國立臺灣博物館資訊管理作業原則

中華民國 101 年 8 月 27 日臺博秘字第 1013001717 號函訂定

第一章 總則

一、 國立臺灣博物館(以下簡稱本館)爲維護資訊作業環境之安全，特訂定國立臺灣博物館資訊管理作業原則(以下簡稱本原則)。

二、 本館資訊作業環境安全管理，包含資訊資產管理、網路使用行為管理與資通安全緊急應變作業管理。

三、 本館資訊資產包含電腦系統、實體設備、作業紀錄、人力以及作業流程。依據各類資產之重要性及可能面臨之風險，訂定管理及保護措施。

四、 本館網路範圍，涵蓋各館區之區域網路、無線網路及連結網際網路專線。

第二章 資訊資產管理

五、 電腦系統管理

（一）涵蓋範圍及重要性

1. 本館電腦系統主要包含作業系統、應用系統、套裝軟體、驅動程式及公用程式等類別。
2. 作業系統為電腦主機運轉平台，重要等級為「高」;應用系統為業務輔助工具，重要等級為「高」；套裝軟體為館務維運工具，重要等級為「中」;驅動程式因可上網免費取得，重要等級為「低」。

（二）面臨的風險

本館電腦系統可能遭受的風險有非法使用、中毒、被植入惡意軟體、被冒充使用及操作錯誤等。

（三）管理及保護措施

1. 本館每年編列預算購置正版軟體，軟體採購驗收時同步進行軟體登錄列管，軟體安裝檔案及授權文件由資訊人員統一保管。
2. 資訊人員應建置全館防毒系統，防止病毒入侵，並透過資安會議、館務會議、或e-mail加強網路安全使用行為之宣導。
3. 本館人員應隨時注意資安漏洞訊息，並依照資訊人員發布之通告修補既有系統漏洞。

4. 資訊人員辦理個人電腦保養作業時，應進行使用者電腦安裝之軟體合法性檢視、惡意程式檢測及軟體漏洞修補等資安防護作業。

六、 實體設備管理

（一）涵蓋範圍及重要性

1. 實體設備主要包含本館個人電腦及周邊、可攜式設備、伺服器、網路主幹設備及機房設施等類別。
2. 個人電腦、伺服器、網路主幹設備及機房設施遭受損害時影響業務運作，重要性等級為「高」。
3. 可攜式設備容易攜出館外，成為資料外洩或駭客入侵管道，重要性等級為「高」。
4. 個人電腦周邊可分享使用、替代性高，重要性等級為「中」。

（二）面臨的風險

實體設備可能遭受的風險有遭竊、損毀、遭駭客入侵、惡意破壞、硬體失能以及操作錯誤等。

（三）管理及保護措施

1. 資訊資產購置時，應由秘書室確實登錄列帳管理，每年應進行資訊設備盤點至少一次。
2. 本館於重要辦公室出入口設置門禁及攝影機，記錄人員進出狀況及所攜帶之物品。
3. 硬體故障應先由資訊人員診斷並排除故障原因，無法修復時再移請專業廠商處理。
4. 可攜式設備由各組室指派專人管理，操作使用時應注意：
   （1）預防設備摔落或重創造成損壞。
   （2）儲存於設備之重要資料應經常備份至館內硬碟。
   （3）攜帶式電腦離線後再次使用本館網路前，應先進行病毒碼更新及系統漏洞修補。
5. 資訊人員應定期進行機房主機維護作業，紀錄硬體使用狀況；秘書室應每年配合大樓消防安檢，進行大樓消防偵煙器材檢測，降低火災的危害。

七、 資訊紀錄管理

（一）涵蓋範圍及重要性

1. 資訊紀錄主要包含採購專案文件、系統文件、維護紀錄、資料庫紀錄以及資料檔案等類別。
2. 採購專案文件與系統文件為系統軟硬體合法取得、規劃開發及操作使用重要文件，重要性等級為「高」。
3. 資料庫紀錄以及資料檔案為本館數位知識資產，重要性等級為「高」。
4. 維護紀錄為實體運作狀況紀錄，重要性等級為「中」。

（二）面臨的風險

資訊紀錄可能遭受的風險有遺失、損毀、洩漏、不當存取及竄改等。

（三）管理及保護措施

1. 採購專案文件由秘書室辦理採購作業時收集及保管。
2. 系統文件於系統驗收完成後，由專案承辦人繳交一份至資訊人員保管。
3. 本館委外開發之系統進行資料異動時，應建立自動儲存建檔者及建檔日期之機制，避免不當操作。
4. 本館資料庫備份作業，應由各系統管理者依資料增長狀況制定備份策略。建置於機房之系統，由資訊人員進行備份，建置於各組室之系統，由該組室負責資料備份。

八、 人力及作業流程管理

（一）涵蓋範圍及重要性

1. 人力管理包含本館員工、臨時人員、承包廠商人員及駐館工程師等人力管理，重要性等級為「高」。
2. 作業流程管理如系統開發作業、藏品數位化作業等流程管理，重要性等級為「高」。

（二）面臨的風險

人力及作業流程可能發生的危安風險有洩密、未授權存取、破壞、偷竊、竄改、操作錯誤、植入後門程式及違反智慧財產權等。

（三）管理及保護措施

1. 本館使用資訊系統人員應遵守其工作執掌與保密相關規定。
2. 本館帳號配發前，使用者須簽署同意遵循本館資安政策之規定。人員離職時，終止帳號之使用。
3. 本館系統使用授權由各系統管理者依使用者職務配發及管理，資訊人員及各系統管理者應每年至少進行一次使用者帳號及權限清查。
4. 本館資訊委外契約明定廠商應負之義務與責任，包括：
   （1）委外廠商及派駐人員應遵守保密之義務與責任，並延長至契約終止後之約定時間。
   （2）委外廠商所處理之資料，不得迂迴經過受限制之第三國或地區。
   （3）委外廠商開發使用之工具，以及整合自其他廠商之軟體套件，均不得違反智慧財產權之規定。

第三章 網路使用行為管理

九、 一般性使用原則

（一）本館網路專供公務使用，使用目的應符合連結網際網路專線管理單位之規定。

（二）本館對外之連線，應透過本館設置之網路為之，未經申請不得以其它連線方式與外界網路串連，以免造成安全漏洞。

（三）新建帳號第一次使用時，使用者應更換預設之密碼為優質密碼，並應定期更新。帳號及密碼應妥為保管，不得借與他人使用。離職時，帳號即予停用。

（四）對於自網際網路上取得之資料，應持保留態度，非經證實，不得據以轉發、發布或作為公務之參考資料。

（五）非本館員工因公務需要，得經本館員工授權，始得使用本館網路資源。如有違反規定之情事，授權人員應負連帶責任。

（六）本館員工因業務需要，需由外界直接進入本館內部網路時，應先向本館資訊人員提出申請，經核定並賦予密碼後方可使用。

（七）本館員工發現資通安全或網路遭受危害或有危害之虞時，應立即依本原則進行通報。

十、 禁止使用行為

（一）製造或散布電腦病毒或其他干擾或破壞系統機能之程式。

（二）侵害智慧財產權，如下載或安裝未經授權電腦程式、任意轉載經作者明示禁止轉載之文章或作品等。

（三）以破解、盜用或冒用他人帳號、密碼及 IP 號碼等方式，未經授權使用網路資源，或無故洩漏他人之帳號及密碼。

（四）匿名、隱藏帳號或使用虛假帳號，但經明確授權使用者不在此限。

（五）擅自截取網路傳輸訊息或窺視他人之電子郵件或檔案。

（六）以任何方式濫用網路資源，如以電子郵件大量傳送廣告信、連鎖信或無用之信息，或以灌爆信箱、掠奪資源等方式，影響系統之正常運作。

（七）透過網路散布詐欺、誹謗、侮辱、猥褻、騷擾、非法軟體交易或其他違法之訊息。

（八）利用網路進行賭博性、猥褻性、不友善性及營利性等非關公務之行為。

（九）未經申請，利用本館主機、個人電腦架設網站與私自架設網路基地台(AP)等有危及資安之行為。

第四章 資訊安全管理分工

十一、 本館資訊安全管理由各組室主管、使用者與資訊人員共同維護。

（一）各組室主管應督導所屬員工依規定使用本館網路。

（二）各組室使用者應養成良好上網使用習慣，參加資安講習並遵守本館所訂之各項規範。

（三）資訊人員之職責

1. 負責本館網路基礎架構之建置與管理。
2. 負責本館IP位址及電腦名稱之配發及管理。
3. 負責本館網路之安全管控，定期進行資安檢測防止駭客入侵。如有發現違反規定之情事，得暫停員工網路使用權，

直至危機解除。

十二、 本館資訊使用者如違反本原則或有涉及不法之情事，應負行政及刑事責任；不受考績規範之人員，由其管理者負連帶責任。

第五章 資訊安全緊急應變作業管理

十三、 設置本館常態性任務編組之「資通安全處理小組」，負責執行資通安全預防、危機通報與緊急應變處理相關措施。

十四、 本館「資通安全處理小組」由副館長擔任召集人，各組室主管為小組成員，並設資通安全緊急聯絡人一名，由資訊人員擔任。

十五、 本館發生資通安全事件時，應依主管機關及行政院國家資通安全會報國家資通安全應變中心之規定進行通報，並進行緊急應變處置，通報流程如附件一。

十六、 本館如遇資通安全事件危及人員生命，或設備遭到破壞等涉及民、刑事案件時，應即時通報檢警單位處理。

十七、 資通安全事件緊急應變措施

（一）內部危安事件：發現或疑似遭人為惡意破壞毀損、作業不慎等危安事件時，應迅速查明事件影響狀況、受損程度等，啟用備分資料、程式或啟動備援計畫相關措施，期儘速回復正常運作。

（二）駭客攻擊事件：

1. 遭受駭客攻擊或非法入侵時，應立即隔離受入侵系統，及拒絕入侵者任何存取動作，並迅速啟動備援系統或程序。
2. 正式紀錄入侵情形、被駭統計分析及損失評估等資料，以供防護與預警之參考。
3. 全面檢討網路安全措施、修補資安漏洞或修正防火牆之設定等具體改善補救措施，以防止類似入侵或攻擊情事再度發生。

（三）天然災害或重大突發事件：

1. 如遇颱風、水災、地震等天然災害或火災、爆炸、核子事故、重大建築災害等重大意外事件，應迅速攜帶重要資料

及程式等離開現場，或建置異地備援系統，以利爾後系統重置復原。

2. 如遇資通訊網路系統骨幹中斷事件，應立即查明障礙點、影響區間及範圍，啟動應變機制，緊急調撥備援系統或替代路由，實施流量控管，執行搶修作業。

附件一：資通安全事件通報流程