行政院農業委員會水產試驗所資訊安全管理作業規範

91.10.08 行政院農業委員會農企字第 0910156761 號函同意備查

壹、依據

依據行政院八十八年九月十五日台經字第三四七三五號函訂頒「行政院所屬各機關資訊安全管理要點」訂定。

貳、目的

為強化本所資訊安全管理，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，保障員工權益，特訂定本規範。由所長及各單位主管督導所屬人員之資訊作業安全，並由企劃資訊組負責推動與協調各單位及網域資訊安全有關管理事項，以防範不法及不當行為。

參、通則

本規範所稱「各單位」係指本所各組、室、研究中心。「各網域」係指總所電腦中心及各派出單位已設置區域網路或網際網路且各自管理之獨立網路網域。

肆、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甄選及進用之人員，其工作職責如須使用處理敏感性、機密性資訊的科技設施，或須處理機密性及敏感性資訊者，應經適當的安全評估程序，並課予機密維護責任。

二、員工應參與資訊安全教育及訓練，使員工瞭解資訊安全的重要性及各種可能的安全風險，以提高員工資訊安全意識，促其遵守資訊安全規定。

伍、電腦系統之安全管理

一、各單位電腦系統作業程序及系統規劃

（一）應以審慎及正式的行政程序，處理資訊安全及電腦當機事件。應在最短的時間內，確認系統已回復正常作業及安全控制。緊急處理的各項行動，應予詳細記載，以備日後查考。

（二）資訊業務委外時，應於事前審慎評估可能的潛在安全風險（例如資料或使用者通行碼被破解、系統被破壞或資料損失等風險），並與廠商簽訂適當的資訊安全或保密協定，以及課予相關的安全管理責任，並納入契約條款。

（三）應規劃資訊系統設備損害或電腦當機時，可維持機關業務繼續正常作業的替代性作業方法。

（四）資訊設施及系統的變更，應建立控制及管理機制，以免造成系統安全上的漏洞。

二、各單位軟體管理及電腦病毒之防範

（一）應依「政府所屬各級行政機關電腦軟體管理作業要點」建立軟體管理政策，各單位軟體應指定專人集中保管，並定期稽核軟體使用情形。軟體異動均需填具「軟體保管單」（附表一）。軟體減損應做清除、銷毀或存檔等處理。

（二）各部門及使用者應遵守智慧財產權及相關軟體授權規定，禁止使用未取得授權的軟體。

（三）個人電腦均須安裝有效之單機版或網路版之防毒軟體，並設定病毒碼之定時自動更新，網路系統則應裝置防毒硬體或軟體。

（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）為防止系統資料庫遭受隱碼型攻擊（SQL Injection），資料庫應用系統軟體應增加對網頁式查詢字串之過濾程式碼。

三、各單位個人資料之保護

（一）應依據「電腦處理個人資料保護法」等相關規定，審慎處理及保護個人資料。

（二）應建立個人資料控制及管理機制，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。

四、各單位日常作業之安全管理

（一）應準備適當及足夠的備援設施，定期執行必要的資料及軟體備份及異地備援作業，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，並報告權責主管人員，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，應依據供應廠商的建議，建立監測系統，隨時監測電腦作業環境，並採取必要的補救措施。
（四）資訊設施及系統的變更，應建立控制及管理機制，以免造成系統安全上的漏洞。
五、各單位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，不再繼續使用或故障送修時，應將儲存的內容消除。
（二）機密性及敏感性資料，應防止洩漏或不法及不當的使用。
（三）系統文件應存放在安全的儲櫃或其他安全場所。
（四）電腦設備、媒體及資料委外處理時，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）與其他單位進行電子資料交換，應採行特別的安全保護措施，以防止未經授權的資料存取及竄改；機密性或敏感性文件，尤應加密或設定安全等級。
（七）因電腦病毒、設備硬體故障、錯誤操作或其他不明原因所導致之文件資料毀損，且無及時備份時，應立即停止作業，並通知相關人員，以利資料之回復處理。

陸、網路安全管理

一、各網域網路服務之管理
（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，提供取得授權的人員使用。
（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，或使用代理伺服器(Proxy Server)進行安全控管。
（四）離（休）職人員應依機關資訊安全規定及程序，取銷其存取網路之權利。
（五）網路系統管理人員如發現有可疑的網路安全或障礙處理等情事，得依授權規定檢查使用者相關檔案。
（六）機密性及敏感性的資料或文件，不得存放在對外開放的資訊系統中或以未加密之電子郵件方式傳送。
（七）網路系統管理人員應負責監督網路資料使用情形，檢查有無違反資訊安全規定之事件發生。
二、各單位網路使用者之管理
（一）網路使用者應遵守「政府網際服務網管理規範」及網路安全相關規定。如有違反網路安全情事，應依資訊安全規定，限制或撤消其網路資源存取權利，並依紀律規定及相關法規處理。
（二）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。
（三）禁止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或竊取他人的登入身份與登入網路通行碼。
（四）網路使用者不得將色情檔案建置在機關網路，亦不得在網路上散播色情文字、圖片、影像、聲音等不法或不當的資訊。
（五）禁止網路使用者發送電子郵件騷擾他人，導致其他使用者之不安與不便。
（六）禁止網路使用者發送匿名信、廣告信，或偽造他人名義發送電子郵件。
三、各網域網路安全規劃與管理
（一）存放機密性及敏感性資料之大型主機或伺服器主機(如DNS,Email,WWW等)，除作業系統既有的安全設定外，應規劃安全等級較高之密碼辨識系統，以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。
（二）與外界網路連接的網點，應加裝防火牆，以控管對外開放的資訊系統，以及外界與機關內

部網路之間的資料傳輸與資源存取。防火牆系統軟體，並應定期更新版本，以因應各種網路攻擊。

（三）電腦設備如遭病毒感染，應立即與網路離線，直到網管人員確認病毒已消除後，才可重新連線。

（四）各網域間的敏感性資料如透過網際網路傳送，宜經由虛擬專用網路(VPN)處理，以確保資料的隱密性。在未建置VPN之前，應以加密方式傳送。

（五）為確保內部網路與外界的服務持續暢通，內部網路與外界網路的連接，應儘量建立一個以上之網路固接連線替代路徑。

（六）對於通過防火牆之來源端主機IP位址、目的端主機IP位址、來源通訊埠編號、目的地通訊埠編號、通訊協定、登入登出時間、存取時間以及採取的行動，均應予確實記錄。

四、各網域遭受網路入侵之處理

（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，如無法切斷則必須關閉防火牆；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。

（六）向本所「資通安全處理小組」通報反應，以獲取必要的協助。

柒、系統存取控制

一、各網域使用者註冊管理

（一）應以書面、電子或其他方式，告知使用者之系統存取權利。

（二）要求使用者確實瞭解系統存取的各項條件及要求。

（三）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。

（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（退）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。

二、各網域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）當有跡象足以顯示系統及使用者密碼可能遭破解時，應立即更改密碼。

（四）使用者密碼的長度最少應由六個字元組成。且應避免以年月日等時間資訊、個人姓名、身分證字號或汽機車牌照號碼、電話號碼、使用者識別碼、使用者姓名、重複出現兩個字以上的識別字碼、以全部數字或是全部字母、英文字典的字、電腦主機名稱、作業系統名稱、地方名稱、專有名詞，等等作為通行密碼。

（五）在安全網域內，應提供使用者第一次登入系統時，更改臨時性通行碼之機制。

（六）應定期更換通行碼，且應儘量避免重複或循環使用舊的通行碼。對有存取系統公用程式等特別權限的帳號，使用者密碼的更改頻率應較一般通行碼為高。

（七）在軟體完成安裝作業後，應立即更改廠商預設的使用者密碼。

三、各網域電腦系統、應用系統及網路存取之安全控制

（一）應建立遠端電腦系統（尤其是開放使用者從公眾網路進入系統）與本單位連線作業之身分鑑別安全機制。

（二）網路系統規模過於龐大者，可考量將不同使用者及電腦系統分開成不同的領域，以降低可

能的安全風險。

（三）不同領域的網路系統，每一領域應以特定的安全設施加以保護；例如，可設置防火牆及網路閘門，隔開不同的網路系統，以安全的閘道控制不同領域的網路系統。

（四）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。

（五）分享式的網路系統（尤其是跨機關的網路系統），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。

（六）應依資訊存取規定，配賦應用系統的使用者（包括應用系統支援人員）與業務需求相稱的資料存取及應用系統使用權限。

（七）重要伺服器或應用系統之硬碟裝置應採用「容錯式獨立磁碟陣列(RAID 1,5)」，以便實體硬碟毀損時，能及時更換啟動及存取資料。

（八）對應用系統原始程式資料之存取，應建立嚴格的安全控制機制。

（九）對機密及敏感性的系統，應考量建置獨立的或是專屬的電腦作業環境。

四、各網域系統存取及應用之監督

（一）應建立及製作資訊安全事項的稽核軌跡，以作為日後調查及監督之用。包括使用者識別碼、登入及登出系統之日期及時間、終端機的識別資料或其位址；並須妥善保存至少三年。

（二）應建立系統使用情形之監督程序，確保使用者只能執行授權範圍內的事項；個別系統接受監督的程度，應依風險評估結果決定。

（三）應定期或設定網路自動校正電腦系統時間，以維持系統稽核紀錄的正確性及可信度，俾作為事後法律上或是紀律處理上的重要依據。本所網路時間校正伺服器為：ntp.tfrin.gov.tw。

五、各單位系統發展及維護之安全管理

（一）應在資訊系統規劃之需求分析階段，即將安全需求納入；新發展的資訊系統，或是現有系統功能之強化，皆應明定資訊安全需求，並將安全需求納入系統功能。

（二）應於相關文件規定資訊安全控制措施，以利使用者及電腦支援人員明瞭電腦系統內建之安全控管系統功能。

（三）作業系統應定期更新其安全漏洞補強套件。作業系統變更時，應評估其對應用系統是否造成負面的影響，或是產生安全問題。

（四）作業系統計劃變更應即時通知相關人員，以便在作業系統變更前，相關人員可以進行適當及充分的評估作業。

（五）廠商提供的套裝軟體，應儘可能不要自行變更或修改，如因特殊需要須修改，應考量是否會破壞系統內建的安全控制，以及危害鑑別系統真確性作業的風險。

（六）除非緊急，原則上應拒絕允許廠商進行遠端遙控維護，致可能形成安全漏洞。現場維護時，應有本所人員陪同監督其作為，並應填寫維護單備查。

捌、實體及環境安全管理

一、各單位資訊設備安全管理

（一）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減少未經授權存取系統的機會。

（二）電腦設備之電源，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。應考量安置預備電源，並使用不斷電系統。

（三）電力及通信用的電纜線，應予適當的保護，以防止被破壞或是資料被截取。

（四）設備之維護只能由授權之維護人員或廠商執行，並應詳載紀錄備查。

（五）含有儲存媒體的設備項目（如軟碟、硬碟、MO 光碟、ZIP 碟片等），應在障礙處理前詳加檢查，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。

二、各單位資訊設施周邊安全管理

（一）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:使用身分識別卡之門禁系統），達成安全控管的目的。

（二）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。
（三）支援重要業務運作的資料中心及電腦機房，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、地震等自然及人為災害發生的可能性，並考量鄰近空間的可能安全威脅。
（四）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。
（五）電腦機房應設置適當的保護措施，防止未被授權的人員進出；為降低未被授權的人員進入電腦機房的風險，可視需要設立一個獨立的物品及設備配送及裝載作業區域。
（六）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。

玖、資訊安全通報與稽核

一、各單位資訊安全事件之處理與通報

（一）員工如發現或懷疑資訊系統或資訊服務施設內部有安全漏洞、受威脅、系統弱點及軟體功能異常時，應迅速通報權責主管單位及人員或是系統服務廠商立即處理，而不應由系統使用者自行修改。
（二）軟體功能不正常時應注意螢幕上出現的徵兆或訊息，並立即停止使用電腦，迅速通知資訊支援單位。任何狀況下，使用者不應自行移除功能不正常的軟體；系統回復作業應由受過適當訓練及有經驗的人員執行。
（三）當網路系統遭受網路入侵、設備設施遭受破壞、資料文件遭受竊取或毀損時，各單位應即依本所「資通安全處理小組設置要點」規定，填具資通安全事件通報單，速送本所「資通安全處理小組」執行秘書簽辦，以獲得進一步協助。發生重大資通安全刑事案件時，並應報請檢警機關，會同政風單位協助調查。

二、各單位資訊安全稽核之應辦理事項

（一）資訊機密維護及稽核使用管理事項，由本所政風單位會同企劃資訊組負責辦理。
（二）各單位應指定資訊作業聯絡人，每半年以「資通安全外部稽核（自我評審）表」（附表二）進行資訊作業安全之自我評審，並接受本所稽核作業。
（三）本所企劃資訊組應建立全所資通安全管理稽核表，以備上級不定時審查之用。
（四）各重要系統中之紀錄檔案，應禁止任意刪除及修改，並妥善保存，以備外部稽核之參考。

拾、業務永續運作計畫之規劃及管理

一、各單位業務永續運作之規劃

（一）各重要應用系統應建立永續運作計畫，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。
（二）每項業務系統之永續運作計畫，應明定行動之條件，以及員工執行計畫之責任；研擬新的資訊計畫，應與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。）

二、各單位業務永續運作計畫之實施

（一）應不定期進行測試各重要應用系統之永續運作計畫，使應變計畫維持在有效及最新的狀態；測試計畫可以定期測試個別計畫的方式進行，以減少測試完整計畫的需求及頻率。
（二）為因應各種人為及天然災害造成業務運作受影響，須於重要系統中安裝救援回復軟體或時光回溯器並定期作全系統映像(IMAGE)或鏡射(MIRROR)備份。
（三）緊急應變作業、人工預備作業及回復作業計畫等，應指定適當的人員負責。

拾壹、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。