國立臺灣藝術大學資訊安全管理要點

95 年 02 月 14 日　94 學年度 第 11 次行政會議通過
97 年 09 月 09 日　97 學年度 第 2 次行政會議修正通過
108 年 11 月 19 日 108 學年度 第 4 次行政會議修正通過
111 年 08 月 16 日 111 學年度 第 1 次行政會議修正通過

一、目的

依據「行政院及所屬各機關資訊安全管理要點」，為強化本校資訊安全管理，建立安全及可信賴之電子化系統，確保資料、系統、設備及網路之安全，特訂定本要點。

二、組織及權責

本校有關資訊安全管理事務依下列分工原則：

（一）資訊安全政策之研議、資訊安全責任之分配、資訊資產保護事項之監督、資訊安全事件之檢討與其他資訊安全相關事項之審核，由「資訊發展暨資訊安全委員會」統籌與協調。

「資訊發展暨資訊安全委員會」由副校長、主任秘書、教務長、學務長、總務長、研發長、各學院院長、國際處處長、圖書館館長、有章博物館館長、藝文中心主任、推教中心主任、文創處處長、體育室主任、人事室主任、主計室主任、電算中心主任共同組成，由副校長擔任召集人。

（二）各項電腦軟硬體設備、應用系統、網路通訊之安全計畫及技術規範之研議、建置及評估、資訊安全教育訓練及宣導等事項，由電子計算機中心(以下簡稱本中心)負責辦理。

（三）資料及資訊系統之安全需求研議、使用管理及維護等事項，由使用單位或業務承辦單位負責辦理。

（四）資訊安全之稽核作業，由資安內部稽核小組研擬資安稽核計畫，經「資訊發展暨資訊安全委員會」審議通過後，陳請校長核定後實施。

（五）各單位應視資訊安全與個人資料保護需要，指定適當人員負責辦理相關事宜。

本中心對所有行政與學術單位，得定期與不定期進行資訊安全稽核。

三、人員管理

（一）各單位對資訊相關職務及工作，應進行安全評估，並於人員進用、工作及任務指派時，審慎評估人員之適任性，並進行必要之考核；各單位對可存取機密性或敏感性資訊或系統之人員，及因工作需要須配賦系統存取特別權限之人員，應加強評估及考核，並簽定保密協定。

（二）各單位負責重要資訊系統之管理、維護、設計及操作之人員，應妥適分工、分散權責，並視需要建立制衡機制，實施人員輪調，建立人力備援制度。

（三）本中心資通安全及資訊人員每年至少二名人員各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；一般使用者及主管每人每年接受三小時以上之一般資通安全教育訓練，提升資訊安全管理能力。

（四）資訊作業相關人員離職時，應取消其進出識別證件，並落實電腦軟硬體及相關文件之移交工作　。

（五）各單位業務主管應負責督導所屬員工之資訊作業安全，防範不法及不當行為。

四、資訊設備安全管理

（一）各單位辦理資訊業務委外作業時，應於事前研提資訊安全需求，明訂廠商及相關外部人員之資訊安全責任及保密規定，並列入契約中，要求廠商遵守及定期考核，並派員監督。

（二）核心資訊設備作業系統變更時，應詳實建立記錄，以備查考。

（三）各單位應依相關法規或契約規定，複製及使用軟體；嚴禁使用非法軟體。

（四）各單位應採行必要之事前預防及保護措施，偵測及防制電腦病毒及其他惡意軟體，確保系統正常運作。

（五）網路攝影機、網路印表機、門禁系統、無線 AP 等物聯網相關設備，需更改預設帳密，加強密碼強度，適當進行權限管理並定期進行作業系統安全性更新，以免受惡意軟體攻擊或資料外洩。

（六）各單位應依主管機關要求，上架至 Apple App Store、Google Play、Microsoft Store 或屬性相似網站之 App，需事先通過資安檢測。

（七）使用本校電腦設備，應遵守**「個人電腦及網路使用注意事項」**。

五、網路安全管理

（一）各單位利用網路公佈及流通資訊時，應評估資料安全等級，機密、敏感性或未經當事人同意之個人隱私資料及文件，不得上網公佈。網站存有個人資料及檔案者，應加強安全保護措施，防止個人隱私資料遭不當或不法之竊取使用。

（二）本校非屬機密性或敏感性之資料及文件，得以電子郵件或其他電子方式傳送。因單位業務性質特殊，須利用電子郵件或其他電子方式傳送機密性或敏感性之資料及文件時，須採用經權責主管機關認可之加密或電子簽章等安全技術處理。

（三）各單位對外服務網站應導入安全傳輸通訊協定（HTTPS），本校定期進行資訊安全弱點掃描、應用程式防火牆(如 WAF、F5 等)資安相關措施，如發現需改善之系統漏洞，應配合改正。

（四）各單位採購資訊軟硬體設施，應依國家標準或權責主管機關訂定之政府資訊安全規範，研提資訊安全需求，並列入採購規格。

六、系統存取控制

（一）各單位對電腦資料庫及檔案應建立分級（機密及安全等級）管理制度。

（二）各項正式作業之電腦系統操作及資料處理，由各權責單位指定專人負責建檔、核對、更新、審查及維護電腦資料之正確性。資訊系統發展人員非經核准不得操作使用或更改已正式作業之系統檔案。

（三）電腦資料庫及檔案，應按不同業務範圍及使用權限，分別設定目錄、識別保護碼；重要或具機密性資料在建檔或提供使用時，應加設通行密碼、使用權限碼，以確保資料安全，且通行密碼應定期更新。

（四）各單位離職、休職、調職人員，除本校配發予個人使用之電子郵件帳號得於規定期限

內，保留使用權限外，應立即取消使用單位內各項資源之所有權限，並列入人員離職、休職、調職之必要手續；人員職務調整及調動，應依系統存取授權規定，限期調整其權限。

（五）各單位開放外界連線作業，應事前簽訂契約或協定，明定其應遵守之資訊安全規定、標準、程序及應負之責任，加強安全控管。

（六）各單位之重要資料及系統委外廠商處理者，不論在機關內外執行，均應採取適當及足夠之安全管制措施，防止資料被竊取、竄改、販售、洩漏及不當備份等情形發生。

（七）各單位定期檢視使用公有雲之必要性，儘量避免存放機敏資料，造成資料外洩的風險，並謹慎管理雲端檔案存取權限，不任意分享檔案連結或與任何他人共用之設定。

七、系統發展及維護安全管理

（一）各單位自行開發或委外發展之系統，應在系統之初始階段即將資訊安全與個人資料保護需求納入考量；系統之維護、更新、上線執行及版本異動等作業，應予安全管制，避免不當軟體及電腦病毒危害系統安全。

（二）對廠商之軟硬體系統建置及維護人員，應規範及限制其可接觸之系統與資料範圍，並嚴禁核發長期性之系統辨識碼及通行密碼；基於實際作業需要，得核發短期性及臨時性之系統辨識與通行密碼供廠商使用，但使用完畢後應立即取消其使用權限。

（三）委託廠商建置及維護重要軟硬體設施時，應在本校相關人員監督及陪同下始得為之。

（四）各單位自行委外開發資訊系統，應遵守本校**「資訊系統委外開發注意事項」**。

八、資訊資產安全管理

（一）各單位對於儲存各項機密資料或程式軟體之磁片、磁碟、磁帶、光碟片及報表等媒體，應設專人管理並定期備份，防止資料洩漏或損毀。

（二）對於需要長期保留或重要檔案之備份資料，應存放於防火、防潮、防磁之儲藏設備中。

（三）各單位應依相關法規，訂定及區分資料安全等級，並依不同安全等級，採取適當及必要之資訊安全措施。

九、實體及環境安全管理

（一）各單位對於電腦設備之裝置地點，應考量使用及管理上之安全，並應指定專人負責管理，非經奉准之人員，不得隨意操作設備。管理或使用人員應詳細記載電腦設備故障、異常及維護等情形，以作為設備更新及作業安全之依據。

（二）各單位應就設備安置、周邊環境及人員進出管制等，訂定妥善之設備及環境安全管理措施。

（三）電腦設備機房或電腦教室應設置適當之滅火設備。人員下班後，應關閉門窗及不必要之電源，以確保安全。

十、業務永續運作之規劃

（一）各單位應訂定業務永續運作計畫，評估各種人為及天然災害對單位正常業務運作之影響，訂定緊急應變與回復作業程序及相關人員之權責，並定期演練及調整更新計畫。

（二）各單位應建立資訊安全事件緊急處理機制，發生資訊安全事件時，應依規定之處理程序，立即向該單位權責人員通報，採取適當反應措施；若情節重大者，並應聯繫檢警調機關協助偵查。

十一、　附則

本要點經行政會議通過，陳請校長核定後實施，修正時亦同。

國立臺灣藝術大學 個人電腦及網路使用注意事項

1. 禁止使用未經授權之電腦軟體。
2. 請勿任意拆卸或加裝其他電腦設備、網路設備(如集線器、無線網路發射器等)。
3. 使用外來檔案，應先掃毒，請勿任意移除或關閉防毒軟體。
4. 安裝學校正式授權防毒軟體，並定期更新病毒碼。
5. 應配合進行軟體更新，修補漏洞，保持更新至最新狀態，勿自行關閉系統自動更新程式。
6. 請勿使用通訊軟體傳輸重要機敏資料檔案。
7. 請儘量避免使用電子郵件傳輸個人機敏資料檔案，若傳輸個人機敏檔案，請先加密處理。
8. 電子郵件軟體應關閉收信預覽功能，請勿任意開啟不明來源的電子郵件、不連結及登入未經確認的網站、不下載非法軟體及檔案，以避免社交工程攻擊。
9. 電腦應使用螢幕保護程式，設定螢幕保護密碼，並將螢幕保護啟動時間設定為 10 分鐘以內。
10. 密碼須經常更換，長度應至少 6-10 碼。
11. 請勿將個人密碼張貼於個人電腦、螢幕或其它容易洩漏之場所。
12. 請勿開啟網路芳鄰分享目錄與檔案，並停用 Guest 帳號。
13. Microsoft Office 軟體(包括 Word、Excel、Powerpoint 等)應將巨集安全性設定為高級或更高，執行特殊程式如須降低安全性，請通知本中心進行安全檢查及管理。
14. 禁止使用點對點互連(P2P)軟體及相關工具下載、提供分享檔案或任何有危害本校網路、設備及造成網路壅塞佔用頻寬等軟體。
15. 電腦內重要資料文件應定期備份，避免資料損毀。
16. 機密性敏感性檔案資料應進行實體隔離(與外部網路隔絕)。

國立臺灣藝術大學 資訊系統委外開發注意事項

1. 業務單位應根據廠商之專業能力、技術經驗及財務能力，慎選優良廠商。
2. 審慎規劃保固期滿後系統之維護與管理，並訂定合適之維護計畫，包含人力及經費配置。
3. 資訊系統委外開發合約中，須訂定保固期間、維護方式及教育訓練計畫、資訊安全與個資保護要求，並制定違約罰則。
4. 應妥善規劃系統委外開發計畫中各項軟體、硬體、網路設備及執行作業之資訊安全管理。
5. 要求承包廠商參與開發之相關工作人員，均須簽訂保密切結書。承包廠商處理本校委託事務，須遵守「資通安全管理法」、「個人資料保護法」規定。業務單位應視資料之重要性，訂定廠商違反規定時之罰則及賠償責任。
6. 承包廠商如有違反個人資料保護相關法令而致個人資料被竊取、洩漏、竄改、毀損、滅失或其他侵害之情事，應立即通知本校，並說明違反事項及採行之補救措施。
7. 承包廠商所開發或維護之系統，於合約有效期間，若發現系統有安全漏洞，應無償配合修改，修改方式及交付時間須經本校同意。
8. 驗收完畢後，承包廠商須歸還開發期間自本校取得之所有個人資料，並無條件銷毀所有型式拷貝版本，例如書面資料及電子檔案。
9. 承包廠商負責相關系統之開發人員或設備維護人員離職時，應儘速通知本校權責單位，並停止其相關作業權限，及繳回所借用之軟硬體設備。
10. 承包廠商提供之軟體，均須為合法軟體，並不得違反智慧財產權之規定。承包廠商所交付之標的物如侵害第三人合法權益時，應由承包廠商承擔一切法律責任及費用。