僑光科技大學資訊安全管理規範實施辦法

民國 97 年 5 月 27 日圖書資訊發展委員會通過
民國 97 年 6 月 10 日行政會議通過
民國 98 年 3 月 26 日行政會議通過

第 一 條　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，依據行政院所屬各機關資訊安全管理規範，訂定僑光科技大學資訊安全管理規範實施辦法（以下簡稱本辦法）。

第 二 條　本要點所稱各單位，指本校所屬各行政單位及教學單位。

第 三 條　人員安全管理及教育訓練

一、 甄選及進用之人員,如其工作職責須使用處理敏感性的資訊科技設施或涉及機密性資訊者，應經適當的安全評估程序。

二、 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。

第 四 條　系統與網路之安全管理：

一、 電腦病毒及惡意軟體之防範

（一）電腦病毒防制軟體應定期更新。

（二）對來路不明及內容不確定的檔案，應在使用前詳加檢查是否感染電腦病毒。

（三）定期修補系統漏洞程式。

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，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，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）攜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）系統文件應鎖在安全的儲櫃或其他安全場所。

（四）委外處理的電腦文件、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。

（五）應保護重要的資料檔案，以防止遺失、毀壞、被偽造或竄改。

（六）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）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進行安全控管。

（三）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。

（四）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。

（五）網路硬體設備視需要應加裝不斷電系統，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」及本校校園網路使用相關規定。

（二）被授權的網路使用者，限於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）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識別碼。

（六）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,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，及防止非法使用者假冒合法使用者身分登入主機進行偷竊、破壞等行為。

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;並於事後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。

（二）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) 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，追蹤入侵者。

(四) 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)應建立及維持系統使用者之註冊資料紀錄，以備日後查考。

(二)使用者調整職務及離（休）職時，應儘速註銷其系統存取權利。

(三)應定期檢查及取消閒置不用的識別碼及帳號。

十、 使用者識別碼之管理

(一)以嚴謹的程序核發識別碼，明確規定使用者應負的責任。

(二)個人應負責保護識別碼，維持識別碼的機密性。

(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。

十一、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)記錄終端機的識別資料或其網路位址。

十二、設備安全管理

(一)設備安置地點之保護

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。

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 電腦作業區應禁止抽煙及飲用食物。

5 在特定的作業環境下，可考慮使用鍵盤保護膜。

6 應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

應妥善地維護設備，以確保設備的完整性及可以持續使用。

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

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。

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，例如設定識別碼或是將檔案資料加密。

4 應隨時遵循設備製造廠商提供的保護使用說明。

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。

(六)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。

十三、周邊安全管理

(一)周圍環境之安全

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，達成安全控管的目的。

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。

實體環境的安全保護原則如下：

1 應明確界定有那些周邊設施須列為安全管制的對象。

2 不應對非相關的人員提供過多有關管制區的作業細節。

3 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，並視需要限制及監督其活動。

(二)人員進出管制

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。

進出管制應考量的事項如下：

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 機關員工離職後，應即撤銷進入管制區的權利。

(三)資料中心及機房之安全管理

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。

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 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。

3 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

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。

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再使用時，應以上鎖、識別碼或其他控制措施保護。

4 應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。

第 五 條　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。

業務永續運作計畫，應考量下列事項：

一、應就緊急應變程序及作業流程，進行員工教育及訓練

二、應測試緊急應變計畫。

三、應定期更新緊急應變計畫。

第 六 條　其他未訂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。

第 七 條　本辦法經圖書資訊發展委員會會議議決，行政會議通過，校長公布後實施，修訂時亦同。