國立臺北藝術大學資訊安全管理要點

Taipei National University of the Arts Information Security Management Main Points

97 年 5 月 20 日 96 學年度第 2 學期第 2 次行政會議審議通過
Passed on May 20th, 2008, 96th Term, Second semester, 2nd Executive Council Approval Meeting
100 年 11 月 22 日 100 學年度第 1 學期第 2 次行政會議審議通過
Passed on November 22, 2011, 100th Term, First Semester, 2nd Executive Council Approval Meeting
104 年 5 月 26 日 103 學年度第 2 學期第 2 次行政會議審議通過
Passed on May 26, 2015, 103th Term, Second Semester, 2nd Executive Council Approval Meeting

壹、目的

I. Purpose

國立臺北藝術大學(以下簡稱本校)為確保本校單位各項資訊蒐集、處理、傳送、儲存及流通之安全，並保障本校教職員工生之權益，特依「行政院及所屬各機關資訊安全管理要點」，訂定「國立臺北藝術大學資訊安全管理要點」(以下簡稱本要點)。

In order to ensure that each school department collects, processes, transmit, and stores information, as well as distributes safety, also to protect the interests of the students and staff of this school, Taipei National University of the Arts (herein referred to as "School"), under the "Executive Council and Subordinate Agencies Information Security Management Points", hereby set the "Taipei National University of the Arts Information Security Management Main Points" (herein referred to as "Points").

貳、通則

II. General

一、本要點應以書面、電子或其他方式告知本校全體教職員工生、連線作業之公私機構及協力廠商共同遵行。

A. These points should be informed to the school's faculty and students in writing, electronically or otherwise, to make the connection. Connections with public or private institutions and supporting vendors should also comply.

二、資訊安全應每年定期或不定期進行稽核。

B. Information security should be audited regularly or irregularly on an annual basis.

參、權責分工

III. Division of Responsibilities

為確保本校資訊安全控管分設「資訊安全推行小組」、「資訊安全管理委員會」,其權責分工如下:

To ensure the School's information security control, establish "Information Security Implementation Team" and "Information Security Management Committee". Division of Responsibilities are as follows:

一、資訊安全推行小組

A. Information Security Implementation Team

(一)負責統籌、協調、研議本校各項資訊安全之政策、計畫及資源調度,另配合業務推動,設置資訊安全長一人,由副校長兼任。

1. Responsible for coordination, negotiations and deliberation of the school's information security policies, plans and resources. Also assist with deployment of sales by establishing Information Security Director, a role to be served by the vice president.

(二)屬常態性任務編組,成員由保護智慧財產權宣導及推動小組兼任,均為無給職。

2. Establish task group members with normality/normalcy. Members are to share roles from the Intellectual Property Rights Protection and Advocacy Group; the rest do not hold positions

(三)至少每一年召開一次資訊安全會議,必要時得召開臨時會議,均由資訊安全長擔任主席,資訊安全長因故不能出席會議時,由資訊安全長指定委員代理之。

3. At least once a year, hold an information security meeting, and when necessary an impromptu meeting, chaired by Information Security Director. When the director cannot attend, they must appoint a member to represent them.

(四)本校資通安全危機事件通報及相關應變作業、資訊系統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(以下簡稱電算中心)負責辦理。

4. The School's information transmission security crisis response operations and related communications, deliberation, establishment and assessment of the information system security planning and technical specification, and information security education training and advocacy and other matters., should be represented by a member as appointed by the Director

of Information Security.

(五)各項資料之安全需求、使用管理及保護等事項,由業務承辦單位或人員負責辦理。

5. Each item's information security requirements, usage management and protection of data, should be the responsibility of the department of business contractors or their personnel.

(六)資訊機密維護及稽核使用管理事項,由電算中心會同相關單位負責辦理。

6. Maintenance of the confidentiality of information or the auditing of the usage of management issues will be the responsibility of the Center for Computing or relevant departments.

二、資訊安全管理委員會

B. Information Security Management Committee

(一)負責執行本校 ISO27001 資訊安全管理審查相關事項。召集人由本校資訊安全長擔任;電算中心主任為當然委員兼執行秘書;校園網路組、系統發展組及教學支援組之組長為當然委員,其餘委員由召集人推派本校專任助理教授以上或行政單位二級主管以上具有資訊專長者二至三人,簽請校長核准聘任。

1. Responsible for implementing the School's ISO 27001 information security management review and related matters. Organizer to be the Director of Information Security; Director of Center of Computing will be a member and security; campus network group, system development group and education support committee directors will be members, rest of the members to consist of 2 to 3 members ranked at assistant professors or administration level 2 managers or higher, with a background in information security. Offer and contract to be made by the Principal.

(二)每年召開一次管理審查會議,必要時得召開臨時會議,以確保資訊安全管理系統之持續適用性、充分性及有效性。

2. Management Review meeting to be held annually, when necessary call an interim meeting, to ensure the consistent applicability, suitability and efficacy of the information security management systems.

(三)本委員會下設資訊安全工作小組、緊急處理組、資訊安全稽核小組,其職責分工於本校電算中心「資訊安全組織章程」另訂之。

3. Such committee to establish the Security Workforce, Emergency Management Group, Information Security Auditing Group. Their respective responsibilities to be created by the Computing Center's "Information Security Organization Constitution".

肆、人員管理

IV. Personnel Management

一、本校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、任務指派及工作時,審慎評估人員之適任性,並進行必要之考核。

A. When each department from our school works under Information related duties and tasks, a safety assessment should be conducted. For personnel allocation and assignment of responsibilities and related tasks, the greater care and consideration should be given to suitability of the personnel for the task.

二、電算中心應針對管理、業務及資訊等不同工作類別之需求,定期辦理資訊安全教育訓練及宣導,建立資訊安全認知,提升各單位資訊安全水準。

B. The Computing Center should have different demands for different categories of jobs such as management, sales and information. Information security education training and promotions should be done on a regular basis, to establish information security awareness and raise each department's standard for information security.

三、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。

C. In the event of turnover of information operations personnel, all their identification documents should be canceled, and all implementations of computer hardware and software and related documents be transferred over.

四、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。

D. Each department's manager is responsible for overseeing their employee's IT security, to prevent illegal and inappropriate behavior.

伍、電腦系統安全管理

V. Computer Systems Security Management

一、各單位辦理資訊業務委外作業,應於事前研提資訊安全需求,明定廠商之資訊安全責任及保密規定,並列入契約,要求廠商遵守並定期考核。

A. In the case that IT work is outsourced, each department should provide in advance their information security requirements. The vendors' information security responsibilities and confidentiality provisions should be stipulated in the contracts and manufacturers should also be required to comply with and accept regular assessment.

二、各單位自行開發或委外發展系統,應在系統生命週期之初始階段,將資訊安全需求納入考量;系統之維護、更新、上線執行及版本異動作業,應予安全管制,避免不當軟體、後門及電腦病毒等危害系統安全。

B. All systems developed by the departments or outsourced, should take into account security requirements at the initial stages of the system life cycle. The maintenance, update, online transactions and version error alerts of the system should include security controls to avoid improper software, backdoor software and virus threats to the system security.

三、電腦系統作業變更時,應詳實建立記錄,以備查考。

C. When the IT system is updated, a detailed log should be established for future reference.

四、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。

D. Each department should abide by regulations or contractual provisions in the copy and use of software. Use of illegal software is strictly forbidden.

五、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。

E. Each department should adopt necessary measures to prevent, protect and detect virus and malware, to ensure the regular operations of the system.

陸、網路安全管理

VI. Web Security Management

一、各單位利用網際網路及全球資訊網公布及流通資訊,應實施資料安全等級評估,機密性、敏感性及未經當事人同意之個人隱私資料及文件,不得上網公布。

A. Each department should use the internet and world wide web to publish and circulate information. Data security ratings should be established. Confidential, sensitive and information that has not received the consent of all parties should not be published online.

二、單位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違法或不當之竊取使用。

B. Department websites that contain personal information and files, should have additional security protection measures to prevent individual private information to be illegally or improperly stolen or used.

三、本校電子郵件使用時,機密性資料及文件,不得以電子郵件或其他電子方式傳送。機密性資料以外之敏感性資料及文件,如有電子傳送之需要,本校應視需要以適當之加密或電子簽章等安全技術處理。

C. When using the School's email system, sensitive or confidential information or documents should not be transmitted via email or other electronic methods. Should there be a need to transmit electronically nonconfidential sensitive information or documents, the School must apply additional encryption or electronic signatures types of security measures.

柒、系統存取控制

VII. Access Control System

一、各單位應訂定系統存取政策及授權規定,並以書面、電子或其他方式告知教職員工生及使用者之相關權限及責任。

A. Each department must set their system access control policy and authorization requirements. Use written, electronic or otherwise methods to inform staff, students and other users of the authority and responsibilities related to access control systems.

二、各電腦系統應建立系統使用者註冊管理制度,建立使用人員名冊。

B. Each computer system should establish system user registration management system, as well as a user listing.

三、本校各單位離(休)職人員,應立即取消使用校內各項資訊資源之所有權限,並列入人員離(休)職之必要手續。各單位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。

C. Any personnel that have quit or been fired, should cancel their permissions to

campus information resources. This should be included as a necessary step in the personnel exit procedure. In the event of position adjustment or movement, system access authorization rules dictate that their permissions should be adjusted in due time.

四、各單位開放外界連線作業,應事前申請，明定其應遵守之資訊安全規定、標準、程序及應負之責任。

D. Any department that opens up external connectivity must apply in advance. It is stipulated that they must comply with the information security rules, standards, procedures and bear responsibility for these rules.

五、各單位對系統服務廠商以遠端登入方式進行系統維護者,應加強安全控管,並建立人員名冊,並要求遵循相關安全保密責任。

E. For systems maintenance vendors that use remote login to maintain the system, each department should boost security control measures, establish a personnel listing and request that they are subject to relevant security and confidentiality duties.

六、各單位資料需委外建檔者,不論在單位內外執行,均應採取適當及必要之安全管制措施,防止資料被竊取、竄改、販售、洩漏及不當備份等情形發生。

F. Any department that requires information to be outsourced to be archived, regardless of whether this is done internally or externally, should apply appropriate and necessary security control measures to prevent that the information be stolen, tampered with, sold, leaked or backed up improperly.

捌、業務永續運作之規劃

VIII. Planning of Business Continuity Operations

一、電算中心訂定緊急應變與回復作業程序及相關人員之權責,定期演練及調整更新計畫,並且安排教育訓練提升全校資安意識。

A. The computing center establishes emergency response and recovery procedures as well as relevant personnel’s responsibilities and permissions, regular update and adjustment of the plan and sets up education training to raise the information security awareness of the whole school.

二、各單位在發生資訊安全事件時,應依本校相關資安法規規定之處理程序,立即向該單位權責人員、電算中心及資訊安全長通報,並於採取反應措施後,由電算中心聯繫檢警調機關偵查。

B. In the event of an information security incident, each department should handle the incident according to the provisions relating to information security rules, immediately notify the department authorities, the compute center and other information security directors, and after taking action, allow the computing center to notify police to close the investigation.

玖、其他安全措施

IX. Other Security Measures

一、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。

A. On the subject of equipment placement and access to surrounding environment and personnel access control, each department should set proper safety equipment and environmental management measures.

二、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。

B. For computer equipment setup locations, each department must consider the security in usage and management. They must designate a personal responsible for management, and non-approved to personnel must not be able to free to use the equipment. Management or other personnel must detail record any computer equipment failure, abnormal situations and maintenance instances, to keep a record of equipment upgrade and task security.

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。

C. Computer equipment rooms or computer classrooms should install appropriate fire retardant equipment. During off hours, all windows should be closed and nonessential power be cut, to ensure safety.

拾、附則

X. Supplementary

本要點經行政會議審議通過,陳請校長核定後公布實施,修正時亦同。

These main points will not be publically in place until approved by the executive council and by our principal; same for amendments.