臺北市立大學資訊安全作業要點

95年9月25日資訊推動委員會第二次會議通過

95年11月30日核定後實施

104年10月13日資訊推動委員會會議修正通過

111年11月25日資訊推動委員會會議修正通過

**壹、目的**

一、臺北市立大學(以下簡稱本大學)為確保本大學各單位各項資訊蒐集、處理、傳送、儲存及流通之安全，並保障本大學教職員工生之權益，特依「個人資料保護法」、「資通安全管理法」訂定本要點。

**貳、通則**

二、本要點應以書面、電子或其他方式告知本大學全體教職員工生、連線作

業之公私機構及提供資訊服務之廠商共同遵行。

三、本要點應至少每年評估一次，以順應技術、業務等相關環境之趨勢，確

保實務作業之有效性。

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、作業程

序、資訊安全控管文件等。

五、資訊安全應定期或不定期進行稽核。

**參、權責分工**

六、於實施本要點時，其權責分工如下：

(一)為統籌、協調、研議本大學各項資訊安全之政策、計畫及資源調度，

特成立「資訊安全推行小組」。「資訊安全推行小組」由教務長、學生事務長、總務長三長、主任秘書、人事、會計室主任、計算機與網路中心主任共同組成；由教務長擔任召集人，計算機與網路中心為業務承辦單位。

(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、建置及評估等，由所屬資訊或管理單位或人員負責辦理。

(三)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。

(四)資訊機密維護及稽核使用管理事項，由秘書室會同相關單位負責辦

理。

**肆、人員管理**

七、本大學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。

八、各單位對可存取機密性與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。

 九、各單位應針對管理、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，提升單位資訊安全水準。

 十、單位應加強資訊安全人力之培訓，提升資訊安全管理能力。

十一、各單位資訊安全人力或經驗如有不足，得洽請學者專家或專業機關(構)

提供顧問諮詢服務。

十二、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。

十三、各相關單位主管應負責所屬員工之資訊安全作業，防範不法及不當行

為。

**伍、電腦系統安全管理**

十四、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。

十五、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，即將資

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、暗門及電腦病毒等危害系統安全。

十六、各單位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。各單位基於

實際作業需要，得核發短期性及臨時性之系統辨識及通行密碼供廠商使

用。但使用完畢後應立即取消其使用權限。各單位委託廠商建置及維護重

要軟硬體設施時，應在單位相關人員監督及陪同下始得為之。

十七、各單位對系統變更作業，應建立控管制度，並建立紀錄，以備查考。

十八、各單位使用軟體之權利及義務應依著作權法及有關議定之合約辦理。各單

位應依據「政府所屬各級行政機關電腦軟體管理作業要點」，建立軟體使

用管理制度。

十九、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。

**陸、網路安全管理**

二十、各單位利用公眾網路傳送資訊或進行交易處理，應遵守「台灣學術網路使

用規範」；並應評估可能之安全風險，確定資料傳輸具完整性、機密性、

身分鑑別及不可否認性等安全需求。

二十一、各單位應針對資料傳輸、撥接線路、網路線路與設備、對外連接介面及

路由器等事項，研擬妥適安全控管措施。

二十二、各單位與外界網路連接之網點，必要時得以防火牆或其他安全設施，控

管外界與單位內部網路之資料傳輸及資源存取。

二十三、各單位開放外界連線作業之資訊系統，必要時得視資料及系統之重要性

及價值，採用資料加密、身分鑑別、電子簽章、防火牆及安全漏洞偵測

等不同安全等級之技術或措施，防止資料及系統被侵入、破壞、竄改、

刪除及未經授權之存取。

二十四、各單位開放外界連線作業之資訊系統，必要時得以代理伺服器等方式提

供外界存取資料，避免外界直接進入資訊系統或資料厙存取資料。

二十五、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。

二十六、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。

二十七、本大學應訂定電子郵件使用規定，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，本大學應視需要以適當之加密或電子簽章等安全技術處

理。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資

料及文件者，得採用權責主管機關認可之加密或電子簽章等安全技術處

理。

二十八、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。各單位發展及應

用加密技術，應採用權責主管機關認可之密碼模組產品。各單位採購外

國產製之密碼模組產品，應請廠商提出輸出許可或相關授權文件，確保

密碼模組之安全性，並避免採購金鑰代管或金鑰回復功能之產品。

**柒、系統存取控制**

二十九、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。

三十、各單位應依資訊安全政策，賦予各級人員必要之系統存取權限；賦予之系

統存取權限，應以執行法定任務所必要者為限。對被賦予系統管理最高權

限之人員及掌理重要技術及作業控制之特定人員，應經審慎之授權評估。

三十一、本大學各單位離(休)職人員，學生應立即取消使用校內各項資訊資源之

所有權限，老師則保留各項資訊資源之權限。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。

三十二、各單位應建立教職員工生及使用者註冊管理制度，加強通行密碼管理，

並要求定期更新；其通行密碼之更新週期，由各單位視作業系統及安全

管理需求決定，最長以不超過六個月為原則。對單位內外擁有系統存取

特別權限之人員，應建立使用人員名冊，加強安全控管，並縮短密碼更

新週期。

三十三、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。

三十四、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，課其相關安全保密責任。

三十五、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。

三十六、各單位應確立系統稽核項目，建立資訊安全稽核制度，定期或不定期進

行資訊安全稽核作業；系統中之稽核紀錄檔案，應禁止任意刪除及修

改。

**捌、業務永續運作之規劃**

三十七、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。

三十八、各單位應建立資訊安全事件緊急處理機制，在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，於採取反應措施後，

並由本大學聯繫檢警調機關偵查。

**玖、其他安全措施**

三十九、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。

四十、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。

**拾、附則**

四十一、本要點經資訊推動委員會通過，陳請校長核定後公布施行。