描述等資訊。
4. 所產生之系統日誌紀錄，應採用單一日誌紀錄機制(如採用Apache Log4J、Log4NETet及Log4PHP等)，確保輸出格式之一致性。
5. 日誌紀錄之時戳，應由系統內部時鐘產生，並可以對應到世界協調時間(UTC)或格林威治標準時間(GMT)，有助於彙整資安事件所發生的各種事件時間點，進而分析資安事件可能發生的原因。
6. 系統應配置日誌紀錄所需之儲存容量(如磁碟或資料庫空間等)，避免因儲存容量不足造成日誌處理失效。系統於稽核處理失效時（如儲存容量不足），應採取適當之行動(如加大儲存容量、覆寫最舊的稽核紀錄或停止產生稽核紀錄等，並寄發警示信件通知管理人員)，避免危害系統服務正常運作。
7. 資訊系統分級為高者，當稽核紀錄無法寫入儲存媒體(如檔案系統或資料庫)時，以信件或簡訊通知系統設定之相關人員。
8. 應設計對日誌紀錄進行適當保護及備份，避免未經授權存取，並定期備份稽核紀錄到與原稽核系統不同之實體系統（如Log伺服器）。
9. 資訊系統分級為中、高者，系統所產出稽核紀錄，內容如有不足之處，應配合本中心承辦人員於專案執行過程中增補。

（六） 安全性檢測與弱點修補作業：

1. 資訊系統客製化開發階段，應執行源碼掃描安全檢測，於交付原始程式碼前，提交檢測報告；於上線或使用前，應依本中心「資通系統獲取、開發及維護管理作業說明書」規定，完成弱點掃描，以確認不存在 OWASP（The Open Web Application Security Project，開放網站應用程式安全專案）歸納公布之最新版十大網路資安風險（OWASP Top 10）或其他中高等級以上風險（CVSS 值大於 4.0(含)之安全性漏洞）後，並提出無中高風險之資安檢測報告、訂定「系統上線及緊急復原計畫」，始得上線。檢測工具由廠商自備，可參考 OWASP 組織整理之免費及商業化工具，如 OWASP ZAP、Burp Suite、Nessus、Acunetix、Netsparker、Metasploit Framework、

OpenVAS 等。

2. 資訊系統如係行動應用軟體，應於上架至軟體市集、或以其他方式正式提供使用者下載安裝前，應確認不存在 OWASP MOBILE TOP 10 RISK 2024 中高風險。
3. 檢測結果屬於中高度風險之弱點（CVSS 值大於 4.0(含)之安全性漏洞），由廠商限期完成修補，檢查結果屬於低度風險（含）以下之弱點，廠商亦應評估進行改善，或出具書面說明不會影響系統安全之證明。
4. 廠商應提供專案範圍軟體物料清單（Software Bill of Materials，SBOM）包含韌體、程式、工具、元件、函式庫等，針對系統所使用的SBOM所列清單將定期評估及更新其安全漏洞。
5. 廠商應配合國家資通安全研究院、資安廠商提出之安全漏洞、本中心檢測系統與主機資安漏洞掃描之結果，執行弱點修補工作。中、高風險弱點一律必須進行修補，檢查結果屬於低風險之弱點，廠商亦應評估進行改善，或出具書面說明不會影響系統安全。廠商收到通知後，中、高風險弱點應於 30 個工作天內，低風險弱點應於 45 個工作天內（或本中心同意之期限內）完成相關弱點修補作業。若修正後尚有漏洞須持續修正至無漏洞為止，修改系統或網站漏洞之相關責任與成本由廠商全權負責。上述風險弱點若無法進行修補則應提出補償性之改善措施，如以最小權限原則限制存取，其改善措施需經由本中心審核同意。

（七） 備份、還原演練機制

1. 廠商須提出系統及資料備份規劃，資料備份至少須包含每日差異性備份及定期完整備份，並完成**附件六：**「備份機制明細表」填寫。本中心得要求不定期查驗備份紀錄及結果，如發現有執行不確實情形，廠商須應本中心要求進行改善。
2. 廠商應進行系統、資料、檔案及紀錄備份作業，並配合本中心相關管理程序，定期進行備份復原測試，驗證其可靠性及資訊之完整性，並做成記錄，如**附件七**：「備份測試查核表」（此項資通系統防護分級為中級以上須納入）。
3. 廠商應規劃完整之備份及還原作業，內容涵蓋系統、資料庫及檔案資料，且須配合本中心資安演練需求，進行系統業務持續演練及相關測試作業。

（八） 緊急復原能力

1. 廠商須針對系統程式、資料庫及使用者資料之損毀、遭外力破壞導致網頁破壞或置換等可能影響本專案各項服務正常運作之情況，提供回復機制或替代方案。
2. 廠商應自接獲本中心通知後，須於 5 個工作天內將系統錯誤程式修改完畢，並經本中心測試完成，如系統問題複雜未及於前開規定之時間內完成修復，應立即通知本中心並預估修復所需時間，經本中心同意後得以延長。
3. 以上應包含契約期間本中心上班時間系統正常維護服務。

三、資訊作業安全規範

（一） 廠商如派員至本中心執行相關作業或活動時，非使用本中心配發之資通訊設備，應符合資通安全管理法及其相關法規規範：

1. 設備部分：
   (1) 禁止使用大陸廠牌設備，並簽署「**附件八：**未使用大陸廠牌切結書」。
   (2) 電腦須安裝防毒軟體，病毒碼更新應設為自動。
2. 軟體部分：
   (1) 作業系統（如Windows Update、Apple、Linux OS等）安全性更新需為最新。
   (2) 應用軟體（如Java、Adobe FlashPlayer、Adobe Reader、其他軟體等）安全性更新需為最新。
   (3) 安裝合法授權軟體，嚴禁下載或使用非法、中國開發之軟體與檔案。
   (4) 瀏覽器應更新至最新版本。
3. 網路部分：
   (1) 禁止未經授權使用本中心內部網路存取資源。
   (2) 禁止使用本中心提供之公用網路自行架設無線網路設備，如因專案業務需要而有架設必要者，應向資訊室提出申請，經同意後始得架設。

（二） 原則禁止廠商遠端連線管理伺服器，如有遠端連線維護需求，應依本中心ISMS規範申請VPN連線，由本中心承辦人審核後提出申請，經核准同意開通後始可使用。廠商每次連線應通知應用系統負責人，說明維護標的、事由、預計作業起訖日期及時間。

（三） 廠商履行契約應提供其使用之軟體，須為合法軟體，不得違反智慧財產權之規定，如有違反事情發生，廠商須承擔所有法律責任。

（四） 廠商所交付之標的物如侵害第三人合法權益時，由廠商負責處理並承擔一切法律責任。

四、資訊軟硬體使用安全規範

（一） 遵循行政院公告之「禁止使用及採購大陸資通訊產品相關規定」，本中心全面禁止使用及採購大陸廠牌資通訊產品。

（二） 資通訊產品之採購，且廠商提供施作服務者，須交付「**附件三：**廠商資安管理作業自評表」與「**附件五：**委外服務團隊成員名冊暨保密同意書與切結書」之簽署。

（三） 廠商提供之資訊軟硬體、資訊服務、雲端服務或勞務資料存取、儲存、備份及備援等作業，其實體設備所在地及資料傳輸不得置於中國大陸地區(含香港、澳門)或該等境內傳輸相關資料之情形，應簽署「**附件九：**資料所在地及跨境傳輸切結書」。需端服務等資安控制措施應遵守國家資通安全研究院網站之共通規範專區所公布「政府機關雲端服務應用資安參考指引」（網址：https://www.nics.nat.gov.tw/cybersecurity_resources/reference_guide/Common_Standards/）

（四） 使用生成式AI模型應遵守行政院所公布「行政院及所屬機關（構）使用生成式AI 參考指引」（網址：https://www.nstc.gov.tw/folksonomy/list/c79bf57b-dc94-4aff-8d14-3262b5559cfc?l=ch）。

五、資通安全稽核

（一） 配合上級主管機關稽核作業

1. 配合本中心ISO27001管理相關規定維護本專案資通系統，並應依本中心通知於ISO27001驗證作業需求下，指派合適之工作人員到場參與或線上協助處理。
2. 若本中心當年度被行政院、文化部遴選為政府機關（構）資通安全稽核之受稽機關，廠商須協助本中心進行相關稽核準備工作，如有需要廠商應至少派1員陪同進行實地受稽作業。
3. 若遇數位發展部資通安全署或文化部等上級主管機關辦理相關網路攻防演練、情境演練與其他必要之演練，廠商須協助提供相關建議與諮詢服務。
4. 若有資訊系統資安相關議題之會議，須配合本中心協助備妥相關會議資料並視需求列席參與其會議。

（二） 委外廠商稽核要求

1. 本中心保有對廠商進行資安稽核之權利，且廠商必須配合填寫「**附件十：委外廠商查核項目表**」，並檢附相關佐證資料。本中心得視需要定期或不定期（以實地查核或書面方式）查核廠商提供之服務是否符合契約和資訊安全規範，廠商應配合辦理，並提供本中心書面資料及邀集相關人員列席備詢。
2. 上述查核得以不預告之方式進行之，廠商不得無故拒絕，有關稽核缺失廠商應限期改善不得推諉。本中心必要時得委由專業之第三方，稽核所提供之服務。

六、資安事件處理

（一） 若專案發生第3、4級資安事件，廠商須於1個小時內回應本中心通知，第1、2級資安事件，廠商須於4個小時內回應本中心通知。若因廠商作業所致資安事件，回應內容含事件說明及影響範圍、擬訂損害控制與復原措施及預估完成時間。待資安事件完成損害控制或復原作業後，正式提報調查、處理及改善報告至本中心，內容含資通安全管理法施行細則第8條規定事項等。

（二） 廠商應負責維護標的伺服器日誌蒐集保存，並於資安事件發生時，協助日誌分析與問題查找。

七、其他

（一） 實際提供資訊軟硬體或資訊服務之分包廠商不得為經濟部投資審議委員會網站公告之陸資資訊服務業者，亦不得使用前開陸資企業出品之產品。

（二） 契約如包含資訊系統開發或資訊服務，原則應全部於我國境內進行及完成，如部分或全部於我國境外辦理者，應事先通知本中心並同意後，始得為之。前開境外地區不得為中國大陸、香港、澳門或其他經機關評估具資安風險地區。

（三） 下列人員不得為契約專案團隊成員或派駐人員或參與軟體開發、測試：

1. 任職於中國大陸、香港、澳門或外國公營機構或政府機關者。
2. 任職於經濟部投資審議委員會網站公告之陸資資訊服務業者。
3. 具中國大陸國籍者。

（四） 系統開發或維護廠商對專案契約各項文件內容及資料，應負保密責任，非經本中心書面同意，不得提供給其他個人、機關、團體或公司行號。

（五） 對於使用者的個資、密碼、交易資料、交易過程產生之敏感資料等，進行適當的保護與管理。

（六） 契約履約或終止後，廠商應刪除或銷毀執行服務所特有本中心之相關資料，或依本中心之指示返還之，並保留執行紀錄與簽署「**附件十一**：資料返還、刪除、銷毀切結書」。

（七） 契約專案因期限屆滿、解除或其他原因而終止時，廠商及其工作人員仍負有前款之保密責任。

附件一

資通安全責任等級C級之公務機關應辦事項

制度面向	辦理項目	辦理項目細項	辦理內容
管理面	資通系統分級及防護基準		初次受核定或等級變更後之一年內，針對自行或委外開發之資通系統，依附表九完成資通系統分級；其後應每年至少檢視一次資通系統分級妥適性；並應於初次受核定或等級變更後之二年內，完成附表十之控制措施。
	資訊安全管理系統之導入		初次受核定或等級變更後之二年內，全部核心資通系統導入 CNS 27001 或ISO 27001 等資訊安全管理系統標準、其他具有同等或以上效果之系統或標準，或其他公務機關自行發展並經主管機關認可之標準，並持續維持導入。
	資通安全專責人員		初次受核定或等級變更後之一年內，配置一人。
	內部資通安全稽核		每二年辦理一次。
	業務持續運作演練		全部核心資通系統每二年辦理一次。
技術面	安全性檢測	弱點掃描	全部核心資通系統每二年辦理一次。
		滲透測試	全部核心資通系統每二年辦理一次。
	資通安全健診	網路架構檢視	每二年辦理一次。
		網路惡意活動檢視	
		使用者端電腦惡意活動檢視	
		伺服器主機惡意活動檢視	
		目錄伺服器設定及防火牆連線設定檢視	
	資通安全弱點通報機制		一、 關鍵基礎設施提供者初次受核定或等級變更後之二年內，完成資通安全弱點通報機制導入作業，並持續維運及依主管機關指定之 二、 本辦法中華民國一百十年八月二十三日修正施行前已受核定者，應於修正施行後二年內，完成資 三、 通安全弱點通報機制導入作業，並持續維運及依主管機關指定之方式提交資訊資產盤點資料。
	資通安全防護	防毒軟體	初次受核定或等級變更後之一年內，完成各項資通安全防護措施之啟用，並持續使用及適時進行軟、硬體之必要更新或升級。
		網路防火牆	
		具有郵件伺服器者，應備電	

		子郵件過濾機制	
認知與訓練	資通安全教育訓練	資通安全專責人員	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。
		資通安全專責人員以外之資訊人員	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。
		一般使用者及主管	每人每年接受三小時以上之資通安全通識教育訓練。
	資通安全專業證照		初次受核定或等級變更後之一年內，至少一名資通安全專責人員持有證照一張以上，並持續維持證照之有效性。

備註：

一、資通系統之性質為共用性系統者，由該資通系統之主責設置、維護或開發機關判斷是否屬於核心資通系統。

二、特定非公務機關辦理本表「資通安全健診」時，除依本表所定項目、內容及時限執行外，亦得採取經中央目的事業主管機關認可之其他具有同等或以上效用之措施。

三、資通安全弱點通報機制，指結合資訊資產管理與弱點管理，掌握整體風險情勢，並協助機關落實本法有關資產盤點及風險評估應辦事項之作業。

四、資通安全專業證照，指由主管機關認可之國內外發證機關（構）所核發之資通安全證照。

五、特定非公務機關之中央目的事業主管機關得視實際需求，於符合本辦法規定之範圍內，另行訂定其所管特定非公務機關之資通安全應辦事項。

附件二：「資通系統防護需求分級原則」、「資通系統安全等級評估表」與「資通系統資安防護基準要求與查核表」

資通系統防護需求分級原則

防護需求等級 / 構面	高	中	普
機密性	發生資通安全事件致資通系統受影響時，可能造成未經授權之資訊揭露，對機關之營運、資產或信譽等方面將產生非常嚴重或災難性之影響。	發生資通安全事件致資通系統受影響時，可能造成未經授權之資訊揭露，對機關之營運、資產或信譽等方面將產生嚴重之影響。	發生資通安全事件致資通系統受影響時，可能造成未經授權之資訊揭露，對機關之營運、資產或信譽等方面將產生有限之影響。
完整性	發生資通安全事件致資通系統受影響時，可能造成資訊錯誤或遭竄改等情事，對機關之營運、資產或信譽等方面將產生非常嚴重或災難性之影響。	發生資通安全事件致資通系統受影響時，可能造成資訊錯誤或遭竄改等情事，對機關之營運、資產或信譽等方面將產生嚴重之影響。	發生資通安全事件致資通系統受影響時，可能造成資訊錯誤或遭竄改等情事，對機關之營運、資產或信譽等方面將產生有限之影響。
可用性	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非常嚴重或災難性之影響。	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嚴重之影響。	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。
法律遵循性	如未確實遵循資通系統設置或運作涉及之資通安全相關法令，可能使資通系統受影響而導致資通安全事件，或影響他人合法權益或機關執行業務之公正性及正當性，並使機關所屬人員負刑事責任。	如未確實遵循資通系統設置或運作涉及之資通安全相關法令，可能使資通系統受影響而導致資通安全事件，或影響他人合法權益或機關執行業務之公正性及正當性，並使機關或其所屬人員受行政罰、懲戒或懲處。	其他資通系統設置或運作於法令有相關規範之情形。

備註：資通系統之防護需求等級，以與該系統相關之機密性、完整性、可用性及法律遵循性構面中，任一構面之防護需求等級之最高者定之。

資通系統安全等級評估表

資通系統名稱：

功能說明：

業務屬性：□行政類 □業務類

填表日期：　　年　　月　　日

影響構面				資通系統安全等級
1. 機密性	2. 完整性	3. 可用性	4. 法律遵循性	
□普□中□高	□普□中□高	□普□中□高	□普□中□高	□普□中□高 （任一構面之防護需求等級之最高者定之）

步驟 1：設定影響構面等級

項目	安全等級		原因說明
1. 機密性	初估	□普□中□高	
	異動	□普□中□高	
2. 完整性	初估	□普□中□高	
	異動	□普□中□高	
3. 可用性	初估	□普□中□高	
	異動	□普□中□高	
4. 法律遵循性	初估	□普□中□高	
	異動	□普□中□高	
備註：資通系統屬「無客製化之套裝軟體」、「資通訊硬體設備」免填本表			

業務承辦	承辦主管	資訊室	資通安全長

資通系統資安防護基準要求與查核表

系統名稱：　　安全等級：□普 □中 □高

查核日期：

存取控制					
帳號管理					
安全需求檢核項目	資通系統資安等級（此欄勿動）			是否符合（請依實際狀況填寫）	佐證資料或作法說明 1、灰色字體為填表說明，請依各系統實際執行情形填寫。 2、黑色字體表共通作業部分，毋須個別填寫。 3、左欄勾選不適用者，請說明原因。
	普	中	高		
建立帳號管理機制，包含帳號之申請、開通、停用及刪除之程序。	●	●	●	□是 □不適用 □否，預計完成時間　年　月　日	資通系統之帳號應透過正式的帳號申請程序所建立，完成開通審核程序始能使用，因此應具備帳號管理機制，可對系統帳號進行申請、建立、修改、啟用、停用或刪除之行為。
已逾期之臨時或緊急帳號應刪除或禁用。		●	●	□是 □不適用 □否，預計完成時間　年　月　日	若具有臨時帳號或緊急帳號時，應實作已逾期之系統帳號檢查機制，於帳號逾期時自動停用或刪除，以避免帳號遭有心人士盜用。
資通系統閒置帳號應禁用。		●	●	□是 □不適用 □否，預計完成時間　年　月　日	宜記錄系統帳號最後登入時間，可透過工作排程，檢查是否有持續一段時間(如半年等)未登入系統之帳號，並實作自動停用該帳號之功能。
定期審核資通系統帳號之建立、修改、啟用、禁用及刪除。		●	●	□是 □不適用 □否，預計完成時間　年　月　日	請說明是否定期辦理帳號清查並留下清查紀錄
機關應定義各系統之閒置時間或可使用期限與資通系統之使用情況及條件。			●	□是 □不適用 □否，預計完成時間　年　月　日	
逾越機關所定預期閒置時間或可使用期限時，系統應自動將使用者登出。			●	□是 □不適用 □否，預計完成時間　年　月　日	會談(Session)機制目的為管理使用者與伺服器之間的連線狀態，使用者於系統中若一段時間未進行活動，系統應有自動機制將該使用者的會談階段設為失效而登出系統，以降低資安風險。
應依機關規定之情況及條件(如上班時間或指定 IP 來源)使用資通系統。			●	□是 □不適用 □否，預計完成時間　年　月　日	請說明是否有系統使用時間規定、遠端連線來源 IP 限制

監控資通系統帳號，如發現帳號違常使用時回報管理者。			●	□是 □不適用 □否，預計完成時間 年 月 日	應具備監控及通知機制，向系統管理者回報帳號異常使用行為(如短期內大量帳號登入失敗或存取未經授權之資源等)。

最小權限

安全需求檢核項目	資通系統資安等級			是否符合	佐證資料或作法說明
	普	中	高		
採最小權限原則，僅允許使用者(或代表使用者行為之程序)依機關任務及業務功能，完成指派任務所需之授權存取。		●	●	□是 □不適用 □否，預計完成時間 年 月 日	請說明是否依據權責設置帳號權限

遠端存取

安全需求檢核項目	資通系統資安等級			是否符合	佐證資料或作法說明
	普	中	高		
對於每一種允許之遠端存取類型，均應先取得授權，建立使用限制、組態需求、連線需求及文件化。	●	●	●	□是 □不適用 □否，預計完成時間 年 月 日	
使用者之權限檢查作業應於伺服器端完成。	●	●	●	□是 □不適用 □否，預計完成時間 年 月 日	
應監控遠端存取機關內部網段或資通系統後臺之連線。	●	●	●	□是 □不適用 □否，預計完成時間 年 月 日	
應採用加密機制。	●	●	●	□是 □不適用 □否，預計完成時間 年 月 日	請說明遠端連線是否採安全通道如 SSL VPN 等
遠端存取之來源應為機關已預先定義及管理之存取控制點。		●	●	□是 □不適用 □否，預計完成時間 年 月 日	遠端存取採限定來源 IP 位址、限定連線 PORT、限定連線時間之方式提供使用

事件日誌與可歸責性

記錄事件

安全需求檢核項目	資通系統資安等級			是否符合	佐證資料或作法說明
	普	中	高		
訂定日誌之記錄時間週期及留存政策，並保留日誌至少六個月 。	●	●	●	□是 □不適用 □否，預計完成時間 年 月 日	請說明稽核紀錄(Log)保存方式與保存時間 (依規定，紀錄之保存期限須考量組織需求與法令法規要求
確保資通系統有記錄特定事件之功能，並決定應記錄之特定資通系統事件。	●	●	●	□是 □不適用 □否，預計完成時間 年 月 日	資通系統應實作記錄特定事件之功能，如身分驗證失敗、存取資源失敗、重要行為、重要資料異動、功能錯誤及管理者行為等。
應記錄資通系統管理者帳號所執行之各項功能。	●	●	●	□是 □不適用 □否，預計完成時間 年 月 日	請說明對管理者帳號所為之各種操作是否留下稽核紀錄
應定期審查機關所保留資通系統產生之日誌 。		●	●	□是 □不適用 □否，預計完成時間 年 月 日	請說明是否留下定期審查稽核紀錄(log)之佐證資料

稽核與可歸責性

日誌紀錄內容					
安全需求檢核項目	資通系統資安等級			是否符合	佐證資料或作法說明
	普	中	高		
資通系統產生之日誌應包含事件類型、發生時間、發生位置及任何與事件相關之使用者身分識別等資訊，採用單一日誌機制，確保輸出格式之一致性，並應依資通安全政策及法規要求納入其他相關資訊。	●	●	●	□是 □不適用 □否，預計完成時間 年 月 日	日誌應詳細描述所觸發的事件，包含人、事、時、地、物等關鍵資訊，宜包含：使用者帳號(避免個資類型)、時間、執行之功能或存取之資源名稱、事件類型或優先等級、執行結果或事件描述、事件發生當下相關物件資訊、網路來源與目的位址，以及錯誤代碼等。系統開發人員應盡可能採用單一的 Log 機制，如不得同時混用兩種以上日誌產生套件(如 Log4Net 與 Nlog 等)，並應確保日誌內容格式之可讀性，以便於事件比對與追查。日誌應依據資通安全政策及其他法規要求，納入任何有必要留存之資訊，如憑證資訊、日誌層級、會談識別碼等。
日誌儲存容量					
安全需求檢核項目	資通系統資安等級			是否符合	佐證資料或作法說明
	普	中	高		
依據日誌儲存需求，配置所需之儲存容量。	●	●	●	□是 □不適用 □否，預計完成時間 年 月 日	
日誌處理失效之回應					
安全需求檢核項目	資通系統資安等級			是否符合	佐證資料或作法說明
	普	中	高		
資通系統於日誌處理失效時，應採取適當之行動。	●	●	●	□是 □不適用 □否，預計完成時間 年 月 日	當資通系統發生日誌處理失效狀況時，應採取相對應的處理措施(如覆寫最舊的日誌紀錄、停止產生日誌紀錄或對特定人員提出警告等)，避免危害系統可用性，或是當資安事件發生時缺乏系統日誌以供比對追查之情況。
機關規定需要即時通報之日誌處理失效事件發生時，資通系統應於機關規定之時效內，對特定人員提出警告。			●	□是 □不適用 □否，預計完成時間 年 月 日	應定義需要即時通報的特定日誌處理失效事件、即時通報的時效以及特定通知對象，並實作通知機制，以利及早釐清事件發生原因並進行故障排除。如當日誌紀錄無法正常寫入資料庫時，以信件或簡訊通知系統維護人員。
時戳及校時					

安全需求檢核項目	資通系統資安等級			是否符合	佐證資料或作法說明
	普	中	高		
資通系統應使用系統內部時鐘產生日誌所需時戳，並可以對應到世界協調時間(UTC)或格林威治標準時間(GMT)。	●	●	●	□是 □不適用 □否，預計完成時間 年 月 日	使用系統內部時鐘產生日誌所需時戳，如Windows 作業系統顯示之日期時間等。採用全系統一致的時間標準，有助於彙整資安事件所發生的各種事件時間點，進而分析資安事件可能發生的原因。
系統內部時鐘應定期與基準時間源進行同步。		●	●	□是 □不適用 □否，預計完成時間 年 月 日	日誌紀錄必須維持使用精確的時間，以利事件追蹤及稽核取證等用途，實務上，可使用網路時間協定(Network Time Protocol, NTP)，讓機關內各個系統及網路設備定期與校時伺服器進行同步，如國家標準時間伺服器(time.stdtime.gov.tw)或使用機關自建之伺服器。
日誌資訊之保護					
安全需求檢核項目	資通系統資安等級			是否符合	佐證資料或作法說明
	普	中	高		
對日誌之存取管理，僅限於有權限之使用者。	●	●	●	□是 □不適用 □否，預計完成時間 年 月 日	請說明稽核紀錄的存取限制方式為何(如僅提供特定權限人員可透過系統介面查詢)
應運用雜湊或其他適當方式之完整性確保機制。		●	●	□是 □不適用 □否，預計完成時間 年 月 日	請說明系統是否提供雜湊驗證碼供資料取得者檢核所取得資料之完整性，避免資料遭竄改
定期備份日誌至原系統外之其他實體系統。(如 Log 伺服器)。			●	□是 □不適用 □否，預計完成時間 年 月 日	定期進行日誌異機備份，如建置 Log 伺服器或設定系統排程等方式，集中管理及保存日誌備份，可降低因系統損毀或人為惡意刪除之風險。

營運持續計畫					
系統備份					
安全需求檢核項目	資通系統資安等級			是否符合	佐證資料或作法說明
	普	中	高		
訂定系統可容忍資料損失之時間要求。	●	●	●	□是 □不適用 □否，預計完成時間 年 月 日	請說明系統可容許損失資料之時間(RPO)為何
執行系統源碼與資料備份。	●	●	●	□是 □不適用 □否，預計完成時間 年 月 日	
應定期測試備份資訊，以驗證備份媒體之可靠性及資訊之完整性。		●	●	□是 □不適用 □否，預計完成時間 年 月 日	請說明貴管系統是否定期執行備份還原演練
應將備份還原，作為營運持續計畫測試之一部分。			●	□是 □不適用 □否，預計完成時	

				間 年 月 日	
應在與運作系統不同地點之獨立設施或防火櫃中，儲存重要資通系統軟體與其他安全相關資訊之備份 。			●	□是 □不適用 □否，預計完成時間 年 月 日	
系統備援					
安全需求檢核項目	資通系統資安等級			是否符合	佐證資料或作法說明
	普	中	高		
訂定資通系統從中斷後至重新恢復服務之可容忍時間要求。		●	●	□是 □不適用 □否，預計完成時間 年 月 日	請說明貴管系統對「可用性」之評估結果為高或中或低? 其可容忍之最大中斷時間為何? (建議：<=8 小時(高)、8-24 小時(中)、超過 24 小時(普))
原服務中斷時，於可容忍時間內，由備援設備或其他方式取代並提供服務 。		●	●	□是 □不適用 □否，預計完成時間 年 月 日	

識別與鑑別					
內部使用者之識別與鑑別(Identification and Authentication)					
安全需求檢核項目	資通系統資安等級			是否符合	佐證資料或作法說明
	普	中	高		
資通系統應具備唯一識別及鑑別機關使用者(或代表機關使用者行為之程序)之功能，禁止使用共用帳號。	●	●	●	□是 □不適用 □否，預計完成時間 年 月 日	請說明系統機制是否可唯一識別且足供鑑別機關內部使用者，禁止使用共同帳號
對資通系統之存取採取多重認證技術。(如鎖 IP)。			●	□是 □不適用 □否，預計完成時間 年 月 日	多重認證技術係指 MFA，意即身分驗證時應具備兩種以上驗證類型，驗證類型一般區分為所知之事(如密碼、特定問題之答案)、所持之物(如晶片卡、憑證)及所具之形(如指紋、虹膜辨識等生物特徵)。使用情境範例如系統管理者透過自然人憑證登入系統後台服務，同時具備所知之事 (PIN 碼)與所持之物(憑證卡片)之要求。
身分驗證管理					
安全需求檢核項目	資通系統資安等級			是否符合	佐證資料或作法說明
	普	中	高		
使用預設密碼登入系統時，應於登入後要求立即變更。	●	●	●	□是 □不適用 □否，預計完成時間 年 月 日	使用者註冊時係由資通系統或人工配發預設密碼者，於使用者首次登入時，應強制其變更預設密碼。
身分驗證相關資訊不以明文傳輸。	●	●	●	□是 □不適用 □否，預計完成時間 年 月 日	身分驗證相關資訊於網路傳輸時，不可直接傳輸明文(如密碼原始字串)，避免被惡意攔截網路封包而外洩。
具備帳戶鎖定機制，帳號登入進行身分驗證失敗達五次後，至少十五分鐘內不	●	●	●	□是 □不適用 □否，預計完成時	系統應實作帳戶鎖定機制，於鎖定期間禁止該

允許該帳號繼續嘗試登入或使用機關自建之失敗驗證機制。				間　年　月　日	帳號所有登入嘗試，超過鎖定時間則重新計次。
基於密碼之鑑別資通系統應強制最低密碼複雜度；強制密碼最短及最長之效期限制。(非內部使用者，可依機關自行規範辦理。)	●	●	●	□是 □不適用 □否，預計完成時間　年　月　日	密碼長度與複雜度是否有要求
使用者更換密碼時，至少不可以與前三次使用過之密碼相同。(非內部使用者，可依機關自行規範辦理。)	●	●	●	□是 □不適用 □否，預計完成時間　年　月　日	更換密碼是否有歷程之要求
身分驗證機制應防範自動化程式之登入或密碼更換嘗試。		●	●	□是 □不適用 □否，預計完成時間　年　月　日	身分驗證是否有防止自動化方式登入(例如增加圖形驗證碼之輸入)
密碼重設機制對使用者重新身分確認後，發送一次性及具有時效性符記。		●	●	□是 □不適用 □否，預計完成時間　年　月　日	密碼重設時發送之驗證過程(如:驗證碼、驗證連結)應有時效限制
鑑別資訊回饋					
安全需求檢核項目	資通系統資安等級			是否符合	佐證資料或作法說明
	普	中	高		
資通系統應遮蔽在鑑別過程中之資訊(如通行碼)，以防止未授權之使用者可能之窺探/使用。	●	●	●	□是 □不適用 □否，預計完成時間　年　月　日	系統登入時之密碼是否不以明文顯示
加密模組鑑別					
安全需求檢核項目	資通系統資安等級			符合度	佐證資料或作法說明
	普	中	高		
資通系統如以密碼進行鑑別時，該密碼應加密或經雜湊處理後儲存。		●	●	□是 □不適用 □否，預計完成時間　年　月　日	密碼是否以明碼方式儲存
非內部使用者之識別與鑑別					
安全需求檢核項目	資通系統資安等級			符合度	佐證資料或作法說明
	普	中	高		
資通系統應識別及鑑別非機關使用者(或代表機關使用者行為之程序)。	●	●	●	□是 □不適用 □否，預計完成時間　年　月　日	請說明系統機制是否可識別且足供鑑別機關內、外部使用者

系統與服務獲得					
系統發展生命週期需求階段					
安全需求檢核項目	資通系統資安等級			是否符合	佐證資料或作法說明
	普	中	高		
針對系統安全需求(含機密性、可用性、完整性)進行確認。	●	●	●	□是 □不適用 □否，預計完成時間　年　月　日	建議可使用本附件進行系統安全需求檢核。
系統發展生命週期設計階段					
安全需求檢核項目	資通系統資安等級			是否符合	佐證資料或作法說明
	普	中	高		
根據系統功能與要求，識別可能影響系統之威脅，進行風險分析及評估。		●	●	□是 □不適用 □否，預計完成時間　年　月　日	可參照「安全軟體設計參考指引」[3]之第3章安全軟體設計階段實務活動，包含「安全設計原則」，進行系統設計時應參考使用的設計原則；「執行攻擊面分析」，進行攻擊面的定義、識別與對應方式，包含如何進行攻擊面的衡量與評估，並進行管

					理等；「執行風險分析」，軟體設計過程中，如何透過使用威脅建模與架構風險分析，進行系統架構與威脅的分析，並使用通用性的安全設計原則與控制措施，提供軟體安全風險分析與控制；「安全設計審查」，在進行一連安全軟體設計的實務活動之後，應確保安全設計符合需求階段提出的相關安全需求及安全設計，以符合軟體安全的基準線。
將風險評估結果回饋需求階段之檢核項目，並提出安全需求修正。		●	●	□是 □不適用 □否，預計完成時間 年 月 日	應用系統安全需求查檢表
系統發展生命週期開發階段					
安全需求檢核項目	資通系統資安等級			是否符合	佐證資料或作法說明
	普	中	高		
應針對安全需求實作必要控制措施。	●	●	●	□是 □不適用 □否，預計完成時間 年 月 日	應用系統安全需求查檢表
應注意避免軟體常見漏洞(如 OWASP TOP 10)及實作必要控制措施。	●	●	●	□是 □不適用 □否，預計完成時間 年 月 日	應用系統安全需求查檢表、資安檢測報告
發生錯誤時，使用者頁面僅顯示簡短錯誤訊息及代碼，不包含詳細之錯誤訊息。	●	●	●	□是 □不適用 □否，預計完成時間 年 月 日	請說明系統是否已避免於系統錯誤時顯示詳細錯誤訊息(如明確指出是帳號或密碼錯誤)，以免有心人士得知系統太多細節
執行「源碼掃描」安全檢測。			●	□是 □不適用 □否，預計完成時間 年 月 日	是否有源碼檢測紀錄
系統應具備發生嚴重錯誤時之通知機制。			●	□是 □不適用 □否，預計完成時間 年 月 日	系統在嚴重錯誤時是否有通知機制?機制為何?
系統發展生命週期測試階段					
安全需求檢核項目	資通系統資安等級			是否符合	佐證資料或作法說明
	普	中	高		
執行「弱點掃描」安全檢測。	●	●	●	□是 □不適用 □否，預計完成時間 年 月 日	是否有弱點掃描紀錄
執行「滲透測試」安全檢測。			●	□是 □不適用 □否，預計完成時間 年 月 日	是否有滲透測試紀錄
系統發展生命週期部署與維運階段					
安全需求檢核項目	資通系統資安等級			是否符合	佐證資料或作法說明
	普	中	高		
於部署環境中應針對相關資通安全威脅，進行更新與修補，並關閉不必要服務及埠口。	●	●	●	□是 □不適用 □否，預計完成時間 年 月 日	就作業系統或平台之安全更新，定期評估、測試與更新。系統上線前，就作業系統或平台預設開啟的服務與埠口(Port)進行檢視與評

					估，正面表列需要開啟該服務及埠口之理由，並關閉不必要之項目。
資通系統不使用預設密碼。	●	●	●	□是 □不適用 □否，預計完成時間 年 月 日	資通系統使用之相關軟體是否使用預設密碼?
於系統發展生命週期之維運階段，須注重版本控制與變更管理。		●	●	□是 □不適用 □否，預計完成時間 年 月 日	版本版次之管理方式為何? 系統變更是否填寫變更申請單?
系統發展生命週期委外階段					
安全需求檢核項目	資通系統資安等級			是否符合	佐證資料或作法說明
	普	中	高		
資通系統開發如委外辦理，應將系統發展生命週期各階段依等級將安全需求(含機密性、可用性、完整性)納入委外契約。	●	●	●	□是 □不適用 □否，預計完成時間 年 月 日	
獲得程序					
安全需求檢核項目	資通系統資安等級			是否符合	佐證資料或作法說明
	普	中	高		
開發、測試以及正式作業環境應為區隔。		●	●	□是 □不適用 □否，預計完成時間 年 月 日	開發、測試及正式環境是否區隔
系統文件					
安全需求檢核項目	資通系統資安等級			是否符合	佐證資料或作法說明
	普	中	高		
應儲存與管理系統發展生命週期之相關文件。	●	●	●	□是 □不適用 □否，預計完成時間 年 月 日	資通系統從評估、規劃、招標、建置乃至維運過程之相關文件是否妥善保存

系統與通訊保護					
傳輸之機密性與完整性					
安全需求檢核項目	資通系統資安等級			是否符合	佐證資料或作法說明
	普	中	高		
資通系統應採用加密機制，以防止未授權之資訊揭露或偵測資訊之變更。但傳輸過程中有替代之實體保護措施者，不在此限。			●	□是 □不適用 □否，預計完成時間 年 月 日	網站傳輸資料時，是否採用 HTTPS(透過 SSL 或 TLS 等加密協定)協定以確保資料以密文方式傳輸
使用公開、國際機構驗證且未遭破解之演算法。			●	□是 □不適用 □否，預計完成時間 年 月 日	不使用自行創造的加密方式，採用公開、國際認可之演算法，例如 AES、RSA 及 SHA 安全雜湊等演算法
支援演算法最大長度金鑰。			●	□是 □不適用 □否，預計完成時間 年 月 日	請說明系統採用之密碼學演算法，是否使用該演算法目前支援的最大金鑰長度，以減少被暴力破解之可能。例如 AES 256 bits、RSA 2048 bits、SHA-512 等或以上。
加密金鑰或憑證週期性更換。			●	□是 □不適用 □否，預計完成時間 年 月 日	產生網站 HTTPS 使用之憑證，應具備使用年限限制，並於到期前進行

					更 換。系統若另行使用自行產生之加密金鑰，亦需定期更換。
伺服器端之金鑰保管應訂定管理規範及實施應有之安全防護措施。			●	□是 □不適用 □否，預計完成時間 年 月 日	請說明針對使用的金鑰是否以密碼保護，並進行備份及妥善保管；且加密金鑰不與加密資料存放於同一系統中，並對於加密金鑰的存取進行限制

資料儲存之安全

安全需求檢核項目	資通系統資安等級			是否符合	佐證資料或作法說明
	普	中	高		
資通系統重要組態設定檔案及其他具保護需求之資訊應加密或以其他適當方式儲存。			●	□是 □不適用 □否，預計完成時間 年 月 日	請說明系統是否已定義哪些資料屬機密資料?其於資料庫或其他儲存裝置上是否加密儲存?以減少機敏資料因儲存媒體或裝置有其他存取管道而洩漏的風險

系統與資訊完整性

漏洞修復

安全需求檢核項目	資通系統資安等級			是否符合	佐證資料或作法說明
	普	中	高		
系統之漏洞修復應測試有效性及潛在影響，並定期更新。	●	●	●	□是 □不適用 □否，預計完成時間 年 月 日	系統弱點掃描、漏洞修補紀錄
定期確認資通系統相關漏洞修復之狀態。		●	●	□是 □不適用 □否，預計完成時間 年 月 日	系統弱點掃描、漏洞修補紀錄

資通系統監控

安全需求檢核項目	資通系統資安等級			是否符合	佐證資料或作法說明
	普	中	高		
發現資通系統有被入侵跡象時，應通報機關特定人員。	●	●	●	□是 □不適用 □否，預計完成時間 年 月 日	
監控資通系統，以偵測攻擊與未授權之連線，並識別資通系統之未授權使用。		●	●	□是 □不適用 □否，預計完成時間 年 月 日	
資通系統應採用自動化工具監控進出之通信流量，並於發現不尋常或未授權之活動時，針對該事件進行分析。			●	□是 □不適用 □否，預計完成時間 年 月 日	請說明是否對系統進出流量進行監控，於發現異常時之處置為何?

軟體及資訊完整性

安全需求檢核項目	資通系統資安等級			是否符合	佐證資料或作法說明
	普	中	高		
使用完整性驗證工具，以偵測未授權變更特定軟體及資訊。		●	●	□是 □不適用 □否，預計完成時間 年 月 日	請說明是否使用完整性驗證工具(checksum 原理)偵測軟體或資訊是否遭受未經授權之變更
使用者輸入資料合法性檢查應置放於應用系統伺服器端。		●	●	□是 □不適用 □否，預計完成時間 年 月 日	請說明對於使用者輸入欄位資料，是否於伺服器端進行合法性檢查，僅允許輸入特定白名單內容，檢查其邏輯規則是否合法。

發現違反完整性時，資通系統應實施機關指定之安全保護措施。		●	●	□是 □不適用 □否，預計完成時間 年 月 日	
應定期執行軟體與資訊完整性檢查。			●	□是 □不適用 □否，預計完成時間 年 月 日	是否定期執行軟體與資訊完整性檢查並留下紀錄

註：

- 如套裝軟體有低度客製化，仍屬於自行或委外開發之資通系統，須依資通安全責任等級分級辦法第11條規定，完成資通系統防護需求分級，並依系統防護基準執行相關控制措施。
- 依資通系統防護需求分級後，系統為「中」者須同時符合「普、中」要求；系統為「高」者須同時符合「普、中、高」要求。

承辦人: 單位主管： 資訊室複核：

附件三：廠商資安管理作業自評表

參與國家電影及視聽文化中心辦理
「_____」（標案名稱）
資安管理作業自評表

填表日期：　年　月　日

評估項目	辦理情形
1.管理面	
1.1 辦理本專案受託業務相關程序及環境之資通安全管理措施或通過第三方驗證	□辦理本專案受託業務之相關程序及環境已(將)通過_____認(驗)證並持續有效，驗證公司為_____ □辦理本專案受託業務之相關程序及環境已具備完善資安管理措施，詳_____文件(如未載明於既有文件內，請於備註欄內說明相關措施) □本專案受託業務之相關程序及環境未導入適當資安管理措施 備註：_____
1.2 本專案之資安負責人、資安專責主管或其他資安人員之人力配置規劃	□本專案之資安負責人(專案主管)為____ □本專案之資安人員為____ □本專案未指派資安負責人、資安專責主管或其他資安人員 備註：_____
1.3 本專案之資安風險評估，包含可能之資通系統機密性、完整性、可用性風險，及採取之對應控制措施	□本專案受託業務相關程序及環境之資安風險評估結果已(將)載明於____文件，已(將)採取對應之控制措施詳____文件(如未載明於既有文件內，請於備註欄內說明相關措施) □未就本專案進行資安風險評估 備註：_____
1.4 本專案範圍內之資安事件通報應變程序，包含知悉資安事件發生或有發生之虞之相關通報時效規定、通報方式、資安事件調查、處理及改善流程	□本專案受託業務相關程序及環境之資安事件通報應變程序已(將)載明於_____文件(如未載明於既有文件內，請於備註欄內說明相關措施)，知悉資安事件或發現有事件發生之虞時，應於__小時內向甲方等相關利害關係人通報，通報對象包含____ □未就本專案訂定相關資安事件通報及應變程序 備註：_____
1.5 由招標公告日起算，過去 3 年是否發生因管理議題肇因之重大資安事件	□過去 3 年無發生因管理議題肇因之資安事件 □是，共__次，事件發生主要根因為____ 備註：_____
2.技術面	
2.1 本專案範圍內之資通系統，包含主要履約標的之資通系統及其他執行本專案業務所需使用之業務、行政相關資通系統，辦理安全性檢測	□本專案範圍內之資通系統將規劃執行_____(如源碼掃描、弱點掃描、滲透測試)，檢測項目及本專案範圍為：_____ □未就本專案範圍內之資通系統規劃安全性檢測 備註：_____

2.2 辦理本專案受託業務環境及設備導入之相關資通安全防護措施	□本專案受託業務之環境及設備已(將)導入(啟用)_____(如防毒軟體、防火牆、電子郵件過濾機制、入侵偵測及防禦機制等)，導入項目及本專案範圍為：_____ □本專案受託業務之環境及設備未導入相關資通安全防護措施 備註：_____
2.3 本專案範圍內之資通系統及專案資料之存取控制等權限管理機制，如PM、系統管理員、一般使用者帳號之權限分級原則及控管方式	□本專案範圍內之資通系統帳號或使用者權限分成__種等級，相關存取控制、權限管理機制說明如下：____ □未規劃本專案範圍內之資通系統及專案資料相關存取控制及權限管理機制 備註：_____
3.認知訓練面	
3.1 本專案直接履約相關人員之資安教育訓練	□本專案直接履約相關人員之資安教育訓練包含__小時之資安通識教育訓練，對象包含____；__小時之資安專業教育訓練，對象包含____ □未規劃相關資安教育訓練 備註：_____
3.2 本專案團隊人員取得之資通安全專業證照	□本專案具資安證照之團隊成員有：__位 □本專案團隊人員未具備資通安全專業證照 備註：_____

廠商用印：

國家電影及視聽文化中心
資通安全政策

一、　確保本範圍內各項資通作業均符合相關法規要求。
二、　確保本範圍內妥適保護所屬資通資產之機密性、完整性及可用性，避免未經授權之存取與修改。
三、　確保本範圍內對外資通相關服務之持續運作。

本中心爲國內唯一典藏影視聽資產專責行政法人機構，致力於影視聽資產典藏研究修復推廣、實現資產公共化任務為宗旨。期以建立安全資訊作業環境，保護各類資訊資產之安全，避免因外來之威脅、內部人員不當的管理或使用，而導致資訊資產遭受竄改、揭露、破壞或遺失等風險發生，確保資訊資產之機密性、完整性與可用性獲得保障。據此，建立本中心資訊安全管理體系與資訊安全管理準則，期能合理與有效地降低營運風險，特訂定「資通安全政策」。

資通安全政策 112 年 8 月 28 核定公告

附件五：「委外服務團隊成員名冊暨保密同意書與切結書」、「資通安全聯絡人員表」

委外服務團隊成員名冊

廠商及分包商名稱及地址	廠商及分包廠商國別	姓名	職稱	國籍	學歷/經歷	負責工作項目

保密同意書

茲緣於簽署人 ……（簽署人姓名，以下稱簽署人）參與……（廠商名稱，以下稱廠商）得標**國家電影及視聽文化中心**（本中心名稱）（以下稱本中心）資訊業務委外案「114 年網頁應用程式防火牆汰換案」（案名）（以下稱「本案」），於本案執行期間有知悉或可得知悉或持有政府公務秘密及業務秘密，為保持其秘密性，簽署人同意恪遵本同意書下列各項規定：

第1條　簽署人承諾於本契約有效期間內及本契約期滿或終止後，對於所得知或持有一切本中心未標示得對外公開之公務秘密，以及本中心依契約或法令對第三人負有保密義務之業務秘密，均應以善良管理人之注意妥為保管及確保其秘密性，並限於本契約目的範圍內，於本中心指定之處所內使用之。非經本中心事前書面同意，不得為本人或任何第三人之需要而複製、保有、利用該等秘密或將之洩漏、告知、交付第三人或以其他任何方式使第三人知悉或利用該等秘密，或對外發表或出版，亦不得攜至本中心或本中心所指定處所以外之處所。

第2條　簽署人知悉或取得本中心公務秘密與業務秘密應限於其執行本契約所必需且僅限於本契約有效期間內。簽署人同意公務秘密與業務秘密，應僅提供、告知有需要知悉該秘密之履約廠商團隊成員人員。

第3條　簽署人在下述情況下解除其所應負之保密義務：

原負保密義務之資訊，由本中心提供以前，已合法持有或已知且無保密必要者。

原負保密義務之資訊，依法令業已解密、依契約本中心業已不負保密責任、或已為公眾所知之資訊。

原負保密義務之資訊，係自第三人處得知或取得，該第三人就該等資訊並無保密義務。

第4條　簽署人若違反本同意書之規定，本中心得請求簽署人及其任職之廠商賠償本中心因此所受之損害及追究簽署人洩密之刑責，如因而致第三人受有損害者，簽署人及其任職之廠商亦應負賠償責任。

第5條　簽署人因本同意書所負之保密義務，不因離職或其他原因不參與本案而失其效力。

第6條　本同意書一式叁份，本中心、簽署人及……（廠商）各執存一份。

簽署人姓名及簽章：

身分證字號：

聯絡電話：

戶籍地址：

所屬廠商名稱及蓋章：

所屬廠商負責人姓名及簽章：

所屬廠商地址：

中　華　民　國　　年　　月　　日

保密切結書

立切結書人.....（簽署人姓名）等，受.....（廠商名稱）委派至**國家電影及視聽文化中心**（本中心名稱，以下稱本中心）處理業務，謹聲明恪遵本中心下列工作規定，對工作中所持有、知悉之資訊系統作業機密或敏感性業務檔案資料，均保證善盡保密義務與責任，非經本中心權責人員之書面核准，不得擷取、持有、傳遞或以任何方式提供給無業務關係之第三人，如有違反願賠償一切因此所生之損害，並擔負相關民、刑事責任，絕無異議。

1、 未經申請核准，不得私自將本中心之資訊設備、媒體檔案及公務文書攜出。
2、 未經本中心業務相關人員之確認並代為申請核准，不得任意將攜入之資訊設備連接本中心網路。若經申請獲准連接本中心網路，嚴禁使用數據機或無線傳輸等網路設備連接外部網路。
3、 經核准攜入之資訊設備欲連接本中心網路或其他資訊設備時，須經電腦主機房掃毒專責人員進行病毒、漏洞或後門程式檢測，通過後發給合格標籤，並將其粘貼在設備外觀醒目處以備稽查。
4、 廠商駐點服務及專責維護人員原則應使用本中心配發之個人電腦與週邊設備，並僅開放使用本中心內部網路。若因業務需要使用本中心電子郵件、目錄服務，應經本中心業務相關人員之確認並代為申請核准，另欲連接網際網路亦應經本中心業務相關人員之確認並代為申請核准。
5、 本中心得定期或不定期派員檢查或稽核立切結書人是否符合上列工作規定。
6、 本保密切結書不因立切結書人離職而失效。
7、 立切結書人因違反本保密切結書應盡之保密義務與責任致生之一切損害，立切結書人所屬公司或廠商應負連帶賠償責任。

立切結書人：

姓名及簽章	身分證字號	聯絡電話及戶籍地址
_____	_____	_____
_____	_____	_____

立切結書人所屬廠商：

廠商名稱及蓋章	廠商負責人姓名及簽章	廠商聯絡電話及地址
_____	_____	_____

填表說明：

1、 廠商駐點服務人員、專責維護人員，或逗留時間超過三天以上之突發性維護增援、臨時性系統測試或教育訓練人員（以授課時需連結本中心網路者為限）及經常到本中心洽公之業務人員皆須簽署本切結書。
2、 廠商駐點服務人員、專責維護人員及經常到本中心洽公之業務人員每年簽署本切結書乙次。

中　華　民　國　　年　　月　　日

資通安全聯絡人員表

單位	職稱	姓名	電話	手機	工作職掌

附件六：備份機制明細表

備份機制明細表

資通系統/檔案名稱：　　填寫日期：

序號	備份方式					備份來源地					備份目的地		
	備份軟體/方式	備份種類	備份型態	備份週期	備份方式	備份頻率	主機名稱	主機IP	系統名稱	存放路徑	備份資料名稱	檔案預估大小	存放路徑
1		□資料庫 □程式碼 □電子檔 □其他	□完整 □差異 □增量	□定期 □不定期									
2		□資料庫 □程式碼 □電子檔 □其他	□完整 □差異 □增量	□定期 □不定期									
3		□資料庫 □程式碼 □電子檔 □其他	□完整 □差異 □增量	□定期 □不定期									
4		□資料庫 □程式碼 □電子檔 □其他	□完整 □差異 □增量	□定期 □不定期									
5		□資料庫 □程式碼 □電子檔 □其他	□完整 □差異 □增量	□定期 □不定期									

系統廠商	業務單位		資訊室	
	承辦人	單位主管	承辦人	單位主管

附件七：備份測試查核表

備份測試查核表

測試人員：_____ 測試時間：_____	
測試主機名稱：_____ 測試主機來源 IP：_____ 測試主機作業系統：_____	
來源主機名稱：_____ 來源 IP：_____ 來源作業系統：_____	
本地備份測試狀況說明：	
異地備份測試狀況說明：	
其他事項：	
承辦人員	承辦單位主管
備註： 1.備份回復測試應至少每年執行 1 次。 2.請檢附測試復原步驟相關佐證資料（如系統畫面等）。	

附件八：未使用大陸廠牌切結書

本廠商＿＿＿＿＿＿承攬國家電影及視聽文化中心【114年網頁應用程式防火牆汰換案】採購案，已充分了解公務機關及委外廠商、分包廠商，不得採購及使用大陸廠牌資通訊產品，禁止使用大陸廠牌資通訊產品處理公務事務或介接公務環境，保證本廠商所提供之資通軟體或系統、資通訊設備、資通服務，包括但不限於以下內容：

一、 軟體：資通軟體或系統，如應用軟體、系統軟體、開發工具、客製化套裝軟體、APP及電腦作業系統等。

二、 硬體：具連網能力、資料處理或控制功能者皆屬廣義之資通訊設備，如個人電腦、伺服器、無人機、印表機、網路通訊設備、可攜式設備及物聯網設備（包括監視系統、網路電話、會議系統、電話總機系統、電視、影印機、門禁系統、事務機等）等。

三、 服務：資通服務，如客服服務及軟硬體資產維護服務等。

保證絕無採購或使用「大陸廠牌資通訊產品及服務」，如有違反，願無條件全部更換為國產或貴中心所指定之相當非大陸廠商產品。

立書人

廠 商：　　（蓋章）

負責人：　　（蓋章）

地址：

電話：

中 華 民 國　　年　　月　　日

附件九：資料所在地及跨境傳輸切結書

資料所在地及跨境傳輸 切結書

本廠商_____參與（招標機關）辦理_____招標案，對於廠商之責任，包括刑事、民事與行政責任，已充分瞭解相關之法令規定，並願確實遵行，簽結承諾事項如下：

1、 本公司目前是否有中國大陸地區廠商或人民持股情形？
□本公司無中國大陸地區廠商或人民持股情形。
□有中國大陸地區廠商或人民持股情形，其佔比情形及相關說明如下：
_____
_____

2、 本公司及涉及本案之分包廠商是否為中國大陸地區廠商？
□本公司及涉及本案之分包廠商皆非屬中國大陸地區廠商。
□有中國大陸地區廠商，說明如下：
_____
_____

3、 執行本案之團隊成員是否有中國大陸國籍人士(多重國籍者，若有屬中國大陸國籍者亦屬之)？
□執行本案之團隊成員皆無陸籍人士。
□本案之團隊成員有陸籍人士，說明如下：
_____
_____

4、 本公司及涉及本案之分包廠商，是否於中國大陸地區(含香港、澳門)設立相關團隊據點？如是，則該據點與本案履約間之關係為何？
□否，本公司及涉及本案之分包廠商，皆未於中國大陸地區設立相關團隊據點。
□是，該據點與本案履約間之關係，說明如下：
_____
_____

5、 本公司針對本案所提供機關(共用)產品或服務之所屬一切資料存取、備份及備援之實體所在地是否有置於中國大陸地區(含香港、澳門)之情形？或跨該等境內傳輸相關資料？
□否，本公司針對本案所提供機關(共用)產品或服務之所屬一切資料存取、儲存、備份及備援等作業，皆無置於中國大陸地區(含香港、澳門)之情形，且未經該等境內傳輸相關資料。
□是，有置於中國大陸地區(含香港、澳門)或該等境內傳輸相關資料，說明如下：
_____
_____

廠　商：　　（簽名蓋章）

負責人：　　（簽名蓋章）

中華民國　　年　　月　　日

附件十：委外廠商查核項目表

委外廠商查核項目表

契約案名/編號：○○

填表日期：　　年　　月　　日

查核項目	查核內容	查核結果			說明
		符合	不符合	不適用	
1.資通安全政策之推動及目標訂定	1.1 是否定義符合組織需要之資通安全政策及目標？	□	□	□	
	1.2 組織是否訂定資通安全政策及目標？	□	□	□	
	1.3 組織之資通安全政策文件是否由管理階層核准並正式發布且轉知所有同仁？	□	□	□	
	1.4 組織是否對資通安全政策、目標之適切性及有效性，定期作必要之審查及調整？	□	□	□	
	1.5 是否隨時公告資通安全相關訊息？	□	□	□	
2.設置資通安全推動組織	2.1 是否指定適當權責之高階主管負責資通安全管理之協調、推動及督導等事項？	□	□	□	
	2.2 是否指定專人或專責單位，負責辦理資通安全政策、計畫、措施之研議，資料、資通系統之使用管理及保護，資安稽核等資安工作事項？	□	□	□	
	2.3 是否訂定組織之資通安全責任分工？	□	□	□	
3.配置適當之資通安全專業人員及適當之資源	3.1 是否訂定人員之安全評估措施？	□	□	□	
	3.2 是否符合組織之需求配置專業資安人力？	□	□	□	
	3.3 是否具備相關專業資安證照或認證？	□	□	□	
	3.4 是否配置適當之資源？	□	□	□	
4.資訊及資通系統之盤點及風險評估	4.1 是否建立資訊及資通系統資產目錄，並隨時維護更新？	□	□	□	
	4.2 各項資產是否有明確之管理者及使用者？	□	□	□	
	4.3 是否定有資訊、資通系統分級與處理之相關規範？	□	□	□	
	4.4 是否進行資訊、資通系統之風險評估，並採取相應之控制措施？	□	□	□	
5.資通安全管理措施之實施情況	5.1 人員進入重要實體區域是否訂有安全控制措施？	□	□	□	
	5.2 重要實體區域的進出權利是否定期審查並更新？	□	□	□	
	5.3 電腦機房及重要地區，對於進出人員是否作必要之限制及監督其活動？	□	□	□	
	5.4 電腦機房操作人員是否隨時注意環境監控系統，掌握機房溫度及溼度狀況？	□	□	□	
	5.5 各項安全設備是否定期檢查？同仁有否施予適當的安全設備使用訓練？	□	□	□	
	5.6 第三方支援服務人員進入重要實體區域是否經過授權並陪同或監視？	□	□	□	

查核項目	查核內容	查核結果			說明
		符合	不符合	不適用	
	5.7 重要資訊處理設施是否有特別保護機制？	□	□	□	
	5.8 重要資通設備之設置地點是否檢查及評估火、煙、水、震動、化學效應、電力供應、電磁幅射或民間暴動等可能對設備之危害？	□	□	□	
	5.9 電源之供應及備援電源是否作安全上考量？	□	□	□	
	5.10通訊線路及電纜線是否作安全保護措施？	□	□	□	
	5.11設備是否定期維護，以確保其可用性及完整性？	□	□	□	
	5.12設備送場外維修，對於儲存資訊是否訂有安全保護措施？	□	□	□	
	5.13可攜式的電腦設備是否訂有嚴謹的保護措施(如設通行碼、檔案加密、專人看管)？	□	□	□	
	5.14設備報廢前是否先將機密性、敏感性資料及版權軟體移除或覆寫？	□	□	□	
	5.15公文及儲存媒體在不使用或不在班時是否妥為存放？機密性、敏感性資訊是否妥為收存？	□	□	□	
	5.16系統開發測試及正式作業是否區隔在不同之作業環境？	□	□	□	
	5.17是否全面使用防毒軟體並即時更新病毒碼？	□	□	□	
	5.18是否定期對電腦系統及資料儲存媒體進行病毒掃瞄？	□	□	□	
	5.19是否定期執行各項系統漏洞修補程式？	□	□	□	
	5.20是否要求電子郵件附件及下載檔案在使用前需檢查有無惡意軟體(含病毒、木馬或後門等程式)？	□	□	□	
	5.21重要的資料及軟體是否定期作備份處理？	□	□	□	
	5.22備份資料是否定期回復測試，以確保備份資料之有效性？	□	□	□	
	5.23對於敏感性、機密性資訊之傳送是否採取資料加密等保護措施？	□	□	□	
	5.24是否訂定可攜式媒體(磁帶、磁片、光碟片、隨身碟及報表等)管理程序？	□	□	□	
	5.25是否訂定使用者存取權限註冊及註銷之作業程序？	□	□	□	
	5.26使用者存取權限是否定期檢查(建議每六個月一次)或在權限變更後立即複檢？	□	□	□	
	5.27通行碼長度是否超過 6 個字元(建議以 8 位或以上為宜)？	□	□	□	
	5.28通行碼是否規定需有大小寫字母、數字及符號組成？	□	□	□	
	5.29是否依網路型態(Internet、Intranet、Extranet)訂定適當的存取權限管理方式？	□	□	□	
	5.30對於重要特定網路服務，是否作必要之控制措施，如身份鑑別、資料加密或網路連線控制？	□	□	□	

查核項目	查核內容	查核結果			說明
		符合	不符合	不適用	
	5.31是否訂定行動式電腦設備之管理政策(如實體保護、存取控制、使用之密碼技術、備份及病毒防治要求)?	□	□	□	
	5.32重要系統是否使用憑證作為身份認證?	□	□	□	
	5.33系統變更後其相關控管措施與程序是否檢查仍然有效?	□	□	□	
	5.34是否可及時取得系統弱點的資訊並作風險評估及採取必要措施?	□	□	□	
6.訂定資通安全事件通報及應變之程序及機制	5.1 是否建立資通安全事件發生之通報應變程序?	□	□	□	
	5.2 機關同仁及外部使用者是否知悉資通安全事件通報應變程序並依規定辦理?	□	□	□	
	5.3 是否留有資通安全事件處理之記錄文件，記錄中並有改善措施?	□	□	□	
7.定期辦理資通安全認知宣導及教育訓練	7.1 是否定期辦理資通安全認知宣導?	□	□	□	
	7.2 是否對同仁進行資安評量?	□	□	□	
	7.3 同仁是否依層級定期舉辦資通安全教育訓練?	□	□	□	
	7.4 同仁是否瞭解單位之資通安全政策、目標及應負之責任?	□	□	□	
8.資通安全維護計畫實施情形之精進改善機制	8.1 是否設有稽核機制?	□	□	□	
	8.2 是否定有年度稽核計畫?	□	□	□	
	8.3 是否定期執行稽核?	□	□	□	
	8.4 是否改正稽核之缺失?	□	□	□	
9.資通安全維護計畫及實施情形之績效管考機制	10.1是否訂定安全維護計畫持續改善機制?	□	□	□	
	10.2是否追蹤過去缺失之改善情形?	□	□	□	
	10.3是否定期召開持續改善之管理審查會議?	□	□	□	

廠商名稱：

廠商用印：

本中心複核人員:

附件十一：資料返還、刪除、銷毀切結書

資料返還、刪除、銷毀切結書

立書人（廠商名稱）執行國家電影及視聽文化中心 「○○○○購案(案號：　　)」(以下稱本案)，於結束本案或契約約定之保固期限期滿時，保證返還、刪除或銷毀因執行本案取得或持有之應保密之資料、檔案或其他任何形式之紀錄、影本或複本，並留存相關軌跡紀錄或其他佐證資料，且確認參與本案之相關人員未以任何形式留存任何應保密內容。若有違反本切結書之情形時，願負相關法律及賠償責任。

此致

國家電影及視聽文化中心

廠商名稱：

負責人：

統一編號：

地址：

日 期：