國立彰化師範大學資訊安全管理要點

94 年 9 月 14 日行政會議通過
105 年 10 月 05 日行政會議討論修正通過

一、目的

為強化本校各單位暨所屬單位資訊安全管理，確保資料、系統、設備及網路安全，保障教職員工生權益，依據行政院所屬各機關資訊安全管理要點及相關規定，訂定國立彰化師範大學資訊安全管理要點（以下簡稱本要點）。

二、通則

本要點適用對象為本校各單位（含宿舍）暨附屬單位。

三、資訊安全政策

（一）資訊安全之範圍分列如下：

1.管理制度，2.作業流程，3.人員，4.軟體，5.應用系統，6.電腦作業系統，7.硬體，8.通訊設備，9.資料、文件、媒體的儲存及 10.實體設施等。

（二）資訊安全管理之範圍分列如下：

1. 資訊安全組織及權責。
2. 資產分類與控管。
3. 人員安全管理及教育訓練。
4. 電腦系統實體及環境安全管理。
5. 網路、通訊與操作管理。
6. 系統存取控制。
7. 系統開發與維護。
8. 永續經營管理。

（三）本要點應適時評估，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）本要點應以書面、電子郵件或其他方式告知全體教職員工生、連線作業之公私機構及提供資訊服務之廠商共同遵行。

（五）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。

（六）資訊安全應定期或不定期進行稽核。

四、資訊安全組織及權責

（一）為統籌、協調、研議本校各項資訊安全之政策、計畫及資源調度，並考量實務推行效率與組織簡化，由本校各單位 IP 管理者或指定專責人員負責各單位資通安全事件通報、協助執行安全預防、危機處理及緊急應變等工作之職掌。

（二）各項電腦軟硬體設備、應用系統、網路通訊之安全計畫、緊急應變計畫及技術規範之研議、訂定、建置及評估等，由所屬資訊或管理單位負責辦理。

（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。

（五）附屬單位必須指派資訊或適當單位負責資訊安全管理，並依本校規定辦理。

（六）委外與第三方[協力廠商]依據合約內容配合，負責委外或協力部份之資訊安全運作。

五、資產分類與控管

各單位對於重要的資產(含資訊、軟體、實體等)均指定專人負責，並建置資產清冊且隨時

更新。

六、人員安全管理及教育訓練

（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，並進行必要的考核。

（二）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。

（三）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或宣導，建立員工資訊安全認知，提升單位資訊安全水準。

（四）各單位應加強資訊安全人力之培訓，提升資訊安全管理能力。

（五）各單位資訊安全人力或經驗如有不足，得洽請學者專家、專業機關（構）或本校圖書與資訊處提供顧問諮詢服務。

（六）各單位負責重要系統之管理、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。

（七）各單位主管應負責督導所屬員工之資訊安全作業，防範不法及不當行為。

七、電腦系統實體及環境安全管理

（一）設置電腦機房及重要地區之單位，對於進出人員必須由管理人員作必要之限制及監督其活動、各項安全設備必須定期檢查，並訂定電腦機房安全管理規定，員工必須施予適當的安全設備使用訓練。

（二）各單位設置有機密性工作站或伺服器者必須由專人管理。

（三）各單位應依著作權等相關法規或契約規定，複製及使用軟體，並應依據「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。

（四）各單位設備之維護必須由授權之維護人員執行，應採行必要的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）本校各單位電腦系統安全管理

1. 校內使用者端電腦系統對校外網路之存取，僅限於使用服務，禁止對外提供商業相關網路服務。
2. 伺服器應使用合法授權之軟體，並經常修補安全漏洞。
3. 資料備份：
   （1）執行必要的資料及軟體備份，以便發生災害或是儲存媒體失效時，可迅速回復正常作業。
   （2）應定期測試備份資料，以確保備份資料之可用性及時效性。

（六）各單位對於重要之攜帶型的電腦設備須有嚴謹的保護措施(如設通行碼、檔案加密、專人看管)並落實執行。

（七)具敏感性或機密性資料之單位其資訊財產攜出辦公處所,必須訂有安全之攜出管理規則。

（八）公務用電腦：

1. 應啟用螢幕保護程式，設定螢幕保護密碼，並將螢幕保護啟動時間設定為十分鐘以內。
2. 應安裝防毒軟體，定期更新病毒碼。
3. 應定期或即時(real time)掃瞄電腦系統及資料儲存媒體。
4. 在不影響系統正常運作下，應定期更新修正程式，修補系統漏洞。

5. 應遵守智慧財產權，使用合法授權軟體。

八、網路、通訊與操作管理

（一）各單位利用公眾網路傳送資訊或進行交易處理，應遵守「臺灣學術網路管理規範」；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。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）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。

（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。

（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庫存取資料。

（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。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。

（六）本校建置有郵件伺服器之單位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，本校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。

（七）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。

（八）各單位應視需求建置防火牆、防毒軟體及入侵偵防系統，重要伺服主機應單獨外掛硬體防火牆、防毒軟體及入侵偵防系統。

（九）本校圖書與資訊處應配合教育部定期檢測網路運作環境之安全漏洞、公告有關網路安全之事項、定期檢討網路安全控管事項之執行。

（十）本校圖書與資訊處應公告有關電腦作業系統及應用軟體安全之事項。

（十一）關於個人資料的蒐集、處理、利用及相關的申請登記、損害賠償、處罰等事宜應依個人資料保護法等相關法令規定辦理。

九、系統存取控制

（一）凡建置多人使用之應用系統之單位應訂定系統存取政策及授權制度，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，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。

（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與資料。

（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，且通行密碼應經常更新。

（四）各單位離職、解聘、不續聘或停聘人員，應限期內停止使用校內各項資訊資源之所有權限，並列入人員離職必辦之手續。各單位人員職務異動，應依系統存取授權規定，限期調整其權限。

（五）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。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。

（六）各單位若開放外界連線作業，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。

（七）需由系統服務廠商以遠端登入方式進行系統維護之單位，應加強安全控管，並建立人員名冊，課其相關安全保密責任。

（八）各單位資料或系統需委外建檔者，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。

（九）凡建置多人使用之應用系統之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。

十、系統開發與維護

（一）自行開發或委外發展系統之單位，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等作業，應予安全管制，避免不當軟體、暗門及電腦病毒危害系統安全。

（二）辦理資訊業務委外作業之單位，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。

（三）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。

（四）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。

（五）各單位自行開發或委外發展系統之變更作業，應建立控管制度，並建立紀錄，以備查考。

（六）各單位於系統開發與維護階段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。

（七）為避免影響系統正常運作，各單位於系統開發與維護階段應建立系統測試環境，完成系統測試後上線運作。

（八）本校校務行政系統與資料之資訊安全管理與維護，應由系統管理單位負責，其資訊安全規定如下：

1. 校務行政網路應適度與宿網、教學研究網路系統隔離，若使用網際網路必須使用合適之隔離或加密措施。
2. 所有校務行政電腦資料應具備異動紀錄，紀錄異動時間與異動者等資料。
3. 所有校務行政電腦資料必須有復原計畫，復原計畫所需時間與正確性必須符合業務所需，且每年至少確實執行一次。

十一、永續經營管理

（一）各單位應評估各種人為及天然災害對單位正常業務運作之影響，視需要訂定業務永續運作計畫、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）本校電腦、網路及校務行政等系統之業務永續運作計畫

1. 本校校務行政系統、各類伺服器(含電子郵件等)、網路系統與電腦系統中資料庫、應用程式與資料,必須備份分開存放並且提供備援運轉服務,以便當設備發生運轉問題,備援設備可以立即接手取代繼續運轉，以提供本校師生更完善的電腦網路環境，達到支援教學、研究不間斷。
2. 本校校務行政系統、主幹網路系統之永續運作計畫及緊急應變與回復作業程序之訂定、管理與維運，應由本校業務主管單位負責。

（三）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，應依處理程序，通知系統管理人員，並立即向本校資通安全通報窗口通報，於採取反應措施後，陳報本校資訊安全長，必要時向上級或國家資通安全會報通報，或由本校聯繫檢警調機關偵查。

十二、本要點經行政會議討論通過，陳請 校長核定後施行，修正時亦同。