

雲林縣四湖鄉公所暨所屬各單位電腦設備安全暨資訊機密維護要點

中華民國 98 年 8 月 19 日 四鄉政字第 0980013840 號函頒發

壹、總則

- 一、目的：確保本所暨所屬各單位(清潔隊、圖書館、托兒所)現有電腦主機、週邊設備安全及使用電腦設備製作、保存與公務機密有關資料之作業管制，以保障資訊系統組織功能。

貳、設備安全管理

- 二、本所暨所屬各單位應用電腦安全暨資訊機密維護，除依照「國家機密保護法」、「電腦處理個人資料保護法」、「機密檔案管理辦法」與相關法令規定外，悉依本要點辦理。
- 三、製作、傳遞、保存具國家安全或公務機密之儲存媒體、檔案，或基於職權範圍內負責監督、管理，並定期或不定期檢討設備使用與資訊檔案管理情形。
- 四、前項設備所置場所應指定專人負責管理或裝設安全監控系統、自動消防等防護措施並應設置門禁管制。
- 五、重要的電腦系統，應設計使用自動切換備援電路，以免資料不當毀損。各項檔案應依性質，分別訂定備份數，並定期備份。重要檔案宜備份三份以上。各項程式檔案之更新與註銷均應依照一定的程序進行，並訂定電腦系統回復標準程序及注意事項。
- 六、不使用來路不明之儲存媒體，不使用非經許可之軟體程式；電腦設備加裝防毒軟體及規劃網路防毒軟體，

並適時更新防毒軟體。發現病毒侵入或異常畫面等，立即反映本所資訊部門(研考)妥處。

參、建立稽核制度

七、協調資訊主管單位(行政室)建立資訊稽核制度，依據本機關使用電腦狀況會同訂定資訊作業安全稽核表，定期或不定期稽核電腦設備之使用及資訊檔案管理情形。

八、電腦系統管理人員(研考)得在程式及檔案中，加入通行碼之檢測，隨時稽查，以防止非法進入系統存取資料。

九、對各級單位資料作業人員，應持續考核，對不合於安全規定或有顧慮人員，應調整或調離其職務。

肆、資料輸出入管制

十、重要或具機密性資料應自行錄製建檔，並應加設資料存取控制，以防外洩。

十一、各項資料之輸出入，均應建立識別碼、通行碼等之管理制度，並應視需要經常更新。

十二、輸出之機密性報表，應依規定區分機密等級。

十三、委託其他機關或資訊服務廠商代為處理時，應派員在場監督。

十四、電腦大筆資料檔之抓取及提供，應記錄索取單位、日期、資料筆數、型態及是否機密性，以備查考。

十五、外單位申請資料查詢閱覽及複製時，需備文述明所依法令條文，及述明遵照資保法規定運用，經權責長官核准後交付。

伍、規範使用權責

十六、建立操作電腦設備的逐級授權制度，非經授權不得越級操作電腦設備。非辦公時間如需使用相關電腦系統，應將使用目的及時間、人員等報請權責長官核准。

十七、相關電腦系統應設定使用者工作權分級制度，如僅供查詢所需時，則限制不能進一步作修改建檔或系統維護等工作。

十八、每位電腦使用者應有獨立之通行密碼，並定期更換新碼，且密碼應設定內含 1 個大寫英文字母、1 個小寫英文字母、1 個阿拉伯數字、1 個特殊字元，至少符合 3 項上述原則，並至少有 8 個字元以上。避免使用與個人相關之文字或數字編排；退休、離職、調職或更換工作時，其代碼應即註銷或更改授權範圍。

十九、使用單位需變更電腦系統或應用軟體時，應提出維護需要，經核准後才能變更之。

陸、防範委託機構竊密

二十、各單位如委外進行系統維護工作時，對其可接觸之系統與資料範圍，應作適度規範，避免發生不當行為，並於完成作業後，即時取消其可用資源及使用權。

二十一、電腦機房及其附屬設備，如有委外之檢修人員工作時，資訊部門應指派專人辦理協助督導，並確實遵守單位各項安全規定。

二十二、單位之重要資料如需委外建檔時，無論在單位內、外進行登打，均應妥採安全管理措施，避免資料被竊、篡改、刪減、甚至植毒及盜拷備份等不法情事發生。

二十三、單位與委託機構訂定委外建檔或系統維護時，應於契約內明文加註保密責任，並據以執行，以作為發生洩密等案件時，追究刑事、行政責任之依據。

柒、連線作業管制

二十四、使用終端設備與其他機關主機連線作業時，應報請權責單位核准後列管，並於系統內限制其可運作範圍。

二十五、對於電腦之程式及設計、測試、製作等不得擅自更改，如有變更必要時，應報請權責長官核准。

二十六、電腦終端機使用者之識別碼及通行碼應依實際業務限制使用範圍，並嚴禁告知他人。

二十七、存放機密性及敏感性資料之大型主機或伺服器主機，應規劃安全等級較高之密碼辨識系統，以強化安全機制。

二十八、機關與外界網路連接的網點，應加裝防火牆，並由網路系統管理人員執行控管設定，隨時檢討及調整防火牆系統設定，調整系統存取權限，以反應最新的狀況。

捌、資訊檔案管制

二十九、建立資訊檔案管理制度，分級管理，具機密性資料，應依規定區分機密等級。

三十、資訊檔案中之資料，其更新、更正、註銷，均應報經核准，並將其變更內容、作業人員及時間等詳實紀錄。

玖、個人電腦管制

三十一、機密資料以儲存媒體建檔者，應加設資料存取控制。

三十二、印表機之使用應予管制，避免機密資料外流。

三十三、儲存機密資料指定專人管理，每日詳實記錄調借使用情形，定期清點數量，並注意保管之安全措施。

三十四、儲存媒體非必要不得擅自攜離辦公處所，與業務無關之外來儲存媒體不得上機使用。

三十五、非經權責主管核可，不得擅自加裝介面或變更硬體規格。

三十六、停止操作時，應將儲存媒體抽出，並將螢幕上之機密資料消除。

三十七、登入作業系統後於 15 分鐘未有任何動作時，應強迫自動登出系統或進入螢幕保護裝置，並須有密碼保護。

三十八、使用者電腦桌面需隨時保持淨空狀態，機密文件不得擺放於電腦桌面。

拾、網路安全管理

三十九、電腦網路應使用合法軟體，以免涉及智慧財產權或造成電腦中毒，單位網站所登載之資料亦應注意其合法性及適宜性，使用前宜經權責長官核可，避免造成無謂後遺症，甚至觸犯法律。

四十、參與行政機關網站電子資料流通作業時，應注意與網路連線之線路必需與單位內部業務電腦化網路完全阻隔，以免遭非法侵入擷取資料。

四十一、資訊部門(研考)應定期列印電腦使用紀錄備查，並隨時檢視有無異常，如發現有非本單位或非有權人員，進入電腦檔案資料庫查詢、盜拷或竊取機密資料時，應即反映政風等相關部門處理。

四十二、透過撥接式傳輸線路與主機連線之電話號碼，亦應嚴予保密。

壹拾壹、電腦犯罪防制措施：

四十三、嚴格門禁管理、強化各種安全維護設備。

四十四、電腦使用人及單位均應提高安全警覺、審慎過濾新進資訊人員。

四十五、灌輸電腦使用者道德及法紀觀念、經常調動可接觸到敏感機密資料之人員。

四十六、使用密碼(通行碼、識別碼)以及使用者記錄資料、限制業務範圍內之電腦系統使用權限、實施電腦稽核制度。

四十七、嚴密稽核，發掘違常及缺失。

四十八、每年應對人員進行資訊安全教育及訓練，促使其瞭解資訊安全的重要性及各種可能的資訊安

全風險，以提高員工資安意識，促其遵守資訊安全規定。

壹拾貳、實體存取控制：

四十九、電腦機房出入應有門禁管制，人員出入機房須刷卡。

五十、門禁卡應由行政室主管核可後始得配發。

五十一、因執行業務需求須經常性進出機房者，可申請臨時門禁卡，經機房管理人員主管核可後始得配發，並由機房或網路管理相關人員進行適當管控。

五十二、機房進出管制紀錄應定期審查，並保留至少 3 個月以上。

雲林縣四湖鄉公所暨所屬各單位電腦設備安全暨資訊機密維護要點逐點說明

規 定	說 明
壹、總則	
一、確保本所暨所屬各單位現有電腦主機、週邊設備安全及使用電腦設備製作、保存與公務機密有關資料之作業管制，以保障資訊系統組織功能。	一、強化本所暨所屬各單位公務機密維護，保障資訊安全。
貳、設備安全管理	章名
<p>二、本所暨所屬各單位應用電腦安全暨資訊機密維護，除依照「國家機密保護辦法」、「電腦處理個人資料保護法」、「機密檔案管理辦法」與相關法令規定外，悉依本要點辦理。</p> <p>三、製作、傳遞、保存具國家安全或公務機密之儲存媒體、檔案，或基於職權範圍內負監督、管理，並定期或不定期檢討設備使用與資訊檔案管理情形。</p> <p>四、前項設備所置場所應指定專人負責管理或裝設安全監控系統，並應</p>	<p>二、揭示本所暨所屬單位應用電腦安全暨資訊機密維護，除依照「國家機密保護辦法」、「電腦處理個人資料保護法」、「機密檔案管理辦法」與相關法令規定外，悉依本要點辦理。</p> <p>三、揭示設備安全管理範圍及人員。</p> <p>四、明定前項設備所置場所應指定專人負責管理或裝設安全監控系統，並應設置門禁管制、自動消防等防護措施以落實執行。儲存媒體(指記憶卡、隨身碟、隨身硬碟、磁碟片、磁帶、</p>

<p>設置門禁管制、自動消防等防護措施。</p> <p>五、重要的電腦系統，應設計使用自動切換備援電路，以免資料不當毀損。各項檔案應依性質，分別訂定備份數，並定期備份。重要檔案宜備份三份以上。各項程式檔案之更新與註銷均應依照一定的程序進行，並訂定電腦系統回復標準程序及注意事項。</p> <p>六、不使用來路不明之儲存媒體，不使用非經許可之軟體程式；電腦設備加裝防毒軟體及規劃網路防毒軟體，並適時更新防毒軟體。發現病毒侵入或異常畫面等，立即反映資訊等部門或相關部門妥處。</p>	<p>微縮片、績體電路晶片、光碟燒錄片(CD, DVD, MO)等足以記錄資料之任何工具)。</p> <p>五、為避免檔案遺失，重要的電腦系統，應設計使用自動切換備援電路，以免資料不當毀損。各項檔案應依性質，分別訂定備份數，並定期備份。重要檔案宜備份三份以上，確保萬全。</p> <p>六、要求使用合法軟體；電腦設備加裝防毒軟體及規劃網路防毒軟體，並適時更新防毒軟體。發現病毒侵入或異常畫面等，立即反映資訊等部門妥處。</p>
<p>參、建立稽核制度：</p>	<p>章名</p>
<p>七、協調資訊主管單位建立資訊稽核制度，依據本機關使用電腦狀況會同訂定資訊作業安全稽核表，定期或不定期核電腦設備之使用及資訊檔案管理情形。</p>	<p>七、為確保資訊安全，明定協調資訊主管單位建立資訊稽核制度，定期或不定期核電腦設備之使用及資訊檔案管理情形。</p> <p>八、強化電腦系統管理人員權責，得在程式及檔案中，</p>

<p>八、電腦系統管理人員得在程式及檔案中，加入通行碼之檢測，隨時稽查，以防止非法進入系統存取資料。</p> <p>九、對各級單位資料作業人員，應持續考核，對不合於安全規定或有顧慮人員，應調整或調離其職務。</p>	<p>加入通行碼之檢測，隨時稽查，以防止非法進入系統存取資料。</p> <p>九、明定應持續考核各級單位資料作業人員，並適時調整或調離職務。</p>
<p>肆、資料輸出入管制：</p>	<p>章名</p>
<p>十、重要或具機密性資料應自行錄製建檔，並應加設資料存取控制，以防外洩。</p> <p>十一、各項資料之輸出入，均應建立識別碼、通行碼等之管理制度，並應視需要經常更新。</p> <p>十二、輸出之機密性報表，應依規定區分機密等級。</p> <p>十三、委託其他機關或資訊服務廠商代為處理時，應派員在場監督。</p> <p>十四、電腦大筆資料檔之抓取及提供，應記錄索取單位、日期、資料筆數、型態及是否機密性，以備查考。</p> <p>十五、外單位申請資料查詢閱覽及複製時，需備文</p>	<p>十、為落實重要或具機密性資料維護，要求加設資料存取控制，以防外洩。</p> <p>十一、為落實公務機密，明定各項資料之輸出入，均應建立識別碼、通行碼等之管理制度。</p> <p>十二、明定輸出之機密性報表，應依規定區分機密等級。</p> <p>十三、委託其他機關或資訊服務廠商代為處理時，應派員在場監督，防址檔案外洩。</p> <p>十四、近來洩露個資時有所聞，為防止大筆檔案外洩，要求記錄所取檔案單位日期、資料筆數、型態及是否機密性。</p> <p>十五、明定調閱檔案程序及權責。</p>

<p>述明所依法令條文，及述明遵照資保法規定運用，經權責長官核准後交付。</p>	
<p>伍、規範使用權責：</p>	<p>章名</p>
<p>十六、建立操作電腦設備的逐級授權制度，非經授權不得越級操作電腦設備。非辦公時間如需使用相關電腦系統，應將使用目的及時間、人員等報請權責長官核准。</p> <p>十七、相關電腦系統應設定使用者工作權分級制度，如僅供查詢所需時，則限制不能進一步作修改建檔或系統維護等工作。</p> <p>十八、每位電腦使用者應有獨立之通行密碼，並定期更換新碼，且密碼應設定內含 1 個大寫英文字母、1 個小寫英文字母、1 個阿拉伯數字、1 個特殊字元，至少符合 3 項上述原則，並至少有 8 個字元以上。避免使用人與個人相關之文字或數字編排；退休、離職、調職或更換工作時，其代碼應即註銷或更改授權範圍。</p>	<p>十六、明定授權制度，非經授權不得越級操作電腦設備。並要求非上班時間使用電腦系統相關規範。</p> <p>十七、要求使用者工作權分級制度。</p> <p>十八、明定每位電腦使用者應有獨立之通行密碼，並定期更換新碼，並規定密碼設治原則。</p> <p>十九、非經核准不可變更電腦系統或應用軟體。</p>

<p>十九、使用單位需變更電腦系統或應用軟體時，應提出維護需要，經核准後才能變更之。</p>	
<p>陸、防範委託機構竊密：</p>	<p>章名</p>
<p>二十、各單位如委外進行系統維護工作時，對其可接觸之系統與資料範圍，應作適度規範，避免發生不當行為，並於完成作業後，即時取消其可用資源及使用權。</p> <p>二十一、電腦機房及其附屬設備，如有委外之檢修人員工作時，資訊部門應指派專人辦理協助督導，並確實遵守單位各項安全規定。</p> <p>二十二、單位之重要資料如需委外建檔時，無論在單位內、外進行登打，均應妥採安全管理措施，避免資料被竊、篡改、刪減、甚至植毒及盜拷備份等不法情事發生。</p> <p>二十三、單位與委託機構訂定委外建檔或系統維護時，應於契約內明文加註保密責任，並據以執行，以作為發生洩密等案件時，追究刑事責任之依據。</p>	<p>二十、明定委外進行系統維護工作範圍，並於完成作業後，即時取消其可用資源及使用權。</p> <p>二十一、為防止機密外洩，如有委外之檢修人員維修電腦機房及其附屬設備，資訊部門應指派專人辦理協助督導。</p> <p>二十二、重要資料如需委外建檔時，無論在單位內、外進行登打，均應妥採安全管理措施。</p> <p>二十三、明定委外建檔或系統維護時，應於契約內明文加註保密責任，並據以執行。</p>

柒、連線作業管制：	章名
<p>二十四、使用終端設備與其他機關主機連線作業者，應報請權責單位核准後列管，並於系統內限制其可運作範圍。</p> <p>二十五、對於電腦之程式及設計、測試、製作等不得擅自更改，如有變更必要時，應報請權責長官核准。</p> <p>二十六、電腦終端機使用者之識別碼及通行碼應依實際業務限制使用範圍，並嚴禁告知他人。</p> <p>二十七、存放機密性及敏感性資料之大型主機或伺服器主機，應規劃安全等級較高之密碼辨識系統，以強化安全機制。</p> <p>二十八、機關與外界網路連接的網點，應加裝防火牆，並由網路系統管理人員執行控管設定，隨時檢討及調整防火牆系統設定，調整系統存取權限，以反應最新的狀況。</p>	<p>二十四、為落實資訊管控，強化資訊安全，明定使用終端設備與其他機關主機連線作業者，應報請權責單位核准後列管，並於系統內限制其可運作範圍。</p> <p>二十五、電腦之程式及設計、測試、如有變更必要時，應報請權責長官核准，以符合程序。</p> <p>二十六、為防止資料外洩，電腦終端機使用者之識別碼及通行碼應依實際業務限制使用範圍，並嚴禁告知他人。</p> <p>二十七、為強化機密資訊，機密性及敏感性資料之大型主機或伺服器主機，應規劃安全等級較高之密碼辨識系統，以強化安全機制。</p> <p>二十八、為防止駭客入侵，機關與外界網路連接的網點，應加裝防火牆，並由網路系統管理人員執行控管設定，隨時檢討及調整防火牆系統設定，調整系統存取權限。</p>

玖、資訊檔案管制：	章名
<p>二十九、建立資訊檔案管理制度，分級管理，具機密性資料，應依規定區分機密等級。</p> <p>三十、資訊檔案中之資料，其更新、更正、註銷，均應報經核准，並將其變更內容、作業人員及時間等詳實紀錄。</p>	<p>二十九、機密檔案應與一般檔案分別存放，並依機密等級分別保管，其微縮片或其他複製品，亦同。</p> <p>三十、機密檔案經解密後，依一般檔案管理之，其更新、更正、註銷，均應報經核准，並將其變更內容、作業人員及時間等詳實紀錄。</p>
玖、個人電腦管制：	章名
<p>三十一、機密資料以儲存媒體建檔者，應加設資料存取控制。</p> <p>三十二、印表機之使用應予管制，避免機密資料外流。</p> <p>三十三、儲存機密資料指定專人管理，每日詳實記錄調借使用情形，定期清點數量，並注意保管之安全措施。</p> <p>三十四、儲存媒體不得擅自攜離辦公處所，與業務無關之外來儲存媒體不得上機使用。</p> <p>三十五、非經權責主管核可，不得擅自加裝介面或變更硬體規格。</p> <p>三十六、停止操作時，應將儲存媒體抽出，並將螢幕</p>	<p>三十一、指使用電腦或自動化機器為資料之輸入、儲存、編輯、更正、或其他方式建檔者，應加設資料存取控制。</p> <p>三十二、為防止資料外洩，印表機之使用應予管制，避免機密資料外流。</p> <p>三十三、專人管理機密資料，每日詳實記錄機密資料調借使用情形，並定期清點數量。</p> <p>三十四、明定儲存媒體不得擅自攜離辦公處所，與業務無關之外來儲存媒體不得上機使用。</p> <p>三十五、加裝介面或變更硬體規格，應經權責主管核可。</p> <p>三十六、為落實資訊機密維</p>

<p>上之機密資料消除。</p> <p>三十七、登入作業系統後於 15 分鐘未有任何動作時，應強迫自動登出系統或進入螢幕保護裝置，並須有密碼保護。</p> <p>三十八、使用者電腦桌面需隨時保持淨空狀態，機密文件不得擺放於電腦桌面。</p>	<p>護，停止操作時，應將儲存媒體抽出，並將螢幕上之機密資料消除。</p> <p>三十七、為避免暫時離開座位時機密外洩，登入作業系統後於 15 分鐘未有任何動作時，應強迫自動登出系統或進入螢幕保護裝置，並須有密碼保護。</p> <p>三十八、要求使用者電腦桌面需隨時保持淨空狀態，機密文件不得擺放於電腦桌面。</p>
<p>拾、網路安全管理：</p>	<p>章名</p>
<p>三十九、電腦網路應使用合法軟體，以免涉及智慧財產權或造成電腦中毒，單位網站所登載之資料亦應注意其合法性及適宜性，使用前宜經權責長官核可，避免造成無謂後遺症，甚至觸犯法律。</p> <p>四十、參與行政機關網站電子資料流通作業時，應注意與網路連線之線路必需與單位內部業務電腦化網路完全阻隔，以免遭非法侵入擷取資料。</p> <p>四十一、資訊部門應定期列印</p>	<p>三十九、明定電腦網路應使用合法軟體，以免涉及智慧財產權或造成電腦中毒。</p> <p>四十、為防止資料外洩，參與行政機關網站電子資料流通作業時，應注意與網路連線之線路必需與單位內部業務電腦化網路完全阻隔，以免遭非法侵入擷取資料。</p> <p>四十一、為強化資訊機密，資訊部門應定期列印電腦使用紀錄備查，並隨時檢視有無異常，如發現有非本單位或非有權人員，進入電腦檔案資料庫查</p>

<p>電腦使用紀錄備查，並隨時檢視有無異常，如發現有非本單位或非有權人員，進入電腦檔案資料庫查詢、盜拷或竊取機密資料時，應即反映資訊等相關部門處理。</p> <p>四十二、透過撥接式傳輸線路與主機連線之電話號碼，亦應嚴予保密。</p>	<p>詢、盜拷或竊取機密資料時，應即反映資訊等相關部門處理。</p> <p>四十二、為防止機密外洩，透過撥接式傳輸線路與主機連線之電話號碼，亦應嚴予保密。</p>
<p>壹拾壹、電腦犯罪防制措施：</p>	<p>章名</p>
<p>四十三、嚴格門禁管理、強化各種安全維護設備。</p> <p>四十四、電腦使用人及單位均應提高安全警覺、審慎過濾新進資訊人員。</p> <p>四十五、灌輸電腦使用者道德及法紀觀念、經常調動可接觸到敏感機密資料之人員。</p> <p>四十六、使用密碼(通行碼、識別碼)以及使用者記錄資料、限制業務範圍內之電腦系統使用權限、實施電腦稽核制度</p> <p>四十七、嚴密稽核，發掘違常及缺失。</p> <p>四十八、每年應對人員進行資訊安全教育及訓練，促使其瞭解資訊安全的重要性及各種可能的資訊</p>	<p>四十三、門禁管理是否落實，攸關機密維護工作執行成敗，故必須嚴格門禁管理、強化各種安全維護設備，防止機密外洩。</p> <p>四十四、電腦使用各及承辦人及主管人員均應提高安全警覺，具有敏銳度如發現任何異狀應做適當處理並反應權責單位、資訊人員負責管理資訊業務，固品德操守必須良好，方能確保保密義務。</p> <p>四十五、強化法紀教育，灌輸電腦使用者道德及法紀觀念、經常調動可接觸到敏感機密資料之人員，防止弊端發生。</p> <p>四十六、使用密碼(通行碼、識別碼)以及使用者記錄資料應落實管理、為避免</p>

<p>安全風險，以提高員工資安意識，促其遵守資訊安全規定。</p>	<p>同任接觸到非業務相關機密，限制業務範圍內之電腦系統使用權限。</p> <p>四十七、定期實施電腦稽核制度，嚴密稽核，發掘違常及缺失。</p> <p>四十八、預防機密外洩，每年應對人員進行資訊安全教育及訓練。</p>
<p>壹拾貳、實體存取控制：</p>	<p>章名</p>
<p>四十九、電腦機房出入應有門禁管制，人員出入機房須刷卡。</p> <p>五十、門禁卡應由權責單位主管核可後始得配發。</p> <p>五十一、因執行業務需求須經常性進出機房者，可申請臨時門禁卡，經機房權責單位主管核可後始得配發，並由機房或網路管理相關人員進行適當管控。</p> <p>五十二、機房進出管制紀錄應定期審查，並保留至少3個月以上。</p>	<p>四十九、為確保機房門禁維護，嚴防洩密事件發生，機房出入應有門禁管制，人員出入機房須刷卡。</p> <p>五十、為落實門禁管理，門禁卡應由權責單位主管核可後始得配發。</p> <p>五十一、明訂申請臨時門禁卡，經機房權責單位主管核可後始得配發，並由機房或網路管理相關人員進行適當管控。</p> <p>五十二、為保存記錄，機房進出管制紀錄應定期審查，並保留至少3個月以上</p>