國立中正大學資訊安全管理規範實施要點

第二四○次行政會議修正通過 (89.1.3)

壹、依據

教育部台(八八)電字第八八一一四七０九號函及「行政院所屬各機關資訊安全管理規範」。

貳、資訊安全之目的

為強化本校資訊安全管理，建立安全及可信賴之電子化機關，確保資料、系統、設備及網路安全，保障教職員工生權益，特訂定本規範。

參、通則

本要點所稱各單位，指本校所屬各處、室、院、系所、中心及圖書館。

肆、人員安全管理及教育訓練

1. 甄選及進用之人員，如其工作職責須使用處理敏感性資訊的資訊科技設施或涉及機密性及敏感性資訊者，應經適當的安全評估程序。
2. 員工使用資訊科技設施應依相關規定課予機密維護責任，並進行資訊安全教育及訓練。

伍、系統與網路之安全管理

一、電腦病毒及惡意軟體之防範

（一）、建立軟體管理政策，規定使用者應遵守軟體授權規定，禁止使用未取得授權的軟體。
（二）、電腦病毒防制軟體應定期更新。
（三）、使用防毒軟體事前掃瞄電腦系統及資料儲存媒體，偵測有無感染電腦病毒。
（四）、對來路不明及內容不確定的磁片，應在使用前詳加檢查是否感染電腦病毒。
（五）、應遵守智慧財產權相關規定。

二、個人資料之保護

（一）、應依據電腦處理個人資料保護法等相關規定，審慎處理個人資訊。
（二）、應建立個人資料控制及管理機制，並視需要指定負責個人資料保護之人員，以便協調管理人員、使用者及系統服務提供者，促使相關人員瞭解各部門應負的個人資料保護責任，以及應遵守之作業程序。

三、日常作業之安全管理

（一）、應準備足夠的備援設施，定期執行必要的資料及軟體備份及備援作業，以便發生災害或是儲存媒體失效時，可迅速回復正常作業。
（二）、系統發生作業錯誤時，應正式記錄下來，並報告權責主管人員，並採取必要的更正行動。
（三）、電腦作業環境如溫度、溼度及電源供應之品質等，應隨時監測，並採取必要的補救措施。

四、電腦媒體與資料文件之安全管理

（一）、可重複使用的資料儲存媒體，不再繼續使用時，應將儲存的內容消除。
（二）、須離辦公場所的儲存媒體，應建立書面的授權規定，並建立使用紀錄。
（三）、儲存媒體應依製造廠商提供的保存規格，存放在安全的環境。
（四）、系統文件應鎖在安全的儲櫃或其他安全場所。
（五）、委外處理的電腦文具、設備、媒體蒐集及委外處理資料，應慎選有足夠安全管理能力及經驗的機構作為委辦對象。
（六）、應保護重要的資料檔案，以防止遺失、毀壞、被偽造或竄改。
（七）、與他單位進行電子資料交換，應採行保護措施，以防止資料受損及未經授權的資料存取及竄改。

五、網路服務之管理

（一）、系統的最高使用權限，應經權責主管人員審慎評估後，交付可信賴的人員管理。
（二）、網路系統管理人員應負責製發帳號，供授權的人員使用。
（三）、提供給內部人員使用的網路服務，與開放業務有關人員從遠端登入內部網路系統的網路服務，應執行嚴謹的身分辨識作業，或使用防火牆代理伺服器(Proxy Server)進行安全控管。
（四）、離（休）職人員應依資訊安全規定及程序，取銷其存取網路之權利。
（五）、網路系統管理人員未經權責主管人員許可，不得閱覽使用者之私人檔案；但如發現有可疑的網路安全情事，網路系統管理人員得依授權規定檢查其檔案。
（六）、網路系統中各主要主機伺服器應有備援主機，以備主要作業主機無法正常運作時之用。
（七）、網路硬體設備應加裝不斷電系統，以防止不正常的斷電狀況。

六、使用者管理

（一）、使用者應遵守「臺灣學術網路使用規範」及相關規定。
（二）、被授權的網路使用者，只能在授權範圍內存取網路資源。
（三）、使用者應遵守相關安全規定，如有違反，應撤消其網路資源存取權利，並依相關法規處理。
（四）、網路使用者不得將自己的登入身份識別與登入網路的密碼交付他人使用。
（五）、應禁止網路使用者以任何方法竊取他人的登入身份與登入網路通行碼。
（六）、應禁止及防範網路使用者以任何儀器設備或軟體工具竊聽網路上的通訊。

七、主機安全防護

單位存放機密性及敏感性資料之大型主機或伺服器主機(如 Domain Name Server 等)，除作業系統既有的安全設定外，應強化身份辨識之安全機制，防止遠端撥接或遠端登入資料經由電話線路或網際網路傳送時，被偷窺或截取(如一般網路服務 HTTP、Telnet、FTP 等的登入密碼)，及防制非法使用者假冒合法使用者身分登入主機進行偷竊、破壞等情事。

八、系統與網路入侵之處理

（一）、立即拒絕入侵者任何存取動作，防止災害繼續擴大；當防護網被突破時，系統應設定拒絕任何存取；或入侵者已被嚴密監控，在不危害內部網路安全的前題下，得適度允許入侵者存取動作，以利追查入侵者。
（二）、切斷入侵者的連接。或為達到追查入侵者的目的，可考慮讓入侵者做有條件的連接，一旦入侵者危害到內部網路安全，則必須立即切斷入侵者的連接。
（三）、應全面檢討網路安全措施及修正防火牆的設定，以防禦類似的入侵與攻擊。
（四）、對入侵者的追查，除利用稽核檔案提供的資料外，得使用系統指令執行反向查詢，並連合相關單位（如網路服務公司），追蹤入侵者。
（五）、入侵者之行為若觸犯法律規定，構成犯罪事實，應立即告知檢警憲調單位，請其處理入侵者之犯罪事實調查。

九、使用者之註冊管理

（一）、在系統使用者尚未完成正式授權程序前，資訊服務提供者不得對其提供系統存取服務。
（二）、應以書面或其他方式告知使用者之系統存取權利。
（三）、要求使用者簽訂約定，使其確實瞭解系統存取的各項條件及要求。
（四）、應建立及維持系統使用者之註冊資料紀錄，以備日後查考。
（五）、使用者調整職務及離（休）職時，應儘速註銷其系統存取權利。
（六）、應定期檢查及取銷閒置不用的識別碼及帳號。

十、使用者通行碼之管理

（一）、以嚴謹的程序核發通行碼，明確規定使用者應負的責任。
（二）、個人應負責保護通行碼，維持通行碼的機密性。
（三）、當有跡象足以顯示使用者密碼可能遭破解時，應立即更改密碼。
（四）、使用者第一次登入系統時，系統應要求更改臨時性通行碼。

十一、網路存取之安全控制

（一）、網路連線作業之控制

為確保系統安全，跨單位的網路系統可限制使用者之連線作業能力。例如，以網路閘門技術依事前訂定之系統存取規定，過濾網路之傳輸作業。

（二）、網路路由控制

1. 分享式的網路系統，應建立網路路由的控制，以確保電腦連線作業及資訊流動不會影響應用系統的存取政策。
2. 網路路由的控制，應建立實際來源及終點位址之檢查機制；網路路由的控制可以硬體或軟體方式執行，並應事先評估瞭解不同方式的安全控制能力。

十二、系統與網路紀錄

進出系統與網路，應記錄下列事項：

（一）、使用者識別碼。

（二）、登入及登出系統之日期及時間。

（三）、記錄端末機的識別資料或其網路位址。

十三、設備安全管理

（一）設備安置地點之保護

1.設備應安置在適當的地點並予保護，以減少環境不安全引發的危險及未經授權存取系統的機會。

2.設備安置應遵循的原則如下：

（１）、設備應儘量安置在可減少人員不必要經常進出的工作地點。處理機密性及敏感性資料的工作站，應放置在員工可以注意及照顧的地點。

（２）、需要特別保護的設備，應考量與一般的設備區隔，安置在獨立的區域。

（３）、應檢查及評估火災、煙、水、灰塵、震動、化學效應、電力供應、電磁幅射等可能的風險。

（４）、電腦作業區應禁上抽煙及飲用食物。

（５）、在特定的作業環境下，可考慮使用鍵盤保護膜。

（６）、除了考量同一樓層地板可能導致的的危險外，也應考量鄰近建築樓層地板可能導致的危險。

（二）電源供應

1. 電腦設備之設置，應予保護，以防止斷電或其他電力不正常導致的傷害；電源供應依據製造廠商提供的規格設置。
2. 應考量安置預備電源，並考量使用不斷電系統。
3. 資訊安全事件緊急處理應變計畫應將不斷電系統失效之後的應變措施納入；不斷電系統應依據製造廠商的建議，定期進行測試。
4. 應謹慎使用電源延長線，以免電力無法負荷導致火災等安全情事。

（三）設備維護

1. 應妥善地維護設備，以確保設備的完整性及可以持續使用。
2. 設備維護的原則如下：

（１）、應依據廠商建議的維修服務期限及說明進行設備維護。

（２）、設備的維護只能由授權的維護人員執行。

（３）、應將所有的錯誤或是懷疑的錯誤予以記載。

（四）設備放置在機關外部空間之安全管理

1. 設置在單位外部支援單位業務運作的資訊設備，應同樣遵守資訊安全管理授權規定，維持與單位內部資訊設備一樣的安全水準。
2. 設置在單位外部的資訊設備安全措施原則如下：

（１）、如果未採取電腦病毒防範措施，執行單位業務所使用的個人電腦，不應在家裡使用。

（２）、外出差勤時，電腦設備及資料儲存媒體在公共場所應有人看管。

（３）、外勤使用之攜帶型電腦，易於被偷取、遺失或是遭未經授權的取用，應提供適當的存取保護措施，例如設定通行碼或是將檔案資料加密。

（４）、應隨時注意設備製造廠商提供的保護使用說明書。

（５）、各種安全風險如損害、偷竊或竊聽等，可能會因不同的安置地點而有所不同；在決定最適當的安全措施時，應該將不同地點的安全風險納入考量。

（五）設備處理之安全措施

含有儲存媒體的設備項目（例如硬碟）應在處理前詳加檢查，以確保任何機密性、敏感性的資料及有版權的軟體已經被移除。

（七）資訊設施誤用之防止

1. 單位提供的資訊設施，如有業務目的以外的使用，或是超出授權目的以外的使用需求，應經權責主管人員的核准，並課予相關人員的責任。
2. 如從監督性的資訊或是從其他方法發現資訊設施有不當使用情形，應作適當的紀律處理。
3. 應以書面或其他電子方式明確告知使用者的系統存取授權範圍。
4. 單位員工以及其他第三者，除非獲得正式的授權，任何人皆不得進行系統存取。

十四、周邊安全管理

（一）周圍環境之安全

1. 實體環境的安全保護，應以事前劃定的各項周邊設施為基礎，並以設置必要的障礙（例如：使用身分識別卡之安全門），達成安全控管的目的。
2. 每項資訊設施的實體保護程度，以及實體障礙設置的位置，應依資訊資產及服務系統的價值及安全的風險決定。
3. 實體環境的安全保護原則如下：

（１）、周圍設施的安全措施，應視擬保護的資訊資產或資訊服務系統的價值而定。

（２）、應明確界定有那些周邊設施須列為安全管制的對象。

（３）、支援資訊作業的相關設施如影印機、傳真機等，應安置在適當的地點，以降低未經授權的人員進入管制區的風險，及減少敏感性資訊遭破解及洩漏的機會。

（４）、不應對非相關的人員提供過多有關管制區的作業細節。

（５）、為防止可能的不當行動，未經授權的人員在辦公室單獨作業應予適當的管理。

（６）、機關資訊作業如有委外者，自行管理的設備應安置在特定的區域，並與資訊服務提供者管理的設備分開。

（７）、資訊支援人員或維護服務人員，只有在被要求或是被授權的情形下，才能進入管制區域，並視需要限制（例如限制存取敏感性的資料）及監督其活動。

（８）、非經授權，管制區內不得設置照像、錄音及錄影等設備。

（二）人員進出管制

1. 管制區內應有適當的進出管制保護措施，以確保只有被授權的人員始得進入。
2. 進出管制考量應考量的事項如下：

（１）、來訪人員進入管制區應予適當的管制，並記錄進出時間；來訪人員只有在特定的目的或是被授權情形下，才能進入管制區。

（２）、在管制區內，所有的人員應配載身分識別標示，並隨時注意身分不明或可疑的人員。

（３）、機關員工離職後，應立即撤銷進入管制區的權利。

（三）資料中心及機房之安全管理

1. 重要業務運作的資訊中心及電腦機房，應設立良好的實體安全措施；資訊中心及電腦機房地點的選定，應考量火災、水災、地震等災害的可能性，並考量鄰近空間的可能安全威脅。
2. 資料中心及機房安全應考量的事項如下：

（１）、主要的設施應遠離大眾或是公共運輸系統可直接進出的地點。

（２）、資料中心及電腦機房的建築，應儘可能不要有過於明顯的標示；在建築物內部及外部的說明，應以提供最低必要的指引或配置說明為限。

（３）、樓層的配置說明及內部的電話聯絡簿，以不讓有心人士循線找出電腦設施的所在地為原則。

（４）、危險性及易燃性的物品，應存放在遠離資料中心或電腦機房的安全地點。非有必要，電腦相關文具設備不應存放在電腦機房內。

（５）、備援作業用的設備及備援媒體，應存放在安全距離以外的地點，以免資料中心或電腦機房受到損害時也一併受到毀損。

（６）、應安裝適當的安全偵測及防制設備，例如熱度及煙霧偵測設備，火災警報設備、滅火設備及火災逃生設備；各項安全設備應依廠商的使用說明書定期檢查。

（７）、單位資訊安全緊急處理作業程序應以書面方式記載，並定期演練及測試。

（四）辦公桌面之安全管理

1. 應考量採用辦公桌面的淨空政策，以減少文件及磁碟片等在正常的辦公時間之外遭未被授權的人員取用、遺失或是被破壞的機會。
2. 應考量的事項如下：

（１）文件及磁碟片在不使用或是不上班時，應存放在櫃子內。

（２）機密性及敏感性資訊不使用或下班時應該上鎖，最好是放在防火櫃之內。

（３）個人電腦及電腦終端機不使用時，應以上鎖、通行碼或是其他控制措施保護。

（４）應該考量保護一般郵件進出的地點，以及無人看管的傳真機。

（五）財產移轉之安全管理

電腦設備、資料或是軟體，在沒有管理人員書面授權的情形下，不應被帶離辦公室。

陸、業務永續運作之安全管理

一、業務永續運作之規劃程序

（一）、應建立跨部門的業務永續運作計畫程序，研訂及維護業務持續運作之計畫。

（二）、業務永續運作的規劃作業，應研析並降低人為或是意外因素對重要業務運作可能導致的威脅，使重要業務在系統發生事故、設施失敗或是受損害時，仍可持續運作。

（三）、業務永續運作計畫，應考量下列事項：

１、界定重要的業務作業程序，並訂定其優先順序。

２、評估各種災害對業務可能的衝擊。

３、維持單位永續運作之人員責任界定，以及緊急應變措施之安排。

４、建立單位永續運作之作業程序及流程，並以書面或其他電子方式記載。

５、應就緊急應變程序及作業流程，進行員工教育及訓練。

６、應測試緊急應變計畫。

７、應定期更新緊急應變計畫。

二、業務永續運作規劃架構

（一）、應建立及維持單一的永續作業計畫架構，使各種不同層次及等級的計畫相互連貫，並應訂定測試計畫及維護計畫之優先順序。

（二）、每項業務之永續運作計畫，應明定行動之條件，以及員工執行計畫之責任；機關研擬新的資訊計畫，應與機關緊急應變計畫程序相一致（例如疏散計畫、現有電腦服務系統的預備作業安排，以及通信及空間的配置。）

（三）、在業務永續運作之整體架構內，應訂定不同層次及等級的計畫，每一層次及等級的計畫，應涵蓋不同的計畫重點及負責回復作業的人員安排。

（四）、業務永續運作計畫，應考量的作業程序如下：

1. 訂定緊急應變作業程序，規定如何在發生危害業務運作事件發生時，應立即採取的行動。
2. 訂定預備作業程序，規定如何將必要的業務活動或是支援性的服務，移轉至另外一個臨時的作業地點。
3. 訂定回復作業程序，規定如何採取回復作業，使業務回復到原來正常的運作。
4. 訂定測試作業程序，規定如何及什麼時間執行測試作業。

（五）、每一層次的計畫以及每一項個別計畫，都應指定一位計畫執行督導人員。

（六）、緊急應變作業、人工預備作業及回復作業計畫等，應指定適當的單位或人員負責。
（七）、技術服務的預備作業安排（例如電腦及通信系統）應由技術服務提供者負責。

柒、其他未定事項以「行政院所屬各機關資訊安全管理規範」及相關規定規範之。

附錄

1. 行政院及所屬各機關資訊安全管理要點
2. 行政院及所屬各機關資訊安全管理規範