宜蘭縣羅東鎮公所

資通安全維護計畫

V3.2

109 年 02 月 10 日

文件制/修訂紀錄表

文件版本	修訂日期	修訂內容	修訂單位	修訂人
V1.0	107/12/27	新擬訂文件	行政室	張正熙
V2.0	108/02/25	配合宜蘭縣政府修訂	行政室	張正熙
V3.0	108/05/20	修正貳、試用範圍	行政室	張正熙
V3.1	108/10/22	內稽審查	行政室	張正熙
V3.2	109/02/10	配合行政院審查修訂	行政室	張正熙

資通安全維護計畫 V3.2

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機關〔羅東鎮公所及轄下單位（含清潔隊、圖書館、幼兒園、公有市場管理所、殯葬管理所、公用事業管理所、觀光發展所）〕。

參、核心業務及重要性

非核心業務及說明：

本機關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
電子公文交換	電子公文無法即時送達機關，影響機關行政效率。	24 小時

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：

(一)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。

(二)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。

(三)勿開啟來路不明或無法明確辨識寄件人之電子郵件。

二、 資通安全目標

(一)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。

(二)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。

(三)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

資通安全政策由資通安全長核定。

四、 資通安全政策及目標之宣導

本機關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，向機關內所有人員進行宣導。

伍、資通安全推動組織

一、 資通安全長

依本法第 11 條之規定，本機關訂定主任秘書為資通安全長，負責督導機關資通安全相關事項。

二、 資通安全推動小組

(一)組織

為推動本機關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/副主管以上之人員代表成立資通安全推動小組。

(二)分工及職掌

1.稽核組：由政風室擔任。

2.資安組：由行政室擔任資安專責人員。

陸、專責人力及經費配置

專責人力及資源之配置

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 D 級，最低應設置資通安全專責人員 1 人。

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，並提升機關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. 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。

4. 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。

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，分別為資訊資產、軟體資產、實體資產。

2. 資訊及資通系統資產項目如下：

   (1) 資訊資產：以數位等形式儲存之資訊，如資料庫、資料檔案、系統文件、操作手冊、訓練教材、研究報告、作業程序、永續運作計畫、稽核紀錄及歸檔之資訊等。

   (2) 軟體資產：應用軟體、系統軟體、開發工具、套裝軟體及電腦作業系統等。

   (3) 實體資產：電腦及通訊設備、可攜式設備及資通系統相關之設備等。

3. 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。

4. 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。

二、 機關資通安全責任等級分級

本所因自行辦理資通業務，未維運自行或委外開發之資通系統，為資通安全責任等級 D 級機關。

捌、資通安全風險評估

資通安全風險評估

1. 本所應每年針對資訊及資通系統資產進行風險評估。

2. 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。

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時，應留意其資通安全要求事項，並負對應之責任。

2. 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。

3. 非本機關同仁使用本機關之資訊及資通系統，應確實遵守本機關之相關資通安全要求，且未經授權不得任意複製資訊。

4. 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機關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。

二、 存取控制與加密機制管理

(一)網路安全控管

1. 本機關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) ：機關內部單位人員及內部伺服器使用之網路區段。

2. 外部網路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. 本機關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。

5. 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。

6. 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、特殊符號或數字二種以上。

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須經授權方能使用，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.本機關之機密資訊於儲存或傳輸時應進行加密。

2.本機關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。

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)電子郵件安全管理

本機關使用縣府電子郵件系統，依縣府相關規範辦理。

(三)確保實體與環境安全措施

辦公室區域之實體與環境安全措施：

1.機密性及敏感性資訊，不使用或下班時應該上鎖。

2.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。

3.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。

4.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。

(四)資料備份

敏感或機密性資訊之備份應加密保護。

(五)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。

(六)電腦使用之安全管理

1. 禁止私自安裝點對點檔案分享軟體及未經合法授權軟體。

2. 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。

3. 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。

4. 下班時應關閉電腦及螢幕電源。

5. 如發現資安問題，應主動循機關之通報程序通報。

6. 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。

(七)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

四、 資通安全防護設備

本所應建置防毒軟體、網路防火牆，持續使用並適時進行軟、硬體之必要更新或升級。

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，本機關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，配合宜蘭縣政府做適當之因應方式。

壹拾貳、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 D 級。

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. 員工報到時，應使其充分瞭解本機關資通安全相關作業規範及其重要性。

2. 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。

壹拾參、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，及本機關各相關規定辦理之。

壹拾肆、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，使本機關之資通安全管理有效運作，應與本機關之資通安全政策、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. 辦理稽核時，資通安全推動小組應於執行稽核前 30 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。

3. 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。

4. 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. 機關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。

4. 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。

壹拾伍、相關法規、程序及表單

一、 相關法規及參考文件

(一)資通安全管理法

(二)資通安全管理法施行細則

(三)資通安全責任等級分級辦法

(四)資通安全事件通報及應變辦法

(五)資通安全情資分享辦法

(六)公務機關所屬人員資通安全事項獎懲辦法

(七)資訊系統風險評鑑參考指引

(八)政府資訊作業委外安全參考指引

(九)無線網路安全參考指引

(十)網路架構規劃參考指引

(十一) 行政裝置資安防護參考指引

(十二) 政府行動化安全防護規劃報告

(十三) 安全軟體發展流程指引

(十四) 安全軟體設計指引

(十五) 安全軟體測試指引

(十六) 資訊作業委外安全參考指引

(十七) 本機關資通安全事件通報及應變程序

二、 附件表單

(一)資通安全推動小組成員及分工表

(二)資通安全保密同意書

(三)資通安全需求申請單

(四)管制區域人員進出登記表

(五)年度資通安全教育訓練計畫

(六)資通安全認知宣導及教育訓練簽到表

(七)資通安全維護計畫實施情形