

金門縣烈嶼鄉民代表會
資通安全維護計畫

修訂日期：中華民國 112 年 1 月 1 日

目 錄

壹、依據及目的	3
貳、適用範圍	3
參、核心業務及重要性	3
肆、資通安全政策及目標	3
一、資通安全政策.....	3
二、資通安全目標.....	4
三、資通安全政策及目標之核定程序.....	4
四、資通安全政策及目標之宣導.....	4
五、資通安全政策及目標定期檢討程序.....	4
伍、資通安全推動組織	4
一、資通安全長.....	4
二、資通安全推動小組.....	5
陸、專責人力及經費配置	6
一、專責人力及資源之配置.....	6
二、經費之配置.....	6
柒、資訊及資通系統之盤點	6
一、資訊及資通系統盤點.....	6
二、機關資通安全責任等級分級.....	7
捌、資通安全風險評估	7
一、資通安全風險評估.....	7
玖、資通安全防護及控制措施	8
一、資訊及資通系統之管理.....	7
二、存取控制與加密機制管理.....	9
三、作業與通訊安全管理.....	10
四、資通安全防護設備.....	12
壹拾、資通安全事件通報、應變及演練相關機制	13
壹拾壹、資通安全情資之評估及因應	13

一、資通安全情資之分類評估.....	13
二、資通安全情資之因應措施.....	14
壹拾貳、資通系統或服務委外辦理之管理	14
一、選任受託者應注意事項.....	15
二、監督受託者資通安全維護情形應注意事項.....	15
壹拾參、資通安全教育訓練	16
一、資通安全教育訓練要求.....	16
二、資通安全教育訓練辦理方式.....	16
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	16
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	16
一、資通安全維護計畫之實施.....	16
二、資通安全維護計畫實施情形之稽核機制.....	16
壹拾陸、資通安全維護計畫實施情形之提出	18
壹拾柒、相關法規及程序及參考	18

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會。

參、核心業務及重要性

- 一、依地方制度法規定召開定期會與臨時會，代表針對民眾反映與興革建議事項提請公所改善。
- 二、議決鄉規約、議決鄉預算、議決鄉臨時稅課、議決鄉財產之處分、議決鄉（鎮、市）公所組織自治條例及所屬事業機構組織自治條例、議決鄉公所提案事項、審議鄉（鎮、市）決算報告、議決鄉（鎮、市）民代表提案事項、接受人民請願、其他依法律或上級法規、規章賦予之職權。

肆、資通安全政策及目標

資通安全政策訂定及核定、資通安全目標之訂定、資通安全政策及目標宣導及目標定期檢視。

一、資通安全政策

為使本會業務順利運作，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，確保機關業務持續營運。
4. 應因應資通安全威脅情勢變化，辦理資通安全教育訓練，以提高本會同仁之資通安全意識，本機關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。

二、資通安全目標：知悉資安事件發生，規定時間內完成通報應變。

(一) 量化型目標

1. 本機關同仁每年資訊安全教育訓練三小時以上。
2. 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。
3. 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%。

(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. 提升人員資安防護意識、有效偵測與預防外部攻擊等。

三、資通安全政策及目標之核定程序

資通安全政策由本會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，本會訂定單位長官秘書為資通安全長，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項業務人員代表成立資通安全推動小組，其任務包括：

1. 跨組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

本會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，本機關資通安全推動小組分組人員名單及職掌應列冊，並適時更新之：

1. 策略規劃組：

- (1) 資通安全政策及目標之研議。
- (2) 訂定本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本會年度工作計畫。
- (4) 傳達機關資通安全政策與目標。
- (5) 其他資通安全事項之規劃。

2. 資安防護組：

- (1) 資通安全技術之研究、建置及評估相關事項。
- (2) 資通安全相關規章與程序、制度之執行。
- (3) 資訊及資通系統之盤點及風險評估。
- (4) 資料及資通系統之安全防護事項之執行。
- (5) 資通安全事件之通報及應變機制之執行。
- (6) 其他資通安全事項之辦理與推動。

3. 績效管理組：

- (1) 辦理資通安全內部稽核。
- (2) 每半年(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、專責人力及經費配置

一、專責人力及資源之配置

本會資安等級為 D 級，依規定無須配置專責人員。

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，應考量本會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. 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. 本會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、支援服務資產等。
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。
 - (4) 支援服務資產：相關基礎設施級其他機關內部之支援服務，如電力、消防等。
3. 本會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。
5. 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

本會因無資通系統且未提供資通服務為資通安全責任等級 D 級。

捌、資通安全風險評估

一、資通安全風險評估

1. 本會應每年針對資訊及資通系統資產進行風險評估。

2. 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。
3. 本會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. 本會同仁使用資訊及資通系統前應經其管理人授權。
2. 本會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. 本會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. 非本會同仁使用本機關之資訊及資通系統，應確實遵守本會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。並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。
2. 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. 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。
2. 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。
3. 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。
4. 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。
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. 網域名稱系統(DNS)防護。
7. 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。

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

1. 本會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. 使用者不得利用機關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。

(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。

(四) 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. 本機關應每季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。

(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。
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。

(六) 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。

(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

(八) 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) 訊息於傳輸過程應有安全加密機制。
 - (3) 應通過經濟部工業局訂定行動化應用軟體之中級檢測項目。
 - (4) 伺服器端之主機設備及通訊紀錄應置於我國境內。
 - (5) 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

本會接獲資通安全情資，應評估該情資之內容，並視其對本會之影響、本會可接受之風險及本會之資源，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

本會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機關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。

(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

本機關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。
4. 受託業務涉及國家機密者，應考量受託業務所涉及國家機密之機密等級內容，於招標公告、招標文件及契約中，註明受託者辦理該項業務人員及可能接觸該國家機密人員應接受適任性查核，並依國家機密保護法之規定，管制其出境。
5. 前點適任性查核得在必要範圍內就下列事項查核，查核前應經當事人書面同意：
 - (1) 曾犯洩密罪，或於動員戡亂時期終止後，犯內亂罪、外患罪，經判刑確定，或通緝有案尚未結案者。
 - (2) 曾任公務人員因違反相關安全保密規定，受懲戒處分、記過以上行政懲處者。
 - (3) 曾受到外國政府、大陸地區或香港、澳門官方之利誘、脅迫，從事不利國家安全或重大利益情事者。
 - (4) 其他與國家機密保護相關之具體項目。

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. 本機關依資通安全責任等級分級屬 D 級，資安及資訊人員每年至少 1 名人員資安專業課程訓練或資安職能訓練。
2. 本會之一般使用者與主管，每人每年接受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，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紀錄。
2. 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。

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

本會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，使本機關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. 本會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. 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。
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. 本機關之資通安全推動小組應於每年至少一次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¹，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

本機關依據本法第 11(16,17)條之規定，向金門縣政府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