國立臺灣師範大學資訊安全管理要點

民國 100 年 9 月 30 日資訊安全管理委員會通過

壹、目的

一、國立臺灣師範大學(以下簡稱本校)為強化資訊安全管理，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，保障本校教職員工生之權益，特依據「個人資料保護法」、「行政院及所屬各機關資訊安全管理要點」訂定本要點。

貳、通則

二、本要點規範對象為本校各單位及全體教職員工生。

三、各單位應針對所管理之各項資訊系統，採行適當的資訊安全保護措施，確保各單位資料蒐集、處理、傳送、儲存及流通之安全。

四、本要點實施時如有必要，各單位應訂定說明文件，如管理規範、作業要點、注意事項等文件。

參、組織及權責

五、資訊安全政策及技術規範之研擬、建置與評估等事項，由資訊中心負責辦理。

六、資訊系統之安全需求研議、使用管理及維護等事項，由業務承辦單位負責辦理。

七、資訊安全教育訓練及宣導事宜，由資訊中心負責辦理。

八、資訊安全之稽核作業，由資訊中心負責辦理。

九、本校針對所有行政及學術單位，得定期或不定期進行資訊安全稽核。

肆、資訊資產管理

十、各單位資訊資產應設專人管理維護。

十一、各單位儲存機密資料或程式之磁片、磁帶、光碟片等儲存媒體，應設專人管理並妥善保管，防止資料洩漏或損毀。

十二、儲存個人資料檔案之電腦或相關設備，如需報廢或移轉他用時，應確實刪除該設備所儲存之個人資料檔案。

伍、人員管理與資訊安全教育訓練

十三、各單位接觸機敏資料人員，應簽署「保密切結書」，並克盡保密之責。

十四、各單位應指派資訊安全承辦人員，並定期接受資訊安全教育訓練。

十五、各單位重要系統之管理、維護、設計及操作，應建立人力備援機制。

十六、各單位人員離職時，應終止相關資源之存取權限，並確實做好電腦軟硬體及相關文件之移交工作。

十七、各單位主管應負責督導所屬教職員工之資訊作業安全，防範不法及不當行為。

陸、實體及環境安全管理

十八、各單位於新增硬體設備時，應先評估電力負載，以避免電力超載而導致重要服務中斷。

十九、電腦機房或電腦教室應設置適當之滅火設備。

二十、未經授權不得將設備、軟體、儲存資訊之媒體或機敏文件攜出電腦機房或辦公環境。若有需要應經主管人員核准，始得進行。

二十一、儲存個人資料之資訊設備應置放於安全場所，以避免有心人士或非授權人員竊取。

柒、通訊與作業管理

二十二、足以影響單位業務營運管理的資訊系統，避免只由單獨一人知悉。如因人力資源限制，無法區隔責任，則應加強監督與稽核等措施。

二十三、各單位伺服主機及網路設備應指定負責人，負責該主機之正常運作，主機或網路設備負責人無法進行管理時，應由職務代理人負責。

二十四、各單位於網路架構變更、建築物修繕及新建大樓時，應於規畫施工前通知資訊中心。

二十五、資訊系統應設定防火牆，只開放必要之網路服務與通訊協定。

二十六、機敏資料或文件，欲利用電子郵件或其他電子方式傳送時，應以適當的加密技術處理。

二十七、對於個人機敏資料之調閱，應有申請及核准程序，並使用可靠且具備保密機制之傳遞方式。

二十八、機敏業務資料或文件不得存放於對外開放之資訊系統中，若因特殊業務功能之需求，應採取資料加密之安全管控機制。

二十九、對校外開放的資訊系統，如有涉及機敏資訊，其傳輸過程應考量以加密方式處理，並妥善保管資料，以防止被竊取或移作他途之用，導致侵犯個人隱私。

三十、網站或紙本公告之資訊，應經由權責主管之審查與核定，確認未含有機敏資訊及違反智慧財產權或法令所明訂之禁止資訊。

三十一、應避免允許維護人員或系統服務廠商以各種遠端登入方式進行牽涉個人資料的資訊系統維護作業；若需要使用遠端登入方式進行維護，應視需要使用加密通道等各種安全控管技術。

三十二、系統負責人應定期檢視修補系統漏洞及更新防毒軟體病毒碼，以維持系統正常運作。

三十三、資訊系統之設定檔、網頁資料及資料庫資料，均應由各系統負責人員執行定期系統備份排程或手動備份。

捌、系統控制管理

三十四、人員的職務應考量適當的權責區隔，基於業務上之需要，各項工作應訂定工作職務代理人，盡可能符合權責區隔之原則。

三十五、資訊資產之存取應與本身業務相關之範圍為主，任何人未經授權不得存取業務範圍外之資訊資產。

三十六、資訊系統應設置密碼保護，並符合安全密碼的控管要求。

三十七、廠商之維護人員，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密碼，使用完畢後應立即取消其使用權限。

三十八、系統管理者應隨時注意及觀察分析系統之儲存容量，以避免容量不足而導致服務停止或資料毀損。

玖、系統開發與維護

三十九、當發展新資訊系統，或現有系統功能之強化，於系統規劃需求分析階段，應將安全需求要項納入系統功能。

四十、自行開發或委外處理個人資料檔案之資訊系統，應避免以真實個人資料進行測試；如需使用應將可辨識之個人資料修改為無法辨識之模糊資訊，並於完成測試作業後迅速移除。

四十一、網頁應用程式編碼時，應避免撰寫不安全源碼，並於上線前完成相關安全性檢測及網頁弱點掃描。

四十二、設計各種例外狀況處理機制時，應避免直接顯示原始完整錯誤資訊。

四十三、重要系統程式測試應有測試紀錄。若程式內容有重大異動應重新測試，並更新測試紀錄。

拾、委外管理

四十四、承辦單位採購人員應要求委外廠商提供所交付設備之相關文件與技術支援服務，如必要亦應提供教育訓練課程。

四十五、系統若委由外部廠商開發，承辦單位採購人員應要求廠商提供完整之系統架構及規格文件。

四十六、承辦單位採購人員應要求委外廠商及人員遵守「個人資料保護法」及本校相關規定，並簽訂「委外廠商保密切結書」及「委外廠商人員保密切結書」。

四十七、承辦單位採購人員應要求委外廠商針對所交付之系統進行技術安全稽核，以確保系統之安全，並提供相關安全稽核報告。

四十八、委外開發或維護之系統，於合約有效期間，若發現系統有安全漏洞，承辦單位採購人員應要求委外廠商修改，惟修改方式及交付時間須經承辦單位同意。

四十九、個人資料檔案若委外建檔，應於委外合約中載明所處理之個人資料保密義務、資訊安全相關責任及違反之罰則。

拾壹、資訊安全事件及業務永續運作管理

五十、若發生資訊安全事件，各單位應配合資訊中心進行調查及復原作業。

五十一、重大資訊安全事件應保留事件發生之線索及相關佐證紀錄至少半年以上，以作為檢調機關調查之證據。

五十二、資訊安全事件確認處理完成後，相關單位應檢討現行管控措施之完整性，並適當修訂相關作業規範或建置及調整控制措施，以加強系統安全防護。

拾貳、附則

五十三、本要點經資訊安全委員會審議通過，簽請校長核定後實施，修正時亦同。