宜蘭縣
南澳鄉公所

資通安全維護計畫

v5.0

110年07月01日

文件版本	修訂日期	修訂**內容**	修訂單位	修訂人	文件管制員
V1.0	108/01/01	新擬訂文件	行政課	蔡鼎之	秦韻
V2.0	108/02/23	配合宜蘭縣政府修訂	行政課	蔡鼎之	秦韻
V3.0	108/06/14	配合審查意見修訂	行政課	蔡鼎之	秦韻
V4.0	108/07/09	內稽審查	行政課	蔡鼎之	秦韻
V5.0	110/07/01	配合資通安全責任等級降D級修訂	秘書室	柳惠玲	秦韻

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南澳鄉公所、殯葬管理所、托兒所、圖書館、清潔隊、工程隊。

參、業務及重要性

一、本機關之非核心業務及重要性如下表：

非核心業務	重要性說明	MTPD
宜蘭縣公文管理整合系統	公文系統若發生故障則無法正常收發公文，造成服務停頓或不順，僅影響機關非核心業務執行工作效能，可能造成對資訊、資通系統之存取或使用之中斷對機關之營運、資產或信譽等方面將產生有限之影響。	10工作小時
南澳鄉公所全球資訊網： 查詢本所最新消息、一般公告等相關資訊網服務	本網站提供一般性資料瀏覽，發生資通安全事件致資通系統受影響時，可能造成對資訊、資通系統之存取或使用之中斷對機關之營運、資產或信譽等方面將產生有限之影響。	24工作小時

各欄位定義：

1.核心業務名稱：機關內的核心業務名稱。(請參考「資通安全管理法施行細則」第7條之規定列出)

2.作業名稱：該項業務內各項作業程序的名稱。

3.重要性說明：說明該業務對機關之重要性，例如對機關財務及信譽上影響，對民眾影響，對社會經濟影響，對其他機關業務運作影響，法律遵循性影響或其他重要性之說明。

4.MTPD（Maximum Tolerable Period of Disruption）：最大可容忍中斷時間。

5.參考PL-IMS-WI-05_業務持續運作計畫

肆、資通安全政策及目標

一、資通安全政策

為使本機關業務順利運作，防止資訊或資通業務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，並確保其機密

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

1.有效管理資訊資產，持續執行風險評鑑，並採取適當之防護措施。

2.保護資訊及資通業務避免受到未被授權的存取，保持資訊及資通業務的機密性。

3.確保經授權之使用者當需要時能使用資訊及資通業務。

4.符合法令與法規要求。

5.落實資通安全教育訓練，以提高員工之資通安全意識。

6.落實人員辦理業務涉及資通安全事項之獎懲機制。

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、應變及恢復作業。

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10%及2%。

(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，以避免資通業務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.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

1.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，並檢視執行成效。

2.本機關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配合宜蘭縣政府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

依本法第11條之規定，本機關訂定秘書為資通安全長，負責督導機關資通安全相關事項，其任務包括：

1.資通安全政策及目標之核定、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「宜蘭縣南澳鄉公所個人資料保護暨資通安全推動小組」(簡稱：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.個人資料保護措施之協調研議。
5.其他重要資通安全事項及個人資料保護之協調研議。

(二)分工及職掌

1.稽核分組：
(1)成員：由人事主任擔任。
(2)職責
A.訂定個人資料安全維護計畫相關之稽核計畫、執行稽核作業。（個資法細則第12條）
B.訂定資通安全維護計畫相關之稽核計畫、執行稽核作業。（資安法第7、13條、分級辦法第11條、稽核辦法）
C.其他有關個人資料保護及資通安全稽核相關業務。
2.個資與資安分組

(1)成員：由資訊人員擔任資安專責人員、人事主任擔任個資專人。
(2)資安專責人員職責
A. 執行資通安全維護計畫。（資安法第10、12條、資安法細則第6條）。
B. 執行資通安全事件通報、應變及事件調查機制。（資安法第14條、資安法細則第8條）
C. 配合宜蘭縣政府資通安全及個人資料保護內部稽核計畫，本所為受稽單位。
(2)個資專人職責
A. 當事人權利行使之處理。（個資法第10、11、13、14條）
B. 個人資料事件（被竊、洩漏、竄改或其他侵害）之查明及以適當方式通知當事人。（個資法第12條）
C. 個人資料檔案安全維護事項之執行。（個資法第18條、個資法細則第12、24條）。

3.本機關之組織分工及人員職掌應建立「**組織成員名冊**」，並適時更新之。

陸、專責人力及經費配置

一、專職(責)人力資源之配置

1.本機關依「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」。為利推展資通安全及個人資料保護工作，應設置資通安全專職人員及個資專人，其分工與職掌如「**組織成員名冊**」，人員異動應適時更新。

2.本機關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。本機關之相關單位於辦理資通安全業務時，如預判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.本機關負責重要資通業務之管理、維護、設計及操作之人員，應妥適分工，分散權責，以符職權分離原則。若負有機密維護責任者，應簽屬書面約定，並視需要實施人員輪調，以建立人力備援制度。

4.本機關之首長及各級業務主管，應督導所屬人員之資通安全作業，以防範不法及不當行為。

5.資通安全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.「推動小組」於規劃配置相關經費及資源時，應考量本機關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業務時，應一併規劃資通業務之資安防護需求，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，應配合機關預算規劃期程，向「推動小組」提出，以利依整體資通安全資源進行分配，並經資通安全長核定後，進行相關之建置事宜。

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.本機關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、服務、軟體、硬體及人員資產等五類。

2.資訊及資通系統資產類別：

(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)硬體資產：電腦及通訊設備、可攜式設備及資通業務相關之設備等。

(4)服務資產：相關基礎設施及其他機關內部之支援服務，如電力、消防等。

(5)人員資產：內部同仁、外部(常駐型)人員等。

3.本機關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**(僅資訊及資通系統需列等級)**，是否屬核心資通系統及相關資產等。

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、購買日期、型號等資訊。核心資通系統及相關資產，並應加註標示。

5.各單位管理之資訊或資通設備如有異動，應即時通知「推動小組」更新資產清冊。

二、機關資通安全責任等級分級

本所因自行辦理資訊業務，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

一、資通安全風險評估

1.本機關應每年針對資訊及資通系統資產進行風險評估。

2.本機關應每年依據「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。

玖、資通安全防護及控制措施

一、資訊及資通設備之管理

（一）資訊及資通設備之保管

1.資訊及資通設備管理人應確保資訊及資通設備已盤點造冊並適切分級，並持續更新以確保其正確性。

2.資訊及資通設備管理人應確保資訊及資通設備被妥善的保存或備份。

3.資訊及資通設備管理人應確保重要之資訊及資通設備已採取適當之存取控制政策。

(二) 資訊及資通設備之使用

1.本機關同仁使用資訊及資通設備前應經其管理人授權。

2.本機關同仁使用資訊及資通設備時，應留意其資通安全要求事項，並負對應之責任。

3.本機關同仁使用資訊及資通設備後，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.非本機關同仁使用本機關之資訊及資通設備，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。

5.對於資訊及資通設備，宜識別並以文件記錄及實作可被接受使用之規則。

(三) 資訊及資通設備之刪除或汰除

1.資訊及資通設備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設備，或該等資訊及資通設備是否已妥善移轉或備份。

2.資訊及資通設備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設備，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) ：機關內部單位人員使。
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.使用者應依縣府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) 資通業務權限管理

1.本機關之資通設備應設置通行碼管理，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、特殊符號或數字兩種以上。
(3)使用者每90天應更換一次通行碼。
2.使用者使用資通設備前應經授權，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設備時，應立即停用或移除使用者ID，資通設備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.資通設備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.資通設備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.資通設備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.資通設備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.本機關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) 電子郵件安全管理

本機關使用縣府電子郵件系統，依縣府相關規定辦理。

(三) 確保實體與環境安全措施

1.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業務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設備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)資訊或資通業務相關設備，未經管理人授權，不得被帶離辦公室。

(四) 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。

(五) 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，應主動循機關之通報程序通報。
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。

(六) 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

(七) 即時通訊軟體之安全管理

1.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。
2.使用於傳遞公務訊息之即時通訊軟體應具備下列安全性需求：
(1)用戶端應有身分識別及認證機制。
(2)伺服器通訊紀錄（log）應至少保存六個月。

四、資通安全防護設備

1.本機關應建置防毒軟體、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

本機關接獲資通安全情資，應評估該情資之內容，並視其對本機關之影響、可用資源及可接受之風險等，決定以最適當之方式因應，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

本機關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：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，均屬之。

(二)入侵攻擊情資

資通安全情資之內容，如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，列屬入侵攻擊情資。

(三)機敏性之情資

資通安全情資之內容，如：姓名、出生年月日、國民身份證統一編號、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，屬機敏性之情資，應以遮蔽或刪除之方式排除特定區段或文字，或採取去識別化之方式排除之。

(四)涉及核心業務、核心資通業務之情資

資通安全情資之內容，如：機關內部之核心業務資訊、核心資通業務、涉及關鍵基礎設施維運之核心業務或核心資通業務之運作等，屬涉及核心業務、核心資通業務之情資。

二、資通安全情資之因應措施

本機關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)資通安全相關訊息之情資

由「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)入侵攻擊之情資

由資通安全專職(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，另應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、核心資通業務之情資

「推動小組」應就涉及核心業務、核心資通業務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、資通業務或服務委外辦理之管理

本機關若有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.受託者應考量辦理受託業務得否複委託？複委託之範圍與對象？以及複委託之受託者所應具備之資通安全維護措施等。

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，應標示非自行開發之內容、來源，以及提供授權證明。

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，應即通知委託機關並採行之補救措施。

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.本機關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~~安全維護~~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.本機關資通安全責任等級分級屬「D級」。

2.本機關之一般使用者與主管，每人每年至少接受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

本機關所屬人員之平時考核或聘用，依宜蘭縣政府所訂「**宜蘭縣政府及所屬人員辦理資通安全事項獎懲標準表**」辦理。

壹拾伍、資通安全維護計畫及實施情形之持續精進與績效管理機制

一、資通安全維護計畫之實施

為落實本安全維護計畫，確保本機關之資通安全管理有效運作，相關單位於訂定各階程序文件、流程或控制措施時，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.本機關依循「推動小組」應定期(配合縣政府)，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，以確保資通安全維護計畫有效運作。
2.配合縣府「推動小組」應於辦理稽核前擬定資通安全稽核計畫並選派稽核成員。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（查檢表）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.配合縣府「推動小組」辦理稽核時，「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、稽核查檢表及稽核排程等相關資訊提供受稽單位。
4.本機關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；如有聘任稽核委員應填具「壹拾柒、程序及表單所列表單編號及名稱」備查，另於執行稽核時，應依稽核查檢表填具稽核紀錄或工作底稿，待稽核結束後，應將稽核發現彙整至稽核報告，並提供給受稽單位採取矯正預防措施，以持續改善。
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。

(二)稽核改善報告

1.本機關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、規劃改善進度，並加以落實。
2.本機關於稽核實施後發現有缺失或待改善事項，應分析其發生之原因，並評估是否有類似、潛在之缺失，以及可能之待改善項目。
3.本機關於找出缺失或待改善之原因後，應據此提出並矯正及（或或）預防措施，以及改善進度規劃，必要時得修訂本維護計畫或對相關文件進行變更。
4.機關應定期審查受稽單位缺失或待改善項目所採取之矯正預防措施、改善進度規劃及佐證資料之有效性。
5.本機關於執行矯正預防措施時，應留存相關之執行紀錄，並依填寫矯正措施表並檢附相關佐證資料。

三、資通安全維護計畫之持續精進及績效管理

1.本機關配合縣府「推動小組」應於每年12月底前(每年至少一次)召開資通安全管理審查會議，以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)過往管理審查之處理狀態。

(2)與資訊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、「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)資訊安全績效之回饋，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。

3.持續改善機制之管理審查相關執行紀錄並應予保存，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

本機關依據資通安全管理法第12條之規定，每年應依主管機關來函限期內，提出資通安全維護計畫實施情形，使其得瞭解本機關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.資訊系統風險評鑑參考指引

7.政府資訊作業委外安全參考指引

8.無線網路安全參考指引

9.網路架構規劃參考指引

10.行政裝置資安防護參考指引

11.政府行動化安全防護規劃報告

12.安全軟體發展流程指引

13.安全軟體設計指引

14.安全軟體測試指引

15.資訊作業委外安全參考指引

16.本機關資通安全事件通報及應變程序

二、附件表單

1.資通安全組織成員名冊

2.保密同意書

3.資通安全需求申請單

4.管制區域人員進出登記表

5.資通安全維護計畫實施情形自我審查表