田　尾　鄉　公　所
資通安全維護計畫

版次：112.3

目　錄

壹、 依據及目的

本計畫依據「資通安全管理法」第 10 條及施行細則第 6 條訂定。

貳、 適用範圍

本計畫適用範圍涵蓋本所全機關（附屬機關，有清潔隊、圖書館、鄉立幼兒園）。

參、 核心及非核心業務及說明

一、本所之核心業務及說明：本所無核心資訊系統。

二、本所之非核心業務及說明如下表：

非核心業務	業務失效影響說明	最大可容忍中斷時間	復原時間目標	資料復原時間點
公文交換系統	電子公文無法即時送達機關，影響機關行政效率	8 小時	8 小時	8 小時
防火牆服務	對外網路中斷或無管制連線	8 小時	8 小時	前一日
電子郵件系統	同仁無法正常寄送相關資料	36 小時	36 小時	前次備份
墓政系統	影響機關行政效率	48 小時	48 小時	前次備份
差勤系統	同仁無法正常登入使用	72 小時	72 小時	前次備份
薪資系統	影響機關行政效率	72 小時	72 小時	前次備份
財產管理系統	影響機關行政效率	72 小時	72 小時	前次備份

肆、 資通安全政策及目標

一、資通安全政策

為使本所業務順利運作，防止資訊或資通系統受未經授權之存取、使用、控制、洩漏、破壞、竄改、銷毀或其他侵害，並確保其機密性

（Confidentiality）、完整性（Integrity）及可用性（Availability），特制訂本政策如下，以供全體同仁共同遵循：

1. 應建立資通安全風險管理機制，定期因應內外在資通安全情勢變化，檢討資通安全風險管理之有效性。
2. 應保護機敏資訊及資通系統之機密性與完整性，避免未經授權的存取與竄改。
3. 應強固核心資通系統之韌性，確保公所業務持續營運。
4. 應因應資通安全威脅情勢變化，辦理資通安全教育訓練，以提高本所同仁之資通安全意識，本所同仁亦應確實參與訓練。
5. 針對辦理資通安全業務有功人員應進行獎勵。
6. 勿開啟來路不明或無法明確辨識寄件人之電子郵件。
7. 禁止多人共用單一資通系統帳號。
8. 機密資料檔案的讀取及複製，須符合本所各業務單位的規定，並經該單位主管或其授權人員核可。
9. 本政策每年應至少評估檢討一次，以反映本所資訊安全需求、政府法令法規、外在網路環境變化及資訊安全技術等最新發展現況，以確保其對於維持營運和提供適當服務的能力。
10. 本政策如遇重大改變時應立即審查，以確保其適當性與有效性。必要時應告知相關單位及委外廠商，以利共同遵守。

本政策經資通安全長核准，於公告日施行，並以書面、電子或其他方式通知員工及與本所連線作業之有關機關（構）、委外廠商，修正時亦同。

二、資通安全目標

(一) 量化型目標

1. 知悉資安事件發生，能於規定的時間完成通報、應變及復原作業。
2. 電子郵件社交工程演練之郵件開啟率及附件點閱率分別低於 5%

及 2%。

3. 本機關同仁每年皆完成 3 小時資通安全教育訓練。
4. 前次內部稽核發現事項，未完成改善之件數應≦2 件。

(二) 質化型目標

1. 適時因應法令與技術之變動，調整資通安全維護之內容，以避免資通系統或資訊遭受未經授權之存取、使用、控制、洩漏、破壞、竄改、銷毀或其他侵害，以確保其機密性、完整性及可用性。
2. 達成資通安全責任等級分級之要求，並降低遭受資通安全風險之威脅。
3. 加強資安訓練、提升人員資安防護意識、有效偵測與預防外部攻擊。

三、資通安全政策及目標之核定程序

資通安全政策由本所行政室簽陳資通安全長核定。

四、資通安全政策及目標之宣導

1. 本所之資通安全政策及目標應每年透過教育訓練、內部會議、張貼公告等方式，向公所內所有人員進行宣導，並檢視執行成效。
2. 本所應每年向利害關係人（例如 IT 服務供應商、與機關連線作業有關單位）進行資安政策及目標宣導，並檢視執行成效。

五、資通安全政策及目標定期檢討程序

資通安全政策及目標應定期於資通安全管理審查會議中檢討其適切性。

伍、 資通安全推動組織

一、資通安全長

依「資通安全管理法」第 11 條之規定，本所訂定主任祕書為資通安全長，負責督導公所資通安全相關事項，其任務包括：

1. 資通安全管理政策及目標之核定、核轉及督導。
2. 資通安全責任之分配及協調。
3. 資通安全資源分配。
4. 資通安全防護措施之監督。
5. 資通安全事件之檢討及監督。
6. 資通安全相關規章與程序、制度文件核定。
7. 資通安全管理年度工作計畫之核定。
8. 資通安全相關工作事項督導及績效管理。
9. 其他資通安全事項之核定。

二、資通安全推動小組

(一) 組織

為推動本所之資通安全相關政策、落實資通安全事件通報及相關應變處理，由資通安全長召集各業務部門主管成立資通安全推動小組，其任務包括：

1. 跨部門資通安全事項權責分工之協調。
2. 應採用之資通安全技術、方法及程序之協調研議。
3. 整體資通安全措施之協調研議。
4. 資通安全計畫之協調研議。
5. 其他重要資通安全事項之協調研議。

(二) 分工及職掌

本所之資通安全推動小組依下列分工進行責任分組，並依資通安全長之指示負責下列事項，本所「資通安全推動小組」分組人員名單及職掌應列冊於「資通安全推動小組名冊」，並適時更新之：

1. 資通安全處理組：
   (1) 資通安全政策及目標之研議。
   (2) 訂定公所資通安全相關規章與程序、制度文件，並確保相關規章與程序、制度合乎法令及契約之要求。
   (3) 依據資通安全目標擬定公所年度工作計畫。
   (4) 傳達公所資通安全政策與目標。
   (5) 資通安全技術之研究、建置及評估相關事項。
   (6) 資通安全相關規章與程序、制度之執行。
   (7) 資訊及資通系統之盤點及風險評估。
   (8) 資料及資通系統之安全防護事項之執行。
   (9) 資通安全事件之通報及應變機制之執行。
   (10) 其他資通安全事項之規劃、辦理與推動。
2. 資通安全稽核組：
   (1) 辦理資通安全內部稽核，負責訂定及執行內部稽核計畫。
   (2) 執行及追蹤稽核缺失之矯正與預防措施之改善，並追蹤缺失事項之執行情形。
   (3) 評估與檢討資訊安全內部稽核之成效。
   (4) 稽查各種安控機制執行狀況並提出稽核總報告。
   (5) 定期或不定期執行本所之資通安全檢查。
   (6) 每年定期召開資通安全管理審查會議，提報資通安全事項執行情形。

陸、 專職人力及經費配置

一、專職人力及資源之配置

1. 本所依資通安全責任等級分級辦法之規定，屬資通安全責任等級C級，最低應設置資通安全專職人員1人，本所現有資通安全專

職人員名單及職掌應列冊於「資通安全推動小組名冊」，其分工如下，並適時更新。本所附屬機關，有清潔隊、圖書館、鄉立幼兒園，應屬資通安全責任等級E級。

(1) 資通安全管理面業務1人，負責推動資通系統防護需求分級、資通安全管理系統導入、內部資通安全稽核及教育訓練等業務之推動。

(2) 資通系統安全管理業務1人，負責資通系統分級及防護基準、安全性檢測、業務持續運作演練等業務之推動。

(3) 資通安全防護業務1人，負責資通安全監控管理機制、政府組態基準導入，資通安全防護設施建置及資通安全事件通報及應變業務之推動。

(4) 資通安全管理法法遵事項業務1人，負責本所對所屬公務機關或所管特定非公務機關之法遵義務執行事宜。

2. 本所之承辦單位於辦理資通安全人力資源業務時，應加強資通安全人員之培訓，並提升公所內資通安全專業人員之資通安全管理能力。本所之相關單位於辦理資通安全業務時，如資通安全人力或經驗不足，得洽請相關學者專家或專業機關（構）提供顧問諮詢服務。

3. 資安專職人員專業職能之培養，應依據資通安全責任等級分級辦法之規定。

(1) 資安專職人員總計應持有1張以上資通安全專業證照。

(2) 資安專職人員總計應持有1張以上資通安全職能評量證書。

4. 本所負責重要資通系統之管理、維護、設計及操作之人員，應妥適分工，分散權責，若負有機密維護責任者，應簽署「員工保密切結書」，並視需要實施人員輪調，建立人力備援制度。

5. 本所之首長及各級業務主管人員，應負責督導所屬人員之資通安

全作業，防範不法及不當行為。

6. 專業人力資源之配置情形應每年定期檢討，並納入資通安全維護計畫持續改善機制之管理審查。

二、經費之配置

1. 資通安全推動小組於規劃配置相關經費及資源時，應考量本所之資通安全政策及目標，並提供建立、實行、維持及持續改善資通安全維護計畫所需之資源。
2. 各單位於規劃建置資通系統建置時，應一併規劃資通系統之資安防護需求，並於整體預算中合理分配資通安全預算所佔之比例。
3. 各單位如有資通安全資源之需求，應配合公所預算規劃期程向資通安全推動小組提出[1]，由資通安全推動小組視整體資通安全資源進行分配，並經資通安全長核定後，進行相關之建置。
4. 資通安全經費、資源之配置情形應每年定期檢討，並納入資通安全維護計畫持續改善機制之管理審查。

柒、 資訊及資通系統之盤點

一、資訊及資通系統盤點

1. 本所每年辦理資訊及資通系統資產盤點，依管理責任指定對應之資產管理人，並依資產屬性進行分類，分別為人員類、資訊類、硬體類、軟體類、環境保護類等五大類，各分類說明如下：

大分類	小分類	範例
人員類 （People / PE）	編制內人員	正式編制人員、臨時人員、工讀生、專案人員、委外廠商……等。
	臨時鐘點人員	
	委外廠商駐點人員	
	委外廠商	

[1]各機關可填具資通安全需求申請單，格式可參附件：資通安全需求申請單。

資訊類（Information / IF）	作業文件	資料庫與資料檔案、備份資料、原始程式碼、網路架構圖、系統文件、操作或支援程序、使用手冊、教育訓練教材、管理制度文件、緊急應變&復原計畫、營運持續計劃（BCP）、稽核日誌、契約與協議、報表、表單記錄……等。
	系統文件	
	契約	
	資訊紀錄（電子/紙本）	
	系統紀錄（Log）	
硬體類（Hardware / HW）	個人電腦	一般硬體：包含電腦設備（伺服器、筆記型電腦、個人電腦、工作站）、CD/DVD 燒錄器、CD/DVD 光碟機、磁帶機、軟碟機、投影機、PDA、印表機……等。 通訊設備：集線器、橋接器、網路交換器、路由器、數據機、電話自動交換機（PBX）、網路纜線、防火牆、入侵偵測系統、視訊會議設備、傳真機、手機。 儲存媒體：CD/DVD（空白）、硬碟（無資料）、磁片（空白）、磁帶（空白）、移動式硬碟（空白）、錄音/影帶（無資料）……等。
	可攜式電腦	
	伺服器	
	資安設備	
	網路設備	
	可攜式儲存媒體	
	電腦保護設施	
	其他硬體	
軟體類（Software / SW）	作業系統	應用系統軟體、作業系統軟體、開發工具、套裝軟體、公用程式、防火牆軟體、防毒軟體、驗證軟體、資料庫管理系統（DBMS）、加密軟體、文件管理系統、內部開發程式、內部發展系統……等。
	應用系統	
	套裝軟體	
	軟體開發工具	
	資訊安全系統	
環境保護類（Environment / EV）	一般辦公區域	建築類：電腦機房、會議室、辦公室、監控室、接待區、交貨區/裝載區……等。 環境保護設施：不斷電系統、第二電力供應迴路、穩壓器、機櫃、避雷裝置、警報系統、備用發電系統、環境控制系統（火偵測、熱偵測、水偵測、溫濕度偵測、自動消防滅火系統）……等。
	特殊辦公區域	
	資訊機房	
	倉庫/庫房	
	建築保護設施	

2. 本所每年度應依資訊及資通系統盤點結果，製作「資訊及資通系

統資產清冊」，欄位應包含：資訊及資通系統名稱、資產名稱、資產類別、擁有者、管理者、使用者、存放位置、防護需求等級。

3. 資訊及資通系統資產應以標籤標示於設備明顯處，並載明財產編號、保管人、廠牌、型號等資訊。核心資通系統及相關資產，並應加註標示。
4. 各單位管理之資訊或資通系統如有異動，應即時通知資通安全推動小組更新資產清冊。

二、機關資通安全責任等級分級

本所自行或委外開發之資通系統，為資通安全責任等級 C 級機關，本所附屬機關，有清潔隊、圖書館、鄉立幼兒園，應屬資通安全責任等級 E 級。

捌、 資通安全風險評估

一、本所應每年針對資訊及資通系統資產進行風險評估，並將評估結果紀錄於「風險評鑑工作表」。

二、執行風險評估時應參考行政院國家資通安全會報頒布之最新「資訊系統風險評鑑參考指引」，並依其中之「詳細風險評鑑方法」進行風險評估之工作。

三、本所應每年依據資通安全責任等級分級辦法之規定，分別就機密性、完整性、可用性、法律遵循性等構面評估自行或委外開發之資通系統防護需求分級。

四、風險評估項目及計算公式如下：

1. 資產風險計算需考量資產價值(C+I+A)、可能性及衝擊性等項目。
2. 資產價值＝資產之[機密性(C)＋完整性(I)＋可用性(A)]。
3. 資產風險＝ 資產價值(C+I+A) x 可能性 x 衝擊性

4. 風險分佈：

低風險	中風險	高風險
3~28	29~55	56~81

5. 當資產風險為高風險時，應填寫「風險改善計畫表」進行風險改善作業，若為中度風險，則依機關預算案年度進行改善。
6. 資產價值應考量機密性(C)、完整性(I)及可用性(A)，其評估標準請參考「資產價值評估量表」
7. 資產風險計算需評估各事件威脅發生率及脆弱度，其評估標準請參考「威脅發生率及脆弱度評估量表」。

五、威脅暨弱點評估：

將應進行威脅弱點評估之資產，可能面臨之事件(威脅-弱點)分為五類，請參考「威脅弱點對應表」，其類別包括：

1. 資訊資產風險：包含資料、文件之建立、維護、控管、傳遞不當等所產生之風險。
2. 軟體資產風險：包含系統設計、維護、操作不當等所產生之風險。
3. 實體資產風險:包含容量不足或維護之不當等所產生之風險。包含缺少實體安控或環境監控不足等所產生之風險。
4. 環境資產風險：包含容量不足、缺少實體安控或環境監控不足等所產生之風險。
5. 人員資產風險：包含因人員有意或無意行為、安全訓練不足等所產生之風險。

玖、 資通安全防護及控制措施

本所依據前章資通安全風險評估結果、自身資通安全責任等級之應辦事項及核心資通系統之防護基準，採行相關之防護及控制措施如下:

一、資訊及資通系統之管理

(一) 資訊及資通系統之保管

1. 資訊及資通系統管理人應確保資訊及資通系統已盤點造冊並適切分級，並持續更新以確保其正確性。
2. 資訊及資通系統管理人應確保資訊及資通系統被妥善的保存或備份。
3. 資訊及資通系統管理人應確保重要之資訊及資通系統已採取適當之存取控制政策。

(二) 資訊及資通系統之使用

1. 本所同仁使用資訊及資通系統前應經其管理人授權。
2. 本所同仁使用資訊及資通系統時，應留意其資通安全要求事項，並負對應之責任。
3. 本所同仁使用資訊及資通系統後，應依規定之程序歸還。資訊類資訊之歸還應確保相關資訊已正確移轉，並安全地自原設備上抹除。
4. 非本所同仁使用本所之資訊及資通系統，應確實遵守本所之相關資通安全要求，且未經授權不得任意複製資訊。
5. 對於資訊及資通系統，宜識別並以文件記錄及實作可被接受使用之規則。

(三) 資訊及資通系統之刪除或汰除

1. 資訊及資通系統之刪除或汰除前應評估公所是否已無需使用該等資訊及資通系統,或該等資訊及資通系統是否已妥善移轉或備份。
2. 資訊及資通系統之刪除或汰除時宜加以清查，以確保所有機敏性資訊及具使用授權軟體已被移除或安全覆寫。
3. 具機敏性之資訊或具授權軟體之資通系統，宜採取實體銷毀，或以毀損、刪除或覆寫之技術，使原始資訊無法被讀取，並避免僅使用標準刪除或格式化功能。

二、存取控制與加密機制管理

(一) 網路安全控管

1. 本所之網路區域劃分如下：
   (1) 外部網路：對外網路區域，連接外部廣網路（Wide Area Network, WAN）。
   (2) 內部區域網路（Local Area Network, LAN）：公所內部單位人員及內部伺服器使用之網路區段。
2. 外部網路、非軍事區及內部區域網路間連線需經防火牆進行存取控制，非允許的服務與來源不能進入其他區域。
3. 應定期檢視防火牆政策是否適當，並適時進行防火牆軟、硬體之必要更新或升級。
4. 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。
5. 本所內部網路之區域應做合理之區隔，使用者應經授權後在授權之範圍內存取網路資源。
6. 對網路系統管理人員或資通安全主管人員的操作，均應建立詳細的紀錄。並應定期檢視網路安全相關設備設定規則與其日誌紀錄，並檢討執行情形。
7. 使用者應依規定之方式存取網路服務，不得於辦公室內私裝電腦及網路通訊等相關設備。
8. 無線網路防護
   (1) 機密資料原則不得透過無線網路及設備存取、處理或傳送。
   (2) 無線設備應具備安全防護機制以降低阻斷式攻擊風險，且無線網路之安全防護機制應包含外來威脅及預防內部潛在干擾。
   (3) 行動通訊或紅外線傳輸等無線設備原則不得攜入涉及或處理

機密資料之區域。

(4) 用以儲存或傳輸資料且具無線傳輸功能之個人電子設備與工作站，應安裝防毒軟體，並定期更新病毒碼。

(二) 資通系統權限管理

1. 本所之資通系統應設置通行碼管理，通行碼之要求需滿足：
   (1) 通行碼長度 8 碼以上。
   (2) 通行碼複雜度應包含英文大寫小寫、特殊符號或數字三種以上。
   (3) 使用者每 90 天應更換一次通行碼。
2. 使用者使用資通系統前應經授權，並使用唯一之使用者 ID，除有特殊營運或作業必要經核准並紀錄外，不得共用 ID。
3. 使用者無繼續使用資通系統時，應立即停用或移除使用者 ID，資通系統管理者應定期清查使用者之權限。

(三) 特權帳號之存取管理

1. 資通系統之特權帳號請應經正式申請授權方能使用，特權帳號授權前應妥善審查其必要性，其授權及審查記錄應留存。
2. 資通系統之特權帳號不得共用。
3. 對於特權帳號，宜指派與該使用者日常公務使用之不同使用者 ID。
4. 資通系統之特權帳號應妥善管理，並應留存特殊權限帳號之使用軌跡。
5. 資通系統之管理者每季應清查系統特權帳號並劃定特權帳號逾期之處理方式。

(四) 加密管理

1. 本所之機密資訊於儲存或傳輸時應進行加密。
2. 本所之加密保護措施應遵守下列規定：
   (1) 應落實使用者更新加密裝置並備份金鑰。
   (2) 應避免留存解密資訊。

(3) 一旦加密資訊具遭破解跡象，應立即更改之。

三、作業與通訊安全管理

(一) 防範惡意軟體之控制措施

1. 本所之主機及個人電腦應安裝防毒軟體，並時進行軟、硬體之必要更新或升級。
   (1) 經任何形式之儲存媒體所取得之檔案，於使用前應先掃描有無惡意軟體。
   (2) 電子郵件附件及下載檔案於使用前，宜於他處先掃描有無惡意軟體。
   (3) 確實執行網頁惡意軟體掃描。
2. 使用者未經同意不得私自安裝應用軟體，管理者並應每半年定期針對管理之設備進行軟體清查。
3. 使用者不得私自使用已知或有嫌疑惡意之網站。
4. 設備管理者應定期進行作業系統及軟體更新，以避免惡意軟體利用系統或軟體漏洞進行攻擊。

(二) 遠距工作之安全措施

1. 本所資通系統之操作及維護以現場操作為原則，避免使用遠距工作，如有緊急需求時，應申請並經資通安全推動小組同意後始可開通。
2. 資通安全推動小組應定期審查已授權之遠距工作需求是否適當。
3. 針對遠距工作之連線應採適當之防護措施（並包含伺服器端之集中過濾機制檢查使用者之授權），並且記錄其登入情形。
   (1) 提供適當通訊設備，並指定遠端存取之方式。
   (2) 提供虛擬桌面存取，以防止於私有設備上處理及儲存資訊。
   (3) 進行遠距工作時之安全監視。
   (4) 遠距工作終止時之存取權限撤銷，並應返還相關設備。

(三) 電子郵件安全管理

1. 本所人員到職後應經申請方可使用電子郵件帳號，並應於人員離職後刪除電子郵件帳號之使用。
2. 電子郵件系統管理人應定期進行電子郵件帳號清查。
3. 電子郵件伺服器應設置防毒及過濾機制，並適時進行軟硬體之必要更新。
4. 使用者使用電子郵件時應提高警覺，並使用純文字模式瀏覽，避免讀取來歷不明之郵件或含有巨集檔案之郵件。
5. 原則不得電子郵件傳送機密性或敏感性之資料，如有業務需求者應依相關規定進行加密或其他之防護措施。
6. 使用者不得利用公所所提供電子郵件服務從事侵害他人權益或違法之行為。
7. 使用者應確保電子郵件傳送時之傳遞正確性。
8. 使用者使用電子郵件時，應注意電子簽章之要求事項。
9. 本所應定期舉辦(或配合上級機關舉辦)電子郵件社交工程演練，並檢討執行情形。

(四) 確保實體與環境安全措施

1. 資料中心及電腦機房之門禁管理
   (1) 資料中心及電腦機房應進行實體隔離。
   (2) 公所人員或來訪人員應申請及授權後方可進入資料中心及電腦機房，資料中心及電腦機房管理者並應定期檢視授權人員之名單。
   (3) 人員進入管制區應配載身分識別之標示，並隨時注意身分不明或可疑人員。
   (4) 僅於必要時，得准許外部支援人員進入資料中心及電腦機房。
   (5) 人員及設備進出資料中心及電腦機房應留存記錄。

2. 資料中心及電腦機房之環境控制

(1) 資料中心及電腦機房之空調、電力應建立備援措施。

(2) 資料中心及電腦機房之溫濕度管控範圍為：

(3) 資料中心及電腦機房應安裝之安全偵測及防護措施，包括熱度及煙霧偵測設備、火災警報設備、溫濕度監控設備、漏水偵測設備、入侵者偵測系統，以減少環境不安全引發之危險。

(4) 各項安全設備應定期執行檢查、維修，並應定時針對設備之管理者進行適當之安全設備使用訓練。

3. 辦公室區域之實體與環境安全措施

(1) 應考量採用辦公桌面的淨空政策，以減少文件及可移除式媒體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。

(2) 文件及可移除式媒體在不使用或不上班時，應存放在櫃子內。

(3) 機密性及敏感性資訊，不使用或下班時應該上鎖。

(4) 機密資訊或處理機密資訊之資通系統應避免存放或設置於公眾可接觸之場域。

(5) 顯示存放機密資訊或具處理機密資訊之資通系統地點之通訊錄及內部人員電話簿，不宜讓未經授權者輕易取得。

(6) 資訊或資通系統相關設備，未經管理人授權，不得被帶離辦公室。

(五) 資料備份

1. 重要資料及核心資通系統應進行資料備份，其備份之頻率應滿足復原時間點目標之要求，並執行異地存放。

2. 本所應每年確認核心資通系統資料備份之有效性。且測試該等資料備份時，宜於專屬之測試系統上執行，而非直接於覆寫回原資通系統。

3. 敏感或機密性資訊之備份應加密保護。

(六) 媒體防護措施

1. 使用隨身碟或磁片等存放資料時，具機密性、敏感性之資料應與一般資料分開儲存，不得混用並妥善保管。
2. 資訊如以實體儲存媒體方式傳送，應留意實體儲存媒體之包裝，選擇適當人員進行傳送，並應保留傳送及簽收之記錄。
3. 為降低媒體劣化之風險，宜於所儲存資訊因相關原因而無法讀取前，將其傳送至其他媒體。
4. 對機密與敏感性資料之儲存媒體實施防護措施，包含機密與敏感之紙本或備份磁帶，應保存於上鎖之櫃子，且需由專人管理鑰匙。

(七) 電腦使用之安全管理

1. 電腦、業務系統或自然人憑證，若超過十五分鐘不使用時，應立即登出或啟動螢幕保護功能並取出自然人憑證。
2. 禁止私自安裝點對點檔案分享軟體及未經合法授權軟體。
3. 連網電腦應隨時配合更新作業系統、應用程式漏洞修補程式及防毒病毒碼等。
4. 筆記型電腦及實體隔離電腦應定期以人工方式更新作業系統、應用程式漏洞修補程式及防毒病毒碼等。
5. 下班時應關閉電腦及螢幕電源。
6. 如發現資安問題，應主動循公所之通報程序通報。
7. 支援資訊作業的相關設施如影印機、傳真機等，應安置在適當地點，以降低未經授權之人員進入管制區的風險，及減少敏感性資訊遭破解或洩漏之機會。

(八) 行動設備之安全管理

1. 機密資料不得由未經許可之行動設備存取、處理或傳送。
2. 機敏會議或場所不得攜帶未經許可之行動設備進入。

3. 員工一律禁用私人的可攜式設備及可攜式儲存媒體等設施，如公務上須使用則須提出申請經權責主管核准後方可使用。
4. 可攜式設備及可攜式儲存媒體僅限於公務使用，禁止使用於私人用途，使用時應僅防資訊外洩或中毒。
5. 使用者如需使用外來的可攜式資訊設備或可攜式儲存媒體，必須先進行掃毒，確認其不含病毒與惡意程式，掃毒後方可進行資料之上傳及寫入作業，以避免受到惡意程式的威脅。
6. 將機密資料存放於可攜式儲存媒體上時，得採取適當加密處理或設定密碼保護（如 Word、Excel 或壓縮軟體之密碼功能），避免可攜式儲存媒體遺失時造成資訊外洩。
7. 筆記型電腦應安裝防毒軟體，並定期檢查作業系統修正程式與更新病毒碼為最新版本。
8. 存有重要機密性資訊之可攜式資訊設備或儲存媒體攜出時，設備管理人員應負保護之責不得離身，且針對相關檔案資料須執行加密或先清除其機密資訊，以避免資料洩露，另作業完成後須徹底抹去媒體上相關資料。
9. 可攜式設備及儲存媒體遺失時應立即通報單位主管，並評估資料遺失是否具有機密性，依情節之重大程度決定是否向上呈報。

(九) 即時通訊軟體之安全管理

使用即時通訊軟體傳遞機關內部公務訊息，其內容不得涉及機密資料。但有業務需求者，應使用經專責機關鑑定相符機密等級保密機制或指定之軟、硬體，並依相關規定辦理。

四、系統獲取、開發及維護

1. 本所之資通系統應依「資通安全責任等級分級辦法」附表八之規定完成系統防護需求分級，依分級之結果，完成附表九中資通系統防護基準，並注意下列事項：

(1) 開發過程請依安全系統發展生命週期（Secure Software Development Life Cycle, SSDLC）納入資安要求，並參考行政院國家資通安全會報頒布之最新「安全軟體發展流程指引」、「安全軟體設計指引」及「安全軟體測試指引」。

(2) 於資通系統開發前，設計安全性要求，包含機敏資料存取、用戶登入資訊檢核及用戶輸入輸出之檢查過濾，並檢討執行情形。

(3) 於上線前執行安全性要求測試，包含機敏資料存取、用戶登入資訊檢核及用戶輸入輸出之檢查過濾測試，並檢討執行情形。

(4) 執行資通系統源碼安全措施，包含源碼存取控制與版本控管，並檢討執行情形。

五、執行資通安全健診

1. 本所每二年應辦理資通安全健診，其至少應包含下列項目，並檢討執行情形：

(1) 網路架構檢視。

(2) 網路惡意活動檢視。

(3) 使用者端電腦惡意活動檢視。

(4) 伺服器主機惡意活動檢視。

(5) 安全設定檢視。

六、資通安全防護設備

1. 本所應建置防毒軟體、網路防火牆、電子郵件過濾裝置，持續使用並適時進行軟、硬體之必要更新或升級。

2. 資安設備應定期備份日誌紀錄，定期檢視並由主管複核執行成果，並檢討執行情形。

壹拾、資通安全事件通報、應變及演練相關機制

為即時掌控資通安全事件，並有效降低其所造成之損害，本所應訂定資通安全事件通報、應變及演練相關機制，詳「資通安全事件通報應變程序」。

壹拾壹、 資通安全情資之評估及因應

本所接獲資通安全情資，應評估該情資之內容，並視其對本所之影響、本所可接受之風險及本機關之資源，決定最適當之因應方式，必要時得調整資通安全維護計畫之控制措施，並做成紀錄。

一、資通安全情資之分類評估

本所接受資通安全情資後，應指定資通安全專職人員進行情資分析，並依據情資之性質進行分類及評估，情資分類評估如下：

(一) 資通安全相關之訊息情資

資通安全情資之內容如包括重大威脅指標情資、資安威脅漏洞與攻擊手法情資、重大資安事件分析報告、資安相關技術或議題之經驗分享、疑似存在系統弱點或可疑程式等內容，屬資通安全相關之訊息情資。

(二) 入侵攻擊情資

資通安全情資之內容如包含特定網頁遭受攻擊且證據明確、特定網頁內容不當且證據明確、特定網頁發生個資外洩且證據明確、特定系統遭受入侵且證據明確、特定系統進行網路攻擊活動且證據明確等內容，屬入侵攻擊情資。

(三) 機敏性之情資

資通安全情資之內容如包含姓名、出生年月日、國民身分證統一編號、護照號碼、特徵、指紋、婚姻、家庭、教育、職業、病例、醫療、基因、性生活、健康檢查、犯罪前科、聯絡方式、財務情況、社會活動及其他得以直接或間接識別之個人資料，或涉及個人、法人或團體營業上秘密或經營事業有關之資訊，或情資之公開或提

供有侵害公務機關、個人、法人或團體之權利或其他正當利益，或涉及一般公務機密、敏感資訊或國家機密等內容，屬機敏性之情資。

(四) 涉及核心業務、核心資通系統之情資

資通安全情資之內容如包含公所內部之核心業務資訊、核心資通系統、涉及關鍵基礎設施維運之核心業務或核心資通系統之運作等內容，屬涉及核心業務、核心資通系統之情資。

二、資通安全情資之因應措施

本所於進行資通安全情資分類評估後，應針對情資之性質進行相應之措施，必要時得調整資通安全維護計畫之控制措施。

(一) 資通安全相關之訊息情資

由資通安全推動小組彙整情資後進行風險評估，並依據資通安全維護計畫之控制措施採行相應之風險預防機制。

(二) 入侵攻擊情資

由資通安全專責人員判斷有無立即之危險，必要時採取立即之通報應變措施，並依據資通安全維護計畫採行相應之風險防護措施，另通知各單位進行相關之預防。

(三) 機敏性之情資

就涉及個人資料、營業秘密、一般公務機密、敏感資訊或國家機密之內容，應採取遮蔽或刪除之方式排除，例如個人資料及營業秘密，應以遮蔽或刪除該特定區段或文字，或採取去識別化之方式排除之。

(四) 涉及核心業務、核心資通系統之情資

資通安全推動小組應就涉及核心業務、核心資通系統之情資評估其是否對於機關之運作產生影響，並依據資通安全維護計畫採行相應之風險管理機制。

壹拾貳、 資通系統或服務委外辦理之管理

本所委外辦理資通系統之建置、維運或資通服務之提供時，應考量受託者之專業能力與經驗、委外項目之性質及資通安全需求，選任適當之受託者，並監督其資通安全維護情形。

一、選任受託者應注意事項

1. 受託者辦理受託業務之相關程序及環境，應具備完善之資通安全管理措施或通過第三方驗證。
2. 受託者應配置充足且經適當之資格訓練、擁有資通安全專業證照或具有類似業務經驗之資通安全專業人員。
3. 受託者辦理受託業務得否複委託、得複委託之範圍與對象，及複委託之受託者應具備之資通安全維護措施。

二、監督受託者資通安全維護情形應注意事項

1. 受託業務包括客製化資通系統開發者，受託者應提供該資通系統之第三方安全性檢測證明;涉及利用非自行開發之系統或資源者，並應標示非自行開發之內容與其來源及提供授權證明。
2. 受託者執行受託業務，違反資通安全相關法令或知悉資通安全事件時，應立即通知委託機關及採行之補救措施。
3. 委託關係終止或解除時，應確認受託者返還、移交、刪除或銷毀履行委託契約而持有之資料。
4. 受託者應採取之其他資通安全相關維護措施。
5. 本所應定期或於知悉受託者發生可能影響受託業務之資通安全事件時，以稽核或其他適當方式確認受託業務之執行情形。

壹拾參、 資通安全教育訓練

一、資通安全教育訓練要求

1. 本所依資通安全責任等級分級屬 C 級，資安及資訊人員每年至少

1 名人員接受 12 小時以上之資安專業課程訓練或資安職能訓練。

2. 本所之一般使用者與主管，每人每年接受 3 小時以上之一般資通安全教育訓練。

二、資通安全教育訓練辦理方式

1. 承辦單位應於每年年初，考量管理、業務及資訊等不同工作類別之需求，擬定資通安全認知宣導及「教育訓練計畫（表）」，以建立員工資通安全認知，提升機關資通安全水準，並應保存相關之資通安全認知宣導及教育訓練上課紀錄（表）。
2. 本所資通安全認知宣導及教育訓練之內容得包含：
   (1) 資通安全政策(含資通安全維護計畫之內容、管理程序、流程、要求事項及人員責任、資通安全事件通報程序等）。
   (2) 資通安全法令規定。
   (3) 資通安全作業內容。
   (4) 資通安全技術訓練。
3. 員工報到時，應使其充分瞭解本所資通安全相關作業規範及其重要性。
4. 資通安全教育及訓練之政策，除適用所屬員工外，對機關外部的使用者，亦應一體適用。

壹拾肆、 公務機關所屬人員辦理業務涉及資通安全事項之考核機制

本所所屬人員之平時考核或聘用，依據公務機關所屬人員資通安全事項獎懲辦法、彰化縣政府暨所屬機關公務人員平時獎懲標準表，及本所各相關規定辦理之。

壹拾伍、 資通安全維護計畫及實施情形之持續精進及績效管理

機制

一、資通安全維護計畫之實施

為落實本安全維護計畫，使本所之資通安全管理有效運作，相關單位於訂定各階文件、流程、程序或控制措施時，應與本所之資通安全政策、目標及本安全維護計畫之內容相符，並應保存相關之執行成果記錄。

二、資通安全維護計畫實施情形之稽核機制

(一) 稽核機制之實施

1. 資通安全推動小組應定期（至少每年一次）或於系統重大變更或組織改造後執行一次內部稽核作業，以確認人員是否遵循本規範與機關之管理程序要求，並有效實作及維持管理制度。
2. 辦理稽核前資通安全推動小組應擬定「資通安全稽核計畫」並安排稽核成員，稽核計畫應包括稽核之依據與目的、期間、重點領域、稽核小組組成方式、保密義務、稽核方式、基準與項目及受稽單位協助事項，並應將前次稽核之結果納入稽核範圍。
3. 辦理稽核時，資通安全推動小組應於執行稽核前 10 日，通知受稽核單位，並將稽核期程、「稽核項目紀錄表」及稽核流程等相關資訊提供受稽單位。
4. 本所之稽核人員應受適當培訓並具備稽核能力，且不得稽核自身經辦業務，以確保稽核過程之客觀性及公平性；另，於執行稽核時，應填具稽核項目紀錄表，待稽核結束後，應將稽核項目紀錄表內容彙整至稽核結果及改善報告中，並提供給受稽單位填寫辦理情形。
5. 稽核結果應對相關管理階層（含資安長）報告，並留存稽核過程之相關紀錄以作為資通安全稽核計畫及稽核事件之證據。
6. 稽核人員於執行稽核時，應至少執行一項特定之稽核項目（如是

否瞭解資通安全政策及應負之資安責任、是否訂定人員之資通安全作業程序與權責、是否定期更改密碼）。

(二) 稽核改善報告

1. 受稽單位於稽核實施後發現有缺失或待改善項目者，應對缺失或待改善之項目研議改善措施、改善進度規劃，並落實執行。
2. 受稽單位於稽核實施後發現有缺失或待改善者，應判定其發生之原因，並評估是否有其類似之缺失或待改善之項目存在。
3. 受稽單位於判定缺失或待改善之原因後，應據此提出並執行相關之改善措施及改善進度規劃，必要時得考量對現行資通安全管理制度或相關文件進行變更。
4. 公所應定期審查受稽單位缺失或待改善項目所採取之改善措施、改善進度規劃及佐證資料之有效性。
5. 受稽單位於執行改善措施時，應留存相關之執行紀錄，並填寫稽核結果及改善報告。

三、資通安全維護計畫之持續精進及績效管理

1. 本所之資通安全推動小組應於12月召開資通安全管理審查會議，確認資通安全維護計畫之實施情形，確保其持續適切性、合宜性及有效性。
2. 管理審查議題應包含下列討論事項：
   (1) 過往管理審查議案之處理狀態。
   (2) 與資通安全管理系統有關之內部及外部議題的變更，如法令變更、上級機關要求、資通安全推動小組決議事項等。
   (3) 資通安全維護計畫內容之適切性。
   (4) 資通安全績效之回饋，包括：
      A. 資通安全政策及目標之實施情形。
      B. 資通安全人力及資源之配置之實施情形。

C. 資通安全防護及控制措施之實施情形。

D. 內外部稽核結果。

E. 不符合項目及矯正措施。

(5) 風險評鑑結果及風險處理計畫執行進度。

(6) 重大資通安全事件之處理及改善情形。

(7) 利害關係人之回饋。

(8) 持續改善之機會。

3. 持續改善機制之管理審查應做成改善績效追蹤報告，相關紀錄並應予保存，以作為管理審查執行之證據。

壹拾陸、 資通安全維護計畫實施情形之提出

本所依據「資通安全管理法」第 12 條之規定，應於 12 月前向上級，提出資通安全維護計畫實施情形，使其得瞭解本所之年度資通安全計畫實施情形。

壹拾柒、 相關法規、程序及表單

一、相關法規及參考文件

1. 資通安全管理法
2. 資通安全管理法施行細則
3. 資通安全責任等級分級辦法
4. 資通安全事件通報及應變辦法
5. 資通安全情資分享辦法
6. 公務機關所屬人員資通安全事項獎懲辦法
7. 資訊系統風險評鑑參考指引
8. 政府資訊作業委外安全參考指引
9. 無線網路安全參考指引

10.網路架構規劃參考指引

11.行政裝置資安防護參考指引

12.政府行動化安全防護規劃報告

13.安全軟體發展流程指引

14.安全軟體設計指引

15.安全軟體測試指引

16.資訊作業委外安全參考指引

17.本機關資通安全事件通報及應變程序

18.彰化縣政府暨所屬機關公務人員平時獎懲標準表

二、附件表單

1. 資通安全推動小組名冊

2. 員工保密切結書

3. 資訊及資通系統資產清冊

4. 資產價值估量表

5. 威脅弱點對應表

6. 脆弱度及可能性評估量表

7. 風險評鑑工作表

8. 新進人員資安宣導單

9. 教育訓練計畫表

10.教育訓練上課紀錄表

田尾鄉公所資通安全推動小組名冊

版次：112.3

小組職稱	所屬單位	單位職稱	姓名	電話	電子郵件
資通安全長	秘書室	秘書	胡黎娜	04-8832171#100	twts001@tianwei.chcg.gov.tw
資通安全稽核組	政風室	主任	林儀尚	04-8832171#300	twts009@tianwei.chcg.gov.tw
資通安全稽核組	人事室	主任	張輝意	04-8832171#360	twts013@tianwei.chcg.gov.tw
資通安全處理組	財行課	課長	張世欣	04-8832171#320	twts003@tianwei.chcg.gov.tw
資通安全處理組	民政課	課長	黃國綸	04-8832171#120	twts002@tianwei.chcg.gov.tw
資通安全處理組	建設課	課長	鄧皓勻	04-8832171#105	twts004@tianwei.chcg.gov.tw
資通安全處理組	農觀課	課長	洪于閔	04-8832171#330	twts005@tianwei.chcg.gov.tw
資通安全處理組	社政課	課長	嚴淑怡	04-8832171#140	twts006@tianwei.chcg.gov.tw
資通安全處理組	圖書館	管理員	洪麗淑	04-8831540	twts010@tianwei.chcg.gov.tw
資通安全處理組	財行課	課員	倪育璋	04-8832171#370	twts119@tianwei.chcg.gov.tw

彰化縣田尾鄉公所員工保密切結書

本人 _____ 將嚴守工作保密規定與國家相關法令對業務機密負完全保密之責，並尊重智慧財產權。絕不擅自洩漏、傳播職務上任何業務相關資料及任職期間經辦、保管或接觸之所有須保密訊息資料；絕不擅自複製、傳播任何侵害智慧財產權之任何程式、軟體。保密之義務，不因調職或離職而終止。如有違反，依法負刑事、民事及行政責任。

此致

彰化縣田尾鄉公所

立 同 意 書 人：_____

身 分 證 字 號：_____

電　　話：_____

地　　址：_____

中　華　民　國　年　月　日

資訊資產清冊

單位名稱：彰化縣田尾鄉公所

紀錄編號：112.2

列印日期：1120715

NO.	資產類別		資產名稱	資產說明/財產編號	數量	存放位置	風險擁有者(部門)	使用者(部門)	資產評估			資產價值
	大類	小類							機密性	完整性	可用性	
1	軟體類	資訊安全系統	防火牆系統	NTWS0001	1	1樓機房	財行課	田尾鄉公所	3	3	2	8
2	軟體類	套裝軟體	郵件伺服器系統	NTWS0002	1	1樓機房	財行課	田尾鄉公所	1	2	2	5
3	硬體類	伺服器	郵件伺服器主機	NTWS0003	1	1樓機房	財行課	田尾鄉公所	2	2	1	5
4	硬體類	伺服器	網路儲存伺服器(Synology DS1821+)	NTWS0004	1	1樓機房	財行課	田尾鄉公所	2	3	3	8
5	硬體類	伺服器	網路儲存伺服器(Synology DS918)	NTWS0005	1	1樓機房	財行課	田尾鄉公所	1	2	2	5
6	硬體類	伺服器	人事網路儲存伺服器	NTWS0006	1	1樓機房	人事室	人事室	3	2	2	7
7	硬體類	伺服器	建設課網路儲存伺服器	NTWS0007	2	1樓機房	建設課	建設課	2	2	2	6
8	硬體類	伺服器	民政墓政系統主機	NTWS0008	1	1樓機房	民政課	民政課	2	2	2	6
9	環境保護類	資訊機房	機櫃	NTWS0009	3	1樓機房	財行課	財行課	2	1	1	4
10	環境保護類	資訊機房	不斷電系統	NTWS0010	3	1樓機房	財行課	財行課	1	1	2	4
11	環境保護類	資訊機房	空調設備	NTWS0011	2	1樓機房	財行課	財行課	1	2	3	6
12	環境保護類	資訊機房	二氧化碳滅火器	NTWS0012	1	1樓機房	財行課	財行課	1	2	1	4
13	環境保護類	資訊機房	溫濕度偵測計	NTWS0013	1	1樓機房	財行課	財行課	1	1	1	3
14	軟體類	作業系統	WINDOWS 7	NTWS0014	5	電腦主機	財行課	本所各課室	2	2	2	6
15	軟體類	作業系統	WINDOWS 10	NTWS0015	32	電腦主機	財行課	本所各課室	2	2	1	5
16	軟體類	作業系統	WINDOWS 11	NTWS0016	12	電腦主機	財行課	本所各課室	2	2	1	5
17	軟體類	作業系統	WINDOWS SERVER 2012 R2	NTWS0017	1	電腦主機	財行課	民政課	2	2	1	5
18	軟體類	應用系統	OFFICE 2007	NTWS0018	41	電腦主機	財行課	本所各課室	2	2	2	6
19	軟體類	應用系統	OFFICE 2016	NTWS0019	7	電腦主機	財行課	本所各課室	2	2	2	6
20	軟體類	應用系統	OFFICE 2019	NTWS0020	1	電腦主機	財行課	本所各課室	2	2	2	6
21	軟體類	應用系統	差勤系統	NTWS0021	1	電腦主機	人事室	人事室	3	2	1	6
22	軟體類	應用系統	墓政系統	NTWS0022	1	電腦主機	民政課	民政課	3	2	1	6
23	軟體類	應用系統	薪資管理資訊系統	NTWS0023	1	電腦主機	財行課	財行課	3	2	1	6
24	軟體類	應用系統	財產管理系統	NTWS0024	1	電腦主機	財行課	財行課	1	2	1	4
25	硬體類	網路設備	24port網路交換器	NTWS0025	1	機房	財行課	本所各課室	1	3	3	7
26	硬體類	網路設備	24port網路交換器	NTWS0026	1	本所1樓壁櫃	財行課	本所各課室	1	3	3	7
27	硬體類	網路設備	24port網路交換器	NTWS0027	1	本所2樓財行課	財行課	本所各課室	1	3	3	7

資訊資產清冊

單位名稱：彰化縣田尾鄉公所

紀錄編號：112.2

列印日期：1120715

NO.	資產類別		資產名稱	資產說明/財產編號	數量	存放位置	風險擁有者(部門)	使用者(部門)	資產評估			資產價值
	大類	小類							機密性	完整性	可用性	
28	硬體類	網路設備	24port網路交換器	NTWS0028	1	本所3樓	財行課	本所各課室	1	3	3	7
29	硬體類	網路設備	24port網路交換器	NTWS0029	1	本所2樓建設課	財行課	建設課	1	3	3	7
30	硬體類	網路設備	8port網路交換器	NTWS0030	1	秘書室側櫃	財行課	本所各課室	1	2	2	5
31	硬體類	網路設備	8port網路交換器	NTWS0031	1	鄉長室	財行課	本所各課室	1	2	2	5
32	硬體類	網路設備	8port網路交換器	NTWS0032	1	本所3樓財行課	財行課	財行課	1	2	2	5
33	硬體類	網路設備	無線路由器	NTWS0033	1	本所1樓壁櫃	財行課	本所各課室	2	1	1	4
34	硬體類	網路設備	無線路由器	NTWS0034	1	鄉長室	財行課	本所各課室	2	1	1	4
35	硬體類	網路設備	無線路由器	NTWS0035	2	3樓人事室及財行課	財行課	本所各課室	2	1	1	4
36	硬體類	網路設備	無線路由器	NTWS0036	1	4樓會議室天花板	財行課	本所各課室	2	1	1	4
37	硬體類	個人電腦	秘書室個人電腦組	NTWS0037	3	秘書室	財行課	秘書室	2	2	1	5
38	硬體類	個人電腦	民政課個人電腦組	NTWS0038	5	本所1樓民政課	民政課	民政課	2	2	1	5
39	硬體類	個人電腦	社政課個人電腦組	NTWS0039	10	社政課各承辦	社政課	社政課	2	2	1	5
40	硬體類	個人電腦	鄉長室個人電腦組	NTWS0040	3	鄉長室	財行課	財行課	2	2	1	5
41	硬體類	個人電腦	財行課個人電腦組(2樓)	NTWS0041	4	2樓財行課	財行課	財行課	2	2	1	5
42	硬體類	個人電腦	財行課個人電腦組(3樓)	NTWS0042	4	3樓財行課	財行課	財行課	2	2	1	5
43	硬體類	個人電腦	財行課個人電腦組(研考)	NTWS0043	1	3樓人事室研考	財行課	財行課	2	2	2	6
44	硬體類	個人電腦	財行課個人電腦組(檔管)	NTWS0044	1	4樓檔案室	財行課	財行課	2	2	2	6
45	硬體類	個人電腦	財行課個人電腦組(會議室)	NTWS0045	1	4樓會議室	財行課	財行課	1	1	1	3
46	硬體類	個人電腦	建設課個人電腦組	NTWS0046	7	2樓建設課	建設課	建設課	2	2	1	5
47	硬體類	個人電腦	人事室個人電腦組	NTWS0047	2	本所人事室	人事室	人事室	3	2	1	6
48	硬體類	個人電腦	主計室個人電腦組	NTWS0048	3	本所主計室	主計室	主計室	2	2	1	5
49	硬體類	個人電腦	村幹事個人電腦組	NTWS0049	5	本所3樓村幹事	民政課	村幹事	2	1	1	4
50	硬體類	個人電腦	政風室個人電腦組	NTWS0050	1	本所政風室	政風室	政風室	3	2	1	6
51	人員類	編制內人員	秘書	本所幕僚長	1	秘書室	田尾鄉公所	田尾鄉公所	3	3	2	8
52	人員類	編制內人員	機要人員	本所機要人員	1	秘書室	田尾鄉公所	秘書室	2	3	2	7
53	人員類	編制內人員	業務課室主管	民政、財行、建設、農觀、社政等課室主管	6	本所民政課	田尾鄉公所	民政課	2	2	2	6

資訊資產清冊

單位名稱：彰化縣田尾鄉公所

紀錄編號：112.2

列印日期：1120715

NO.	資產類別		資產名稱	資產說明/財產編號	數量	存放位置	風險擁有者(部門)	使用者(部門)	資產評估			資產價值
	大類	小類							機密性	完整性	可用性	
54	人員類	編制內人員	幕僚課室主管	人事、主計、政風等課室主管	3	本所財行課	田尾鄉公所	財行課	2	3	2	7
55	人員類	編制內人員	業務課室承辦	民政、財行、建設、農觀、社政等課室承辦	15	本所建設課	田尾鄉公所	建設課	2	1	2	5
56	人員類	編制內人員	幕僚課室承辦	人事、主計、政風	1	本所農觀課	田尾鄉公所	農觀課	2	2	2	6
57	人員類	編制內人員	公文收發與歸檔人員	公文收發與歸檔人員	2	本所社政課	田尾鄉公所	社政課	3	2	2	7
58	人員類	編制內人員	總務及研考人員	總務及研考人員	2	本所人事室	田尾鄉公所	人事室	2	3	2	7
59	人員類	編制內人員	村幹事	村幹事	5	本所主計室	田尾鄉公所	主計室	2	2	1	5
60	人員類	臨時鐘點人員	業務單位臨時人員	民政、財行、建設、農觀、社政等課室	13	本所民政課	田尾鄉公所	民政課	2	1	1	4
61	人員類	臨時鐘點人員	幕僚單位臨時人員	人事、主計、政風	1	本所政風室	田尾鄉公所	政風室	2	1	1	4
62	人員類	委外廠商	超鍏國際有限公司	本所資訊維護廠商	1	本所財行課	田尾鄉公所	財行課	2	3	2	7
63	人員類	委外廠商	上禾資訊科技有限公司	本所複印機維護廠商	1	本所財行課	田尾鄉公所	財行課	1	2	3	6
64	人員類	委外廠商	至星資訊有限公司	本所網路監聽封包維護廠商	1	本所財行課	田尾鄉公所	財行課	3	2	1	6

田尾鄉公所公所資產價值評估量表

一、機密性(C)量表

機密等級	資產類別	評估標準	數值
普	硬體資產	此資訊資產僅限機關人員存取。	1
	人員資產	機關員工，且無涉及機密性資訊處理之人員。	
	資訊/軟體/環境保護	無特殊之機密性要求，供機關員工使用。	
中	硬體資產	此資訊資產僅限機關相關業務承辦人員存取。	2
	人員資產	機關員工或被授權存取之人員。	
	資訊/軟體/環境保護	此資訊資產僅供機關相關業務承辦人員存取。	
高	資訊/軟體/硬體/環境保護	此資訊資產所包含資訊為機關或法律所規範的機密資訊。	3
	人員資產	可接觸機敏性資產、資料之人員。	

二、完整性(I)量表

完整等級	資產類別	評估標準	數值
低	資訊資產	資料不正確或不完整時，將對機關業務之營運造成輕微影響。	1
	硬體資產	硬體或通訊服務發生損壞或故障時，將對機關業務之營運造成輕微影響。	
	軟體資產	不當使用軟體時，將對機關業務之營運造成輕微影響。	

	環境保護資產	所使用之環境服務發生中斷時，將對機關業務之營運造成輕微影響。	
	人員資產	人員所負責之作業，因操作錯誤造成的資訊不完整，將對業務之營運造成輕微影響。	
中	資訊資產	資料不正確或不完整時，將對機關業務之營運造成中度影響，但不至於造成業務停頓。	2
	實體資產	硬體或通訊服務發生損壞或故障時，將對機關業務之營運造成中度影響，但不至於造成業務停頓。	
	軟體資產	不當使用軟體時，將對機關業務之營運造成中度影響，但不至於造成業務停頓。	
	環境保護資產	所使用之環境服務發生中斷時，將對機關業務之營運造成中度影響，但不至於造成業務停頓。	
	人員資產	人員所負責之作業，因操作錯誤造成的資訊不完整，將對業務之營運造成中度影響，但不至於造成業務停頓。	
高	資訊資產	文件及電磁紀錄具有完整性要求，當完整性被破壞時，將對機關業務之營運造成高度影響且致使業務停頓。	3
	硬體資產	硬體或通訊服務發生損壞或故障時，將對機關業務之營運造成高度影響且致使業務停頓。	
	軟體資產	不當使用軟體時，將對機關業務之營運造成高度影響且致使業務停頓。	
	環境保護資產	所使用之環境服務發生中斷時，將對機關業務之營運造成高度影響且致使業務停頓。	
	人員資產	人員所負責之作業，因操作錯誤造成的資訊不完整，將對業務之營運造成高度影響且致使業務停頓。	

三、可用性(A)量表

可用等級	評估標準	數值
低	16小時「可容忍該資訊資產失效時間」>24小時。	1
中	8小時「可容忍該資訊資產失效時間」＜24小時。	2
高	「可容忍該資訊資產失效時間」＜8小時。	3

田尾鄉公所威脅弱點對應表

一、人員類資通資產

大類	小類	弱點	威脅
人員類	全類	人員請假或離職	人員短缺（無適當代理人力）
		不足的安全訓練及認知	操作人員的錯誤
		缺乏安全的認知	使用人員的錯誤
		不當使用軟體及（或）硬體	非法輸出/入軟、硬體
			操作人員的錯誤
		不當的招募程序	罷工、怠工
			偷竊
			惡意損毀
		無簽署保密協議	機密資料外洩
		缺乏專業領域技能	作業延遲或中斷
		工作場所環境不良	易受環境傷害或意外災難
		缺乏人員離職資產繳回的確認程序	機密/敏感資訊洩漏
		未適當管理於組織外部工作的員工	機密/敏感資訊洩漏
		未適當監控清潔人員或外包人力的工作	機密/敏感資訊竊取
		未對清潔人員或外包人力提出安全保密規定	機密/敏感資訊洩漏
		人員離職或職務變更時未移除存取權限	人員不當存取、身分偽冒
		資訊安全意識及訓練不足	社交工程詐騙帳號、通行碼或窺視作業

二、資訊類資訊資產

大類	小類	弱點	威脅
資訊類	全類	缺乏文件及紀錄之管控	遺失、毀損、未授權存取
		缺乏實體保護	遺失、遭竊
			未授權存取
		缺乏備援拷貝	資料損毀
		缺乏加密機制	資料外洩
			非授權的存取
		攜帶方便、易被拷貝	資料外洩
		稽核軌跡紀錄未適當保護	竄改或刪除稽核軌跡紀錄
		稽核軌跡紀錄未適當處理	機密/敏感資訊遭未授權人員竊取、竄改或刪除
		文件未做適當的保管	機密/敏感資訊竊取
		儲存媒體未妥善保護	竊盜
		缺乏桌面淨空與畫面保護政策	遺失或損害資訊
		儲存媒體未適當處理即報廢或再利用	機密/敏感資訊洩漏
		失效文件未妥善處理	機密/敏感資訊洩漏
		未管制複製行為	機密/敏感資訊竊取

		資訊分級錯誤	未授權者存取（造成資訊外洩）
		測試資料選擇錯誤	個人敏感資料的洩漏
		加密金鑰未適當保護	資訊的揭露
		缺乏對輸入/輸出資料的檢查限制	資訊錯誤或洩漏
		未管制軟體的下載與使用	惡意的軟體
		機密/敏感性傳輸未保護	網路竊聽或資訊收集
		未定期進行備份回復測試	備份媒體損壞
		備份/回復程序不完整	資料遺失或損毀
		缺乏行動電腦的保護機制	對資訊的未授權存取
		未定期檢查使用者作業權限（存取權限設定錯誤）	對資訊的未授權存取
		未定期檢視監控錄影系統	錄影系統主機或鏡頭故障
			影像畫面資料遺失
		缺乏對資料處理的驗證	資訊的損毀
		人員離開座位時未登出或鎖定保護	對資訊的未授權存取或破壞

三、硬體類資訊資產

大類	小類	弱點	威脅
硬體類	個人電腦	不當使用軟體及（或）硬體	資源的不正確使用
			儲存媒體變質
		未保護的儲存空間	偷竊
			惡意損毀
			溫度與濕度超過限值
			儲存媒體變質
		存取控制的錯誤配置	未授權即使用媒體
			資源的不正確使用
		缺乏正確使用通訊媒體與傳訊的政策	未授權即使用媒體
			偷竊
			惡意損毀
			資源的不正確使用
		缺乏監控（monitoring）機制	未授權即使用媒體
			偷竊
			溫度與濕度超過限值
			資源的不正確使用
			儲存媒體變質
		缺乏稽核軌跡	未授權即使用媒體
			資源的不正確使用
		對電磁輻射敏感	硬體故障
			電磁輻射
			靜電
			儲存媒體變質
		對電壓變化敏感	硬體故障
			電壓不穩定
			儲存媒體變質

		對濕度灰塵及塵土敏感	灰塵
			空調故障
			硬體故障
			儲存媒體變質
	可攜式電腦	不足的維護或儲存媒體錯誤的安裝	硬體故障
			維護錯誤
		不當使用軟體及（或）硬體	硬體故障
			資源的不正確使用
		不當的服務維護回應	硬體故障
		未控制通訊線路	由非授權人員存取網路
			流量分析
			訊息轉接（rerouting）
			資源的不正確使用
		存取控制的錯誤配置	偷竊
			惡意損毀
			資源的不正確使用
		缺乏有效的建構變更控制	硬體故障
			維護錯誤
			操作人員的錯誤
		缺乏監控（monitoring）機制	偷竊
			惡意損毀
			硬體故障
			溫度與濕度超過限值
			操作人員的錯誤
		對電壓變化敏感	硬體故障
			電壓不穩定
		廢棄物處理疏於照管	偷竊
			資源的不正確使用
		撥接線路	由非授權人員存取網路
			資源的不正確使用
		儲存媒體未加以適當清除即丟棄或再利用	偷竊
			資源的不正確使用
	伺服器	不足的維護或儲存媒體錯誤的安裝	硬體故障
			維護錯誤
		不當使用軟體及（或）硬體	硬體故障
			資源的不正確使用
		不當的服務維護回應	硬體故障
		存取控制的錯誤配置	偷竊
			惡意損毀
			資源的不正確使用
		缺乏有效的建構變更控制	硬體故障
			維護錯誤
			操作人員的錯誤
		缺乏監控（monitoring）機制	偷竊
			惡意損毀
			硬體故障

			溫度與濕度超過限值
			操作人員的錯誤
		單點失效（Single point of failure）	通訊服務故障
			通訊纜線損壞
			硬體故障
		對電壓變化敏感	硬體故障
			電壓不穩定
		廢棄物處理疏於照管	偷竊
			資源的不正確使用
		儲存媒體未加以適當清除即丟棄或再利用	偷竊
			資源的不正確使用
	其他硬體	不足的維護或儲存媒體錯誤的安裝	硬體故障
			維護錯誤
		不當使用軟體及（或）硬體	硬體故障
			資源的不正確使用
		不當的服務維護回應	硬體故障
		存取控制的錯誤配置	未授權即使用媒體
			非法輸出/入軟體
			偷竊
			惡意損毀
			資源的不正確使用
		缺乏有效的建構變更控制	硬體故障
			維護錯誤
			操作人員的錯誤
		缺乏監控（monitoring）機制	偷竊
			惡意損毀
			硬體故障
			溫度與濕度超過限值
			操作人員的錯誤
		對電壓變化敏感	硬體故障
			電壓不穩定
		廢棄物處理疏於照管	偷竊
			資源的不正確使用
	網路設備	不良的佈線	通訊服務故障
			通訊纜線損壞
			傳輸錯誤
			滲透通訊
			維護錯誤
			操作人員的錯誤
		不良的通行碼（password）管理	由非授權的人員使用軟體
			假冒使用者身分
		不足的維護或儲存媒體錯誤的安裝	通訊服務故障
			硬體故障
			網路組件故障
			維護錯誤
		不當使用軟體及（或）	通訊服務故障

		硬體	硬體故障
			資源的不正確使用
			網路組件故障
		不當的服務維護回應	通訊服務故障
			硬體故障
			網路組件故障
		不當的網路管理	流量超載
			通訊服務故障
		未保護公眾網路連線	由非授權人員存取網路
			資源的不正確使用
		未保護敏感性資訊流	流量分析
			訊息被重組或轉送
		未保護通行碼資料表	由非授權的人員使用軟體
			假冒使用者身分
		未控制通訊線路	流量分析
			訊息轉接（rerouting）
			通訊纜線損壞
		存取控制的錯誤配置	惡意損毀
			資源的不正確使用
		缺乏有效的建構變更控制	硬體故障
			網路組件故障
			維護錯誤
			操作人員的錯誤
		缺乏發送端與接收端識別及鑑別機制	由非授權人員存取網路
			訊息被重組或轉送
			訊息轉接（rerouting）
		缺乏監控（monitoring）機制	惡意損毀
			硬體故障
			溫度與濕度超過限值
			操作人員的錯誤
		缺乏稽核軌跡	以非授權的方式使用網路設施
			由非授權人員存取網路
			惡意損毀
		缺乏識別及鑑別機制（如使用者鑑別）	由非授權的人員使用軟體
			假冒使用者身分
		軟體的已知缺陷	由非授權的人員使用軟體
			軟體故障
			惡意軟體
		通行碼以明碼傳送	由非授權的人員使用軟體
			假冒使用者身分
		單點失效（Single point of failure）	通訊服務故障
			硬體故障
			網路組件故障
		對電壓變化敏感	硬體故障
			電壓不穩定

		繁複的使用者介面	操作人員的錯誤
	通訊設備	不良的佈線	通訊服務故障
			通訊纜線損壞
			傳輸錯誤
			滲透通訊
			維護錯誤
			操作人員的錯誤
			竊聽
		不良的通行碼（password）管理	假冒使用者身分
			資源的不正確使用
		不足的維護或儲存媒體錯誤的安裝	通訊服務故障
			硬體故障
			維護錯誤
		不當使用軟體及（或）硬體	通訊服務故障
			硬體故障
			資源的不正確使用
		不當的服務維護回應	通訊服務故障
			硬體故障
		未保護公眾網路連線	資源的不正確使用
			竊聽
		未保護敏感性資訊流	竊聽
		未控制通訊線路	通訊纜線損壞
			竊聽
		存取控制的錯誤配置	惡意損毀
			資源的不正確使用
		缺乏有效的建構變更控制	通訊服務故障
			硬體故障
			維護錯誤
			操作人員的錯誤
		缺乏發送及接收訊息的證據	否認服務交易或收送訊息
		缺乏發送端與接收端識別及鑑別機制	否認服務交易或收送訊息
			資源的不正確使用
		缺乏監控（monitoring）機制	惡意損毀
			硬體故障
			資源的不正確使用
		缺乏稽核軌跡	惡意損毀
			資源的不正確使用
		缺乏識別及鑑別機制（如使用者鑑別）	否認服務交易或收送訊息
			假冒使用者身分
		單點失效（Single point of failure）	通訊服務故障
			硬體故障
		對電壓變化敏感	硬體故障
			電壓不穩定
		撥接線路	資源的不正確使用
		繁複的使用者介面	使用者錯誤

	可攜式儲存媒體	不良的通行碼（password）管理	未授權即使用媒體
		不足的維護或儲存媒體錯誤的安裝	硬體故障
			儲存媒體變質
		不當使用軟體及（或）硬體	非法使用軟體
			非法輸出/入軟體
			資源的不正確使用
			儲存媒體變質
		未保護的儲存空間	偷竊
			惡意損毀
			溫度與濕度超過限值
			儲存媒體變質
		未控制複製	偷竊
			資源的不正確使用
		存取控制的錯誤配置	未授權即使用媒體
			非法使用軟體
			非法輸出/入軟體
			資源的不正確使用
		缺乏正確使用通訊媒體與傳訊的政策	未授權即使用媒體
			偷竊
			惡意損毀
			資源的不正確使用
		缺乏有效的變更控制	使用者錯誤
			操作人員的錯誤
		缺乏定期替換計畫（schemes）	硬體故障
			儲存媒體變質
		缺乏備援拷貝	水災土石流
			火災
			偷竊
			惡意損毀
			儲存媒體變質
		缺乏發送及接收訊息的證據	否認服務交易或收送訊息
			儲存媒體變質
		缺乏監控（monitoring）機制	未授權即使用媒體
			非法使用軟體
			非法輸出/入軟體
			偷竊
			溫度與濕度超過限值
			資源的不正確使用
			儲存媒體變質
		缺乏稽核軌跡	未授權即使用媒體
			資源的不正確使用
		對電磁輻射敏感	硬體故障
			電磁輻射
			靜電
			儲存媒體變質

		對電壓變化敏感	硬體故障
			電壓不穩定
			儲存媒體變質
		對濕度灰塵及塵土敏感	灰塵
			空調故障
			硬體故障
			儲存媒體變質
		廢棄物處理疏於照管	偷竊
			資源的不正確使用
		儲存媒體未加以適當清除即丟棄或再利用	未授權即使用媒體
			偷竊
			資源的不正確使用
	電腦保護設施	不足的維護或儲存媒體錯誤的安裝	硬體故障
			維護錯誤
		不當的服務維護回應	硬體故障
		存取控制的錯誤配置	惡意損毀
			資源的不正確使用
		位處易有水患之地	水災土石流
		缺乏有效的建構變更控制	硬體故障
			維護錯誤
			操作人員的錯誤
		缺乏定期替換計畫（schemes）	硬體故障
			儲存媒體變質
		缺乏監控（monitoring）機制	惡意損毀
			硬體故障
			溫度與濕度超過限值
			操作人員的錯誤
		單點失效（Single point of failure）	硬體故障
			電力供應故障
			電壓不穩定
		對電壓變化敏感	硬體故障
			電壓不穩定

四、軟體類資訊資產

大類	小類	弱點	威脅
軟體類	軟體開發工具	缺乏備援拷貝	惡意軟體
		缺乏有效變更控制	操作人員的錯誤
			使用者的錯誤
		繁複的使用者介面	操作人員的錯誤
			使用者的錯誤
		缺乏稽核軌跡	未經授權的使用
		缺乏識別及鑑別機制（如使用者鑑別）	假冒使用者身分
		缺乏發送端與接收端識別及鑑別機制	未經授權的使用
			偷竊

		離開工作站沒有登出（Logout）	未經授權的使用
		沒有或不足的軟體測試	軟體故障
		不良的通行碼（password）管理	假冒使用者身分
		通行碼以明碼傳送	未經授權的使用
		軟體的已知缺陷	非法輸出/入軟體
			惡意的軟體
			軟體故障
	資訊安全系統	缺乏備援拷貝	惡意軟體
		缺乏有效變更控制	操作人員的錯誤
			使用者的錯誤
		繁複的使用者介面	操作人員的錯誤
			使用者的錯誤
		不當的服務維護回應	空調故障
			電力供應故障/停水
			硬體故障
			軟體故障
		缺乏稽核軌跡	未經授權的使用
		缺乏有效的建構變更控制	使用者的錯誤
			操作人員的錯誤
			軟體故障
		缺乏識別及鑑別機制（如使用者鑑別）	假冒使用者身分
		缺乏發送端與接收端識別及鑑別機制	未經授權的使用
			偷竊
		離開工作站沒有登出（Logout）	未經授權的使用
		沒有或不足的軟體測試	軟體故障
		不良的通行碼（password）管理	假冒使用者身分
		通行碼以明碼傳送	未經授權的使用
		不明確或不完整的開發規格	軟體故障
		軟體的已知缺陷	非法輸出/入軟體
			惡意的軟體
			軟體故障
	作業系統	缺乏稽核軌跡	未經授權的使用
		缺乏備援拷貝	惡意軟體
		缺乏有效的建構變更控制	操作人員的錯誤
			使用者的錯誤
			軟體故障
		缺乏識別及鑑別機制（如使用者鑑別）	假冒使用者身分
		離開工作站沒有登出（Logout）	未經授權的使用
		沒有或不足的軟體測試	軟體故障

		不良的通行碼（password）管理	未經授權的使用
			假冒使用者身分
		通行碼以明碼傳送	未經授權的使用
		軟體的已知缺陷	非法輸出/入軟體
			惡意軟體
			軟體故障
	應用系統	缺乏備援拷貝	惡意軟體
		缺乏有效變更控制	操作人員的錯誤
			使用者的錯誤
		繁複的使用者介面	操作人員的錯誤
			使用者的錯誤
		不當的服務維護回應	空調故障
			電力供應故障/停水
			硬體故障
			軟體故障
		缺乏稽核軌跡	未經授權的使用
		缺乏有效的建構變更控制	使用者的錯誤
			操作人員的錯誤
			軟體故障
		缺乏識別及鑑別機制（如使用者鑑別）	假冒使用者身分
		缺乏發送端與接收端識別及鑑別機制	未經授權的使用
			偷竊
		離開工作站沒有登出（Logout）	未經授權的使用
		沒有或不足的軟體測試	軟體故障
		不良的通行碼（password）管理	假冒使用者身分
		通行碼以明碼傳送	未經授權的使用
		不明確或不完整的開發規格	軟體故障
		軟體的已知缺陷	非法輸出/入軟體
			惡意的軟體
			軟體故障

◆ 硬體類資訊資產

大類	小類	弱點	威脅
硬體類	個人電腦	不當使用軟體及（或）硬體	資源的不正確使用
			儲存媒體變質
		未保護的儲存空間	偷竊
			惡意損毀
			溫度與濕度超過限值
			儲存媒體變質
		存取控制的錯誤配置	未授權即使用媒體
			資源的不正確使用
		缺乏正確使用通訊媒體與傳訊的政策	未授權即使用媒體
			偷竊

			惡意損毀
			資源的不正確使用
		缺乏監控（monitoring）機制	未授權即使用媒體
			偷竊
			溫度與濕度超過限值
			資源的不正確使用
			儲存媒體變質
		缺乏稽核軌跡	未授權即使用媒體
			資源的不正確使用
		對電磁輻射敏感	硬體故障
			電磁輻射
			靜電
			儲存媒體變質
		對電壓變化敏感	硬體故障
			電壓不穩定
			儲存媒體變質
		對濕度灰塵及塵土敏感	灰塵
			空調故障
			硬體故障
			儲存媒體變質
	可攜式電腦	不足的維護或儲存媒體錯誤的安裝	硬體故障
			維護錯誤
		不當使用軟體及（或）硬體	硬體故障
			資源的不正確使用
		不當的服務維護回應	硬體故障
		未控制通訊線路	由非授權人員存取網路
			流量分析
			訊息轉接（rerouting）
			資源的不正確使用
		存取控制的錯誤配置	偷竊
			惡意損毀
			資源的不正確使用
		缺乏有效的建構變更控制	硬體故障
			維護錯誤
			操作人員的錯誤
		缺乏監控（monitoring）機制	偷竊
			惡意損毀
			硬體故障
			溫度與濕度超過限值
			操作人員的錯誤
		對電壓變化敏感	硬體故障
			電壓不穩定
		廢棄物處理疏於照管	偷竊
			資源的不正確使用
		撥接線路	由非授權人員存取網路
			資源的不正確使用

		儲存媒體未加以適當清除即丟棄或再利用	偷竊
			資源的不正確使用
	伺服器	不足的維護或儲存媒體錯誤的安裝	硬體故障
			維護錯誤
		不當使用軟體及（或）硬體	硬體故障
			資源的不正確使用
		不當的服務維護回應	硬體故障
		存取控制的錯誤配置	偷竊
			惡意損毀
			資源的不正確使用
		缺乏有效的建構變更控制	硬體故障
			維護錯誤
			操作人員的錯誤
		缺乏監控（monitoring）機制	偷竊
			惡意損毀
			硬體故障
			溫度與濕度超過限值
			操作人員的錯誤
		單點失效（Single point of failure）	通訊服務故障
			通訊纜線損壞
			硬體故障
		對電壓變化敏感	硬體故障
			電壓不穩定
		廢棄物處理疏於照管	偷竊
			資源的不正確使用
		儲存媒體未加以適當清除即丟棄或再利用	偷竊
			資源的不正確使用
	其他硬體	不足的維護或儲存媒體錯誤的安裝	硬體故障
			維護錯誤
		不當使用軟體及（或）硬體	硬體故障
			資源的不正確使用
		不當的服務維護回應	硬體故障
		存取控制的錯誤配置	未授權即使用媒體
			非法輸出/入軟體
			偷竊
			惡意損毀
			資源的不正確使用
		缺乏有效的建構變更控制	硬體故障
			維護錯誤
			操作人員的錯誤
		缺乏監控（monitoring）機制	偷竊
			惡意損毀
			硬體故障
			溫度與濕度超過限值
			操作人員的錯誤
		對電壓變化敏感	硬體故障

			電壓不穩定
		廢棄物處理疏於照管	偷竊
			資源的不正確使用
	網路設備	不良的佈線	通訊服務故障
			通訊纜線損壞
			傳輸錯誤
			滲透通訊
			維護錯誤
			操作人員的錯誤
		不良的通行碼（password）管理	由非授權的人員使用軟體
			假冒使用者身分
		不足的維護或儲存媒體錯誤的安裝	通訊服務故障
			硬體故障
			網路組件故障
			維護錯誤
		不當使用軟體及（或）硬體	通訊服務故障
			硬體故障
			資源的不正確使用
			網路組件故障
		不當的服務維護回應	通訊服務故障
			硬體故障
			網路組件故障
		不當的網路管理	流量超載
			通訊服務故障
		未保護公眾網路連線	由非授權人員存取網路
			資源的不正確使用
		未保護敏感性資訊流	流量分析
			訊息被重組或轉送
		未保護通行碼資料表	由非授權的人員使用軟體
			假冒使用者身分
		未控制通訊線路	流量分析
			訊息轉接（rerouting）
			通訊纜線損壞
		存取控制的錯誤配置	惡意損毀
			資源的不正確使用
		缺乏有效的建構變更控制	硬體故障
			網路組件故障
			維護錯誤
			操作人員的錯誤
		缺乏發送端與接收端識別及鑑別機制	由非授權人員存取網路
			訊息被重組或轉送
			訊息轉接（rerouting）
		缺乏監控（monitoring）機制	惡意損毀
			硬體故障
			溫度與濕度超過限值
			操作人員的錯誤

		缺乏稽核軌跡	以非授權的方式使用網路設施
			由非授權人員存取網路
			惡意損毀
		缺乏識別及鑑別機制（如使用者鑑別）	由非授權的人員使用軟體
			假冒使用者身分
		軟體的已知缺陷	由非授權的人員使用軟體
			軟體故障
			惡意軟體
		通行碼以明碼傳送	由非授權的人員使用軟體
			假冒使用者身分
		單點失效（Single point of failure）	通訊服務故障
			硬體故障
			網路組件故障
		對電壓變化敏感	硬體故障
			電壓不穩定
		繁複的使用者介面	操作人員的錯誤
	通訊設備	不良的佈線	通訊服務故障
			通訊纜線損壞
			傳輸錯誤
			滲透通訊
			維護錯誤
			操作人員的錯誤
			竊聽
		不良的通行碼（password）管理	假冒使用者身分
			資源的不正確使用
		不足的維護或儲存媒體錯誤的安裝	通訊服務故障
			硬體故障
			維護錯誤
		不當使用軟體及（或）硬體	通訊服務故障
			硬體故障
			資源的不正確使用
		不當的服務維護回應	通訊服務故障
			硬體故障
		未保護公眾網路連線	資源的不正確使用
			竊聽
		未保護敏感性資訊流	竊聽
		未控制通訊線路	通訊纜線損壞
			竊聽
		存取控制的錯誤配置	惡意損毀
			資源的不正確使用
		缺乏有效的建構變更控制	通訊服務故障
			硬體故障
			維護錯誤
			操作人員的錯誤

		缺乏發送及接收訊息的證據	否認服務交易或收送訊息
		缺乏發送端與接收端識別及鑑別機制	否認服務交易或收送訊息
			資源的不正確使用
		缺乏監控（monitoring）機制	惡意損毀
			硬體故障
			資源的不正確使用
		缺乏稽核軌跡	惡意損毀
			資源的不正確使用
		缺乏識別及鑑別機制（如使用者鑑別）	否認服務交易或收送訊息
			假冒使用者身分
		單點失效（Single point of failure）	通訊服務故障
			硬體故障
		對電壓變化敏感	硬體故障
			電壓不穩定
		撥接線路	資源的不正確使用
		繁複的使用者介面	使用者錯誤
	可攜式儲存媒體	不良的通行碼（password）管理	未授權即使用媒體
		不足的維護或儲存媒體錯誤的安裝	硬體故障
			儲存媒體變質
		不當使用軟體及（或）硬體	非法使用軟體
			非法輸出/入軟體
			資源的不正確使用
			儲存媒體變質
		未保護的儲存空間	偷竊
			惡意損毀
			溫度與濕度超過限值
			儲存媒體變質
		未控制複製	偷竊
			資源的不正確使用
		存取控制的錯誤配置	未授權即使用媒體
			非法使用軟體
			非法輸出/入軟體
			資源的不正確使用
		缺乏正確使用通訊媒體與傳訊的政策	未授權即使用媒體
			偷竊
			惡意損毀
			資源的不正確使用
		缺乏有效的變更控制	使用者錯誤
			操作人員的錯誤
		缺乏定期替換計畫（schemes）	硬體故障
			儲存媒體變質
		缺乏備援拷貝	水災土石流
			火災
			偷竊

			惡意損毀
			儲存媒體變質
		缺乏發送及接收訊息的證據	否認服務交易或收送訊息
			儲存媒體變質
		缺乏監控（monitoring）機制	未授權即使用媒體
			非法使用軟體
			非法輸出/入軟體
			偷竊
			溫度與濕度超過限值
			資源的不正確使用
			儲存媒體變質
		缺乏稽核軌跡	未授權即使用媒體
			資源的不正確使用
		對電磁輻射敏感	硬體故障
			電磁輻射
			靜電
			儲存媒體變質
		對電壓變化敏感	硬體故障
			電壓不穩定
			儲存媒體變質
		對濕度灰塵及塵土敏感	灰塵
			空調故障
			硬體故障
			儲存媒體變質
		廢棄物處理疏於照管	偷竊
			資源的不正確使用
		儲存媒體未加以適當清除即丟棄或再利用	未授權即使用媒體
			偷竊
			資源的不正確使用
	電腦保護設施	不足的維護或儲存媒體錯誤的安裝	硬體故障
			維護錯誤
		不當的服務維護回應	硬體故障
		存取控制的錯誤配置	惡意損毀
			資源的不正確使用
		位處易有水患之地	水災土石流
		缺乏有效的建構變更控制	硬體故障
			維護錯誤
			操作人員的錯誤
		缺乏定期替換計畫（schemes）	硬體故障
			儲存媒體變質
		缺乏監控（monitoring）機制	惡意損毀
			硬體故障
			溫度與濕度超過限值
			操作人員的錯誤
		單點失效（Single point of failure）	硬體故障
			電力供應故障

			電壓不穩定
		對電壓變化敏感	硬體故障
			電壓不穩定

五、環境保護類資訊資產

大類	小類	弱點	威脅
建築與保護類	一般辦公區域	不當的服務維護回應	水供應故障
			空調故障
			硬體故障
			電力供應故障
		未監督外來人員或清潔人員之工作	偷竊
		建築或房間不當或疏於使用實體進出管制	偷竊
			惡意損毀
			資源的不正確使用
		缺乏門禁管制	偷竊
	特殊辦公區域	位處易有水患之地	水災土石流
		不當的服務維護回應	水供應故障
			空調故障
			硬體故障
			電力供應故障
		未監督外來人員或清潔人員之工作	偷竊
		建築或房間不當或疏於使用實體進出管制	偷竊
			惡意損毀
			資源的不正確使用
		缺乏門禁管制	偷竊
	資訊機房	位處易有水患之地	水災土石流
		不當的服務維護回應	水供應故障
			空調故障
			硬　體故障
			電力供應故障
		未監督外來人員或清潔人員之工作	偷竊
		建築或房間不當或疏於使用實體進出管制	偷竊
			惡意損毀
			資源的不正確使用
		缺乏門禁管制	偷竊
		缺乏備援拷貝	水災土石流
			資料遺失或毀損
			惡意損毀
		對溫度變化敏感	空調故障
			溫度與濕度超過限值
	倉庫（庫房）	不當的服務維護回應	水供應故障
			空調故障
			硬體故障

			電力供應故障
		未監督外來人員或清潔人員之工作	偷竊
		位處易有水患之地	水災土石流
		建築或房間不當或疏於使用實體進出管制	偷竊
			惡意損毀
			資源的不正確使用
	建築保護設施（環境控制系統如：火偵測、熱偵測、水偵測系統、自動消防滅火系統、溫濕度偵測等）	位處易有水患之地	水災土石流
		不足的維護或安裝的錯誤	地震
			維護錯誤
			儲存媒體變質
		不當的服務維護回應	水供應故障
			空調故障
			硬體故障
			電力供應故障
		未監督外來人員或清潔人員之工作	偷竊
		不當控管及使用或疏於管制實體進出	偷竊
			惡意損毀
			資源的損壞
		缺乏監控（monitoring）機制	以非授權的方式使用軟體
			以非授權的方式使用網路設施
			非法使用軟體
			非法輸出/入軟體
			溫度與濕度超過限值
		對溫度變化敏感	空調故障
			溫度與濕度超過限值
		對電壓變化敏感	電壓不穩定

社交工程	使用分享的乙太網路意即訊號會廣播到區域網路中之每一部機器。
	缺少要求同仁不可在電話上提供資訊的規範。
	缺少資訊諮詢的規範：待釐清詢問者的身份再給予資訊。
	缺乏交換資訊協議。
	通訊未加密。
	資訊相關辦公室或機房缺少實體安控。
	對有計畫的破壞行動缺乏懲戒處分。
破壞(偷竊,詐欺,竄改)	對有計畫的破壞行動缺乏懲戒處分。
偷竊	未控制資料及/或軟體複製。
詐欺	缺乏應用系統控管導致不實的付款。
誤傳	使用者訓練不足。
	缺少接收訊息證明。
	傳輸機密資料未加適當防護。
竄改或任意變更	缺少實體安控。
	缺少邏輯上(技術或系統)的存取安控。
	缺乏加解密規範與控管機制。
	缺乏有效的軟體變更管理導致未授權軟體變更而製造詐欺事件。

六、資訊資產

威脅	脆弱性
火災	使用易燃性之材質，如紙或盒子。
未授權存取資料	網路存取規劃不當。
	非單位內人員進出未有適當人員陪同。
	缺少實體安控。
	對有計畫的破壞行動缺乏懲戒處分。
	軟體開發者與作業人員的職責未釐清。
	程式人員監督不週。
作業人員或使用者錯誤	安全訓練不足。
	使用者認知不足。
	缺少文件。
	缺少有效的型態管理控制。
	複雜的使用者介面。

作業失能	備份失效
	保存不當
委外作業失能	未釐清委外協議的權責。
社交工程	缺少要求同仁不可在電話上提供資訊的規範。
	缺少資訊諮詢的規範：待釐清詢問者的身份再給予資訊。
冒充	未保護密碼(password)檔。
	缺乏身份鑑別與辨識機制。
	密碼易被人識破/取得。
破壞	存取權限不對。
	缺少實體安控。
	缺少變更管理控制。

	缺少邏輯上(技術或系統)的存取安控。
	對有計畫的破壞行動缺乏懲戒處分。
竊聽	未規範行動與遠端裝置之使用。
	使用分享的乙太網路意即訊號會廣播到區域網路中之每一部機器。
	缺乏交換資訊協議。
	通訊未加密。
	資料通訊室或中心缺少實體安控。
偷竊	未控制資料及/或軟體複製。

七、軟體資產

威脅	脆弱性
軟體程式錯誤	不清楚或不完整之開發規格。
	技術不足的人員。
	系統發展生命週期程序不足。
	缺少有效的型態管理控制。
通訊失能	未規劃與建置通訊線路。
	缺少備援與備份設備。
	缺乏意外處理機制。
惡意破壞資料與設施	缺少實體安控。
	缺少邏輯上(技術或系統)的存取安控。
	缺乏溝通導致離職同仁可存取系統。
	對有計畫的破壞行動缺乏懲戒處分。
惡意程式碼	未定期更新防毒軟體(病毒碼及掃瞄引擎)。
	未規劃與建置通訊線路。
	沒有防毒軟體。
	對人員在軟體病毒的教育不足。
	未實施程式碼檢驗。
	對有計畫的破壞行動缺乏懲戒處分。
詐欺	缺乏應用系統控管導致不實的付款。
傳輸錯誤	佈線不當。
	缺乏意外處理機制。

資料外洩	資料分級錯誤或處理不當。
誤傳	使用者訓練不足。
	缺少接收訊息證明。
	傳輸機密資料未加適當防護。
竄改或任意變更	缺少實體安控。
	缺少邏輯上(技術或系統)的存取安控。
	缺乏加解密規範與控管機制。
	缺乏有效的軟體變更管理導致未授權軟體變更而製造詐欺事件。
入侵	未更新或安裝作業系統/軟體的修補程式。
	開發或設定標準不足。
阻斷服務攻擊	網路管理不足。
	缺乏備援系統。
未授權軟體變更	缺少軟體變更管理規範與程序。
	缺少備份。
	缺少變更管理軟體。
	軟體失能的處理或報告不恰當。
	軟體開發者與作業人員的職責未釐清。
	程式人員監督不週。
未授權撥接存取	缺少使用者身份辨識。
作業人員或使用者錯誤	使用者認知不足。
	缺少有效的型態管理控制。
技術失能	使用者認知不足。
	變更管理流程失誤。
使用盜版軟體	未限制複製軟體。
	缺少人員使用合法軟體的規範。
	缺少軟體稽核。
	軟體派送安裝機制不足。
委外作業失能	未釐清委外協議的權責。
社交工程	缺少要求同仁不可在電話上提供資訊的規範。
	缺少資訊諮詢的規範：待釐清詢問者的身份再給予資訊。

破壞	存取權限不對。
	缺少變更管理控制。
軟體程式錯誤	不清楚或不完整之開發規格。
	技術不足的人員。
	系統發展生命週期程序不足。
	缺少有效的型態管理控制。
惡意程式碼	未定期更新防毒軟體(病毒碼及掃瞄引擎)。
	未控制由網際網路下載及使用軟體。
	沒有防毒軟體。
	資通安全政策不足。

八、實體資產

威脅	脆弱性
水災	位於易有天然災害地區。
	沒有回復資訊與資訊資產的營運持續管理與程序。
	備份檔案或系統無法使用。
火災	位於易有天然災害地區。
	沒有回復資訊與資訊資產的營運持續管理與程序。
	使用易燃性之材質，如紙或盒子。
	缺少火災偵測設備。
	缺少自動滅火系統。
	缺少實體安控。
	備份檔案或系統無法使用。
未授權存取資料	缺少實體安控。
	對有計畫的破壞行動缺乏懲戒處分。
地震	位於易有天然災害地區。
	沒有回復資訊與資訊資產的營運持續管理與程序。
	備份檔案或系統無法使用。
有害動物(蟲、鳥、獸)	位於易受環境影響的地區。
	沒有回復資訊與資訊資產的營運持續管理與程序。
污染	位於易受環境影響的地區。
	沒有回復資訊與資訊資產的營運持續管理與程序。
污染(放射線)	設備與設施缺乏維護。
	備份檔案或系統無法使用。

作業人員或使用者錯誤	使用者認知不足。
技術失能	由於不當的規劃或維護而導致網路容量不夠。
	技術設施維護不恰當。
	沒有回復資訊與資訊資產的營運持續管理與程序。
	使用者認知不足。
	缺少備份設施或流程。
	缺乏環境保護。
	變更管理流程失誤。
委外作業失能	沒有回復資訊與資訊資產的營運持續管理與程序。
	備份檔案或系統無法使用。
破壞	缺少實體安控。
	對有計畫的破壞行動缺乏懲戒處分。
偷竊	缺少實體安控。
通訊服務失能	網路管理不足(路徑彈性)。
惡意破壞資料與設施	缺少實體安控。
	缺乏溝通導致離職同仁可存取系統。
	對有計畫的破壞行動缺乏懲戒處分。
極端的溫濕度	位於易受環境影響的地區。
	沒有回復資訊與資訊資產的營運持續管理與程序。
	環境監控不足。
電力供給失能	電力供應設備容量不足。
電子干擾	位於易受環境影響的地區。
	沒有回復資訊與資訊資產的營運持續管理與程序。
電源不穩	位於易有電源不穩定地區。
	沒有回復資訊與資訊資產的營運持續管理與程序。
	沒有電力調節設備。
暴風雨(土石流,颱風)	位於易有天然災害地區。
	沒有回復資訊與資訊資產的營運持續管理與程序。

九、支援服務資產

威脅	脆弱性
干擾	傳輸介面易遭破壞或干擾。
中斷	缺乏應變計劃。
	容量不足。
	未釐清委外協議的權責。
	維護不當。
誤用	缺乏線路圖或標示不明。
	未釐清委外協議的權責。
	缺乏使用規範。

十、人員資產

威脅	脆弱性
未授權存取資料	未規劃與建置通訊線路。
	非單位內人員進出未有適當人員陪同。
	缺少實體安控。
	傳輸機密資料未加適當防護。
	對有計畫的破壞行動缺乏懲戒處分。
罷工	沒有回復資訊與資訊資產的營運持續管理與程序。
	缺乏勞資協議。
未授權軟體變更	缺少接收訊息證明。
	缺少軟體變更管理規範與程序。
	缺少備份。
	軟體失能的處理或報告不恰當。
	軟體開發者與作業人員的職責未釐清。
	程式人員監督不週。
	傳輸機密資料未加適當防護。
作業人員或使用者錯誤	安全訓練不足。
	使用者認知不足。
	缺少文件。
	缺少有效的型態管理控制。
	複雜的使用者介面。
否認	未使用數位簽章。
	缺少收送訊息證明。
使用盜版軟體	未限制複製軟體。
委外作業失能	未釐清委外協議的權責。

社交工程	使用分享的乙太網路意即訊號會廣播到區域網路中之每一部機器。
	缺少要求同仁不可在電話上提供資訊的規範。
	缺少資訊諮詢的規範：待釐清詢問者的身份再給予資訊。
	缺乏交換資訊協議。
	通訊未加密。
	資訊相關辦公室或機房缺少實體安控。
	對有計畫的破壞行動缺乏懲戒處分。
破壞(偷竊,詐欺,竄改)	對有計畫的破壞行動缺乏懲戒處分。
偷竊	未控制資料及/或軟體複製。
詐欺	缺乏應用系統控管導致不實的付款。
誤傳	使用者訓練不足。
	缺少接收訊息證明。
	傳輸機密資料未加適當防護。
竄改或任意變更	缺少實體安控。
	缺少邏輯上(技術或系統)的存取安控。
	缺乏加解密規範與控管機制。
	缺乏有效的軟體變更管理導致未授權軟體變更而製造詐欺事件。

田尾鄉公所脆弱度及威脅可能性評估量表

一、威脅可能性

可能性	評估標準	數值
低	● 很少發生。 ● 對於可預期之資訊安全威脅具有動機但能力不足以利用脆弱點造成資安事件。 ● 資訊安全事件因控制措施執行得當，有效降低脆弱點被利用，致使威脅發生之可能性極低。 ● 一年發生之次數約1 次，或三年1 次以上3 次以下。	1
中	● 偶爾發生。 ● 對於可預期之資訊安全威脅具有動機且有能力利用脆弱點造成資安事件。 ● 已採行部份資訊安全措施，脆弱點仍未被有效降低或減少，致使威脅發生之機率略高。 ● 一季發生之次數約1 次，或一年1 次以上4 次以下。	2
高	● 經常發生。 ● 對於可預期之資訊安全威脅具有動機且有能力利用脆弱點造成資安事件。 ● 未實行資訊安全措施或安全措施無效，脆弱點仍未被有效降低或減少，致使威脅發生機率偏高。 ● 一個月發生次數1 次以上，或一季發生2 次。	3

二、脆弱性量表

分數	衝擊	評估標準	
1	低	資料保護受到損害	● 資料外洩或竄改僅導致個人權益輕微受損。 ● 資通安全事件發生時，對資產會造成輕微的損失。
		影響業務運作	● 對於整體營運或業務執行影響不大。 ● 修復或進行復原的措施可以在很短時間（1 小時）內完成。 ● 造成的損害可能僅影響單一業務或系統 ● 可以由內部人員進行復原。
		影響法律規章遵循	導致組織違反法律規章並伴隨輕微不良後果。
		人員傷亡	
		損害組織信	對組織的信譽有輕微負面衝擊。
		其他	

2	中	資料保護受到損害	● 資料外洩將導致個人權益嚴重受損。 ● 資通安全事件發生時，對資產會造成較大的損失。 ● 資產機密等級誤判或機密性維護機制失能時對資產本身或相關資產造成間接或輕微的影響。
		影響業務運作	● 對於本組織數項業務營運或執行造成停頓。 ● 復原可能要數個小時到1天才能完成。 ● 造成的損害可能影響多種業務、數個系統、多個部門或合作夥伴。 ● 復原的措施必須由專業人員才能進行。
		影響法律規	導致機關違反法律規章並伴隨嚴重不良後果。
		人員傷亡	可能造成人員遭遇危險或受到輕微傷害。
		損害組織信	對組織的信譽有嚴重的負面衝擊。
		其他	
3	高	資料保護受到損害	● 資產機密等級誤判或機密性維護機制失能時，對資產本身或相關資產造成直接且嚴重的影響。 ● 資通安全事件發生時，對資產會造成嚴重的損失。 ● 資料外洩將危及國家安全、導致個人權益非常嚴重受損、或造成極大規模之個人權益嚴重受損。
		影響業務運作	● 對於本組織全部業務營運或執行造成停頓。 ● 復原無法於1天內完成。 ● 造成的損害可能影響全關或利益相關者。 ● 復原的措施僅能由外部特定專業人員才能進行或修復人員不易取得。
		影響法律規	導致組織從根本上違反法律規章。
		人員傷亡	可能造成人員遭遇危險或受到嚴重傷害。
		損害組織信	威脅到組織的未來。
		其他	

風險評鑑工作表

單位名稱:彰化縣田尾鄉公所	紀錄編號：112.2

資訊資產鑑別與評價								風險評鑑(評估與分析)						
No.	資產名稱	資產類別		資產價值評估				脆弱點評估		威脅評估		風險估計		
		大類	小類	機密性 (C)	完整性 (I)	可用性 (A)	合計	弱點名稱	脆弱度 (V)	威脅名稱	威脅發生機率(T)	風險值 小計	風險等級 (處理前)	
1	防火牆系統	硬體類	資訊安全系統	3	3	2	8	技術設施維護不恰當	3	技術失能	1	24	普	
2	郵件伺服器系統	軟體類	套裝軟體	1	2	2	5	未更新或安裝作業系統	2	阻斷服務攻擊	1	10	普	
3	郵件伺服器主機	硬體類	伺服器	2	2	1	5	電力供應設備容量不足	2	電力供給失能	1	10	普	
4	網路儲存伺服器(Synology DS1821+)	硬體類	伺服器	2	3	3	8	電力供給失能	1	電力供應設備容量不足	1	8	普	
5	網路儲存伺服器(Synology DS918)	硬體類	伺服器	1	2	2	5	技術設施維護不恰當	1	技術失能	2	10	普	
6	人事網路儲存伺服器	硬體類	伺服器	3	2	2	7	技術設施維護不恰當	2	技術失能	1	14	普	
7	建設課網路儲存伺服器	硬體類	伺服器	2	2	2	6	技術設施維護不恰當	2	技術失能	2	24	普	
8	民政墓政系統主機	硬體類	伺服器	2	2	2	6	技術設施維護不恰當	2	技術失能	2	24	普	
9	機櫃	環境保護類	資訊機房	2	1	1	4	缺乏定期更換	3	設備或媒體的破壞	2	24	普	
10	不斷電系統	環境保護類	資訊機房	1	1	2	4	電力供應設備容量不足	2	電力供應故障	1	8	普	
11	空調設備	環境保護類	資訊機房	1	2	3	6	技術設施維護不恰當	2	技術失能	1	12	普	
12	二氧化碳滅火器	環境保護類	資訊機房	1	2	1	4	技術設施維護不恰當	2	技術失能	1	8	普	
13	溫濕度偵測計	環境保護類	資訊機房	1	1	1	3	技術設施維護不恰當	1	技術失能	1	3	普	
14	WINDOWS 7	軟體類	作業系統	2	2	2	6	未更新或安裝作業系統	2	入侵	3	36	中	
15	WINDOWS 10	軟體類	作業系統	2	2	1	5	未更新或安裝作業系統	2	入侵	1	10	普	
16	WINDOWS 11	軟體類	作業系統	2	2	1	5	未更新或安裝作業系統	2	入侵	1	10	普	
17	WINDOWS SERVER 2012 R2	軟體類	作業系統	2	2	1	5	未更新或安裝作業系統	2	入侵	2	20	普	
18	OFFICE 2007	軟體類	應用系統	2	2	2	6	未更新或安裝作業系統	2	入侵	3	36	中	
19	OFFICE 2016	軟體類	應用系統	2	2	2	6	未更新或安裝作業系統	2	入侵	3	36	中	
20	OFFICE 2019	軟體類	應用系統	2	2	2	6	未更新或安裝作業系統	2	入侵	3	36	中	
21	差勤系統	軟體類	應用系統	3	2	1	6	缺少有效的型態管理控制	2	軟體程式錯誤	1	12	普	

風險評鑑工作表

單位名稱:彰化縣田尾鄉公所　　紀錄編號：112.2

資訊資產鑑別與評價								風險評鑑(評估與分析)					
No.	資產名稱	資產類別		資產價值評估				脆弱點評估		威脅評估		風險估計	
		大類	小類	機密性 (C)	完整性 (I)	可用性 (A)	合計	弱點名稱	脆弱度 (V)	威脅名稱	威脅發生機率(T)	風險值 小計	風險等級 (處理前)
22	墓政系統	軟體類	應用系統	3	2	1	6	缺少有效的型態管理控制	2	軟體程式錯誤	1	12	普
23	薪資管理資訊系統	軟體類	應用系統	3	2	1	6	缺少有效的型態管理控制	2	軟體程式錯誤	1	12	普
24	財產管理系統	軟體類	應用系統	1	2	1	4	缺少有效的型態管理控制	2	軟體程式錯誤	1	8	普
25	24port網路交換器	硬體類	網路設備	1	3	3	7	技術設施維護不恰當	3	技術失能	1	21	普
26	24port網路交換器	硬體類	網路設備	1	3	3	7	技術設施維護不恰當	3	技術失能	1	21	普
27	24port網路交換器	硬體類	網路設備	1	3	3	7	缺乏環境保護	3	技術失能	1	21	普
28	24port網路交換器	硬體類	網路設備	1	3	3	7	缺乏環境保護	3	技術失能	1	21	普
29	24port網路交換器	硬體類	網路設備	1	3	3	7	技術設施維護不恰當	3	技術失能	1	21	普
30	8port網路交換器	硬體類	網路設備	1	2	2	5	缺乏環境保護	2	技術失能	1	10	普
31	8port網路交換器	硬體類	網路設備	1	2	2	5	缺乏環境保護	2	技術失能	1	10	普
32	8port網路交換器	硬體類	網路設備	1	2	2	5	缺乏環境保護	2	技術失能	1	10	普
33	無線路由器	硬體類	網路設備	2	1	1	4	技術設施維護不恰當	1	技術失能	1	4	普
34	無線路由器	硬體類	網路設備	2	1	1	4	技術設施維護不恰當	1	技術失能	1	4	普
35	無線路由器	硬體類	網路設備	2	1	1	4	技術設施維護不恰當	1	技術失能	1	4	普
36	無線路由器	硬體類	網路設備	2	1	1	4	技術設施維護不恰當	1	技術失能	1	4	普
37	秘書室個人電腦組	硬體類	個人電腦	2	2	1	5	使用者認知不足	2	作業人員或使用者錯誤	2	20	普
38	民政課個人電腦組	硬體類	個人電腦	2	2	1	5	使用者認知不足	2	作業人員或使用者錯誤	2	20	普
39	社政課個人電腦組	硬體類	個人電腦	2	2	1	5	使用者認知不足	2	作業人員或使用者錯誤	2	20	普
40	鄉長室個人電腦組	硬體類	個人電腦	2	2	1	5	使用者認知不足	2	作業人員或使用者錯誤	2	20	普
41	財行課個人電腦組(2樓)	硬體類	個人電腦	2	2	1	5	使用者認知不足	2	作業人員或使用者錯誤	2	20	普
42	財行課個人電腦組(3樓)	硬體類	個人電腦	2	2	1	5	使用者認知不足	2	作業人員或使用者錯誤	2	20	普

風險評鑑工作表

單位名稱:彰化縣田尾鄉公所	紀錄編號：112.2

資訊資產鑑別與評價								風險評鑑(評估與分析)					
No.	資產名稱	資產類別		資產價值評估				脆弱點評估		威脅評估		風險估計	
		大類	小類	機密性 (C)	完整性 (I)	可用性 (A)	合計	弱點名稱	脆弱度 (V)	威脅名稱	威脅發生機率(T)	風險值 小計	風險等級 (處理前)
43	財行課個人電腦組(研考)	硬體類	個人電腦	2	2	2	6	使用者認知不足	2	作業人員或使用者錯誤	2	24	普
44	財行課個人電腦組(收發檔管)	硬體類	個人電腦	2	2	2	6	使用者認知不足	2	作業人員或使用者錯誤	2	24	普
45	財行課個人電腦組(會議室)	硬體類	個人電腦	1	1	1	3	使用者認知不足	1	作業人員或使用者錯誤	3	9	普
46	建設課個人電腦組	硬體類	個人電腦	2	2	1	5	使用者認知不足	2	作業人員或使用者錯誤	3	30	中
47	人事室個人電腦組	硬體類	個人電腦	3	2	1	6	使用者認知不足	2	作業人員或使用者錯誤	2	24	普
48	主計室個人電腦組	硬體類	個人電腦	2	2	1	5	使用者認知不足	2	作業人員或使用者錯誤	2	20	普
49	村幹事個人電腦組	硬體類	個人電腦	2	1	1	4	使用者認知不足	2	作業人員或使用者錯誤	2	16	普
50	政風室個人電腦組	硬體類	個人電腦	3	2	1	6	使用者認知不足	2	作業人員或使用者錯誤	2	24	普
51	秘書	人員類	編制內人員	3	3	2	8	傳輸機密資料未加適當防護	2	未授權存取資料	1	16	普
52	機要人員	人員類	編制內人員	2	3	2	7	傳輸機密資料未加適當防護	2	未授權存取資料	1	14	普
53	業務單位主管	人員類	編制內人員	2	2	2	6	傳輸機密資料未加適當防護	2	未授權存取資料	1	12	普
54	幕僚單位主管	人員類	編制內人員	2	3	2	7	傳輸機密資料未加適當防護	2	未授權存取資料	1	14	普
55	業務單位承辦人	人員類	編制內人員	2	1	2	5	使用者認知不足	2	使用者錯誤	1	10	普
56	幕僚單位承辦人	人員類	編制內人員	2	2	2	6	使用者認知不足	2	使用者錯誤	1	12	普
57	公文收發與歸檔人員	人員類	編制內人員	3	2	2	7	傳輸機密資料未加適當防護。	2	未授權存取資料	1	14	普
58	總務及研考人員	人員類	編制內人員	2	3	2	7	傳輸機密資料未加適當防護。	2	未授權存取資料	1	14	普
59	村幹事	人員類	編制內人員	2	2	1	5	使用者認知不足	2	使用者錯誤	2	20	普
60	業務單位臨時人員	人員類	臨時鐘點人員	2	1	1	4	缺少資訊諮詢的規範	1	社交工程	2	8	普

風險評鑑工作表

單位名稱:彰化縣田尾鄉公所	紀錄編號：112.2

資訊資產鑑別與評價								風險評鑑(評估與分析)					
No.	資產名稱	資產類別		資產價值評估				脆弱點評估		威脅評估		風險估計	
		大類	小類	機密性 (C)	完整性 (I)	可用性 (A)	合計	弱點名稱	脆弱度 (V)	威脅名稱	威脅發生機率(T)	風險值 小計	風險等級 (處理前)
61	幕僚單位臨時人員	人員類	臨時鐘點人員	2	1	1	4	缺少資訊諮詢的規範	1	社交工程	2	8	普
62	超鍏國際有限公司	人員類	委外廠商	2	3	2	7	未釐清委外協議的權責	2	委外作業失能	1	14	普
63	上禾資訊科技有限公司	人員類	委外廠商	1	2	3	6	未釐清委外協議的權責	2	委外作業失能	1	12	普
64	至星資訊有限公司	人員類	委外廠商	3	2	1	6	未釐清委外協議的權責	1	委外作業失能	1	6	普

資訊系統安全等級評估作業表

系統名稱	（請填全名）		
填表日期	____年____月_____日		
功能說明	（資通系統功能說明）		
系統別	□主管/上級/其他機關 □套裝軟體 □自行或委外開發		1. 主管/上級/其他機關：非本所自行架設，由上層機關維護系統→系統別為此項者，以下項目毋需填報。 2. 套裝軟體：具權限區分及管理功能之定型化軟體。 3. 自行或委外開發：由單位編列預算建構資訊系統並維護運行。
	□核心資通系統 □非核心資通系統		1. 核心系統：指支持課室核心業務持續運作必要之系統，或影響構面之安全等級(機密性、完整性、可用性、法律遵循性)有一項為「高」者，皆稱之。 2. 非核心系統：非屬前項定義之核心系統者。
影響構面	安全等級		原因說明
機密性	初估	□普 □中 □高	
	異動	□普 □中 □高	
完整性	初估	□普 □中 □高	
	異動	□普 □中 □高	
可用性	初估	□普 □中 □高	
	異動	□普 □中 □高	
法律遵循性	初估	□普 □中 □高	
	異動	□普 □中 □高	

<table>
<tr><td>項　　目</td><td>識別業務屬性</td><td colspan="3">原因說明</td></tr>
<tr><td>業 務 屬 性</td><td>□行政類
□業務類</td><td colspan="3">1. 行政類：指機關內部輔助單位之業務，如人士、薪資。
2. 業務類：指機關內部業務單位之業務，如便民服務、殯葬墓政。</td></tr>
<tr><td rowspan="4">風 險 評 鑑</td><td rowspan="4">營運衝擊分析(BIA)
(判斷 RTO 與 RPO，以降低面對損害時之作為。)</td><td>系統復原時間目標（RTO）</td><td colspan="2"></td></tr>
<tr><td>說　明</td><td colspan="2">系統復原時間目標係指判定系統中斷後，於多少時間內可恢復運作，才不會影響業務運作</td></tr>
<tr><td>資料復原時間點目標(RPO)</td><td colspan="2"></td></tr>
<tr><td>說　明</td><td colspan="2">系統備份資料週期時間長度及選定資料的範圍，例如：
(1)如果系統資料毀損，可回溯的資料是多久時間之前?
(2)備份那些資料?(資料簡略說明即可，毋須細項條列)</td></tr>
<tr><td>備註</td><td colspan="4">*系統已無使用者，前述欄位不用填，請於備註欄註明，並註記停用日期(概估即可)。(已停用，停用日期：_____年_____月_____日</td></tr>
<tr><td>承　　辦　　人</td><td>承 辦 課 室 主 管</td><td>秘　　書</td><td colspan="2">鄉長或授權代簽人</td></tr>
<tr><td></td><td></td><td></td><td colspan="2"></td></tr>
</table>

*請確認完畢後由資通系統負責人及所屬主管核章，並請繳回財行課(研考)。

*填表說明：

1、相關填表說明請參照範例。

2、系統安全等級的判定請依「資通系統防護需求分級原則」敘述，依影響機關運作程度高低進行評估，並於「原因說明」欄位敘明其判定的理由。

3、如資通系統安全等級欄位有 1 欄為「高」者，請參閱「附表十：資通系統防護基準」，檢視並自主管控資通系統是否符合其防護基準規則。

彰化縣田尾鄉公所資訊系統異動申請表

申請日期：112 年　月　日

□新進 □離職 □復職 □留職停薪_____假（**請打勾選擇異動類別**）

□調動 （原　　課室調/支援至　　課室）

項目	基本資料	請勾選申請系統
姓名		**1. 公文系統** **（網址 https://gdms.chcg.gov.tw/ ）** **□新建 □公文檔案權責移交(請續填檔案權責移交表)** **□調動(由_____課室調至_____課室)** **□權限異動（填寫權限異動需求：_____）** **□停用 □復用** **2. 電子郵件** **（網址 https://tianwei.chcg.gov.tw/）** **□新建 □復用 □停用** **3. 公所 NAS 系統** **□新建 □調動(由_____課室調至_____課室)** **□停用** **4. 電腦版 LINE 安裝：□安裝 □不安裝** **※異動說明：** **1. 新進同仁之公文系統、電子郵件、NAS 系統之帳號於本申請程序完成後由系統管理員統一給號。** **2. 新進同仁請於收到電子郵件帳號及預設密碼後自行變更密碼之後每 3 個月應變更密碼乙次。** **3. 公文系統及郵件系統於職務異動時，帳號、密碼不變。.** **4. NAS 帳密隨職務異動時一併調整。** **5. 本所人員離職時則由系統管理員設定停用。**
職稱		
課室		
分機		
***離職或異動之同仁，原存放於電腦 C 槽之資料將重新設定，請將交接檔案存放於電腦 D 槽。□是，已完成資料備份至 D 槽 □否，無交接資料** ***調、離職人員若保有『政府資料開放平臺』(cms.data.gov.tw)資料，需進行資料移交 □是，已完成資料移交 □否，未保有資料**		

申請人核章：　　課室主管核章：

本表單申請人填寫後請送交至研考以利後續流程

資訊設定人員	課長	秘書	鄉長