

連江縣南竿鄉公所

109 年資通安全維護計畫 書

目錄

壹、依據及目的.....	4
貳、適用範圍.....	4
參、核心業務及重要性.....	4
一、核心業務及重要性.....	4
二、非核心業務及說明.....	5
肆、資通安全政策及目標.....	6
一、資通安全政策.....	6
二、資通安全目標.....	6
三、資通安全政策及目標之核定程序.....	7
四、資通安全政策及目標之宣導.....	7
五、資通安全政策及目標定期檢討程序.....	7
伍、資通安全推動組織.....	7
一、資通安全長.....	7
二、資通安全推動小組.....	7
陸、專責人力及經費配置.....	9
一、專職(責)人力資源之配置.....	9
二、經費之配置.....	9
柒、資訊及資通系統之盤點.....	10
一、資訊及資通系統盤點.....	10
二、機關資通安全責任等級分級.....	11
捌、資通安全風險評估.....	11
一、資通安全風險評估.....	11
二、核心資通系統及最大可容忍中斷時間.....	11
玖、資通安全防護及控制措施.....	11
一、資通系統權限管理.....	11
二、特權帳號之存取管理.....	12
三、加密管理.....	12
四、作業與通訊安全管理.....	12
五、確保實體與環境安全措施.....	13
六、資料備份.....	14
七、媒體防護措施.....	15
八、電腦使用之安全管理.....	15
九、行動設備之安全管理.....	15
十、即時通訊軟體之安全管理.....	16
十一、業務持續運作演練.....	16
十二、執行資通安全健診.....	16
十三、資通安全防護設備.....	16
十四、系統獲取、開發及維護.....	16
壹拾、資通安全事件通報、應變及演練相關機制.....	17
壹拾壹、資通安全情資之評估及因應.....	17
一、資通安全情資之分類評估.....	17

二、資通安全情資之因應措施	18
壹拾貳、資通系統或服務委外辦理之管理	18
一、選任受託者應注意事項	19
二、監督受託者資通安全維護情形應注意事項.....	19
壹拾參、資通安全教育訓練.....	19
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	20
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	20
一、資通安全維護計畫之實施	20
二、資通安全維護計畫實施情形之稽核機制.....	20
壹拾陸、相關法規、程序及表單.....	21

連江縣南竿鄉公所資通安全維護計畫

壹、依據及目的

一：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。

二：本計畫依據下列法規訂定：

- 一、資通安全管理法第 10 條及其施行細則第 6 條。
- 二、其他業務法規名稱。

貳、適用範圍

本計畫適用範圍涵蓋本所、本所各村辦公處。

參、核心業務及重要性

一、核心業務及重要性

本所之核心業務及重要性如下表：

核心業務	核心資通系統	重要性說明	業務失效影響說明	最大可容忍中斷時間
文書檔案	連江縣公文整合資訊系統	提供電子化公文即時送達機關單位，提升行政效率。	本項目因故致中斷，將可能導致各項電子化公文行政業務運作，降低行政效率，但仍能傳統公文書面形式替代並達成行政目的。	8 小時

各欄位定義：

1. 核心業務名稱：請參考資通安全管理法施行細則第 7 條之規定列示。
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. 最大可容忍中斷時間單位以小時計。

二、非核心業務及說明

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
差勤服務	差勤系統無法使用時，影響機關行政效率。	24 小時
其他	機關其他非屬上開範疇之業務	48 小時
衛生福利社政相關系統	衛生福利社政相關系統無法使用時，影響機關行政效率。	10 小時
庶務	財產管理系統，若因故致系統中斷影響財產及物品管理。惟仍能調閱建入系統前之留存紙本或相關記錄，作為辦理依據達成業務目的。	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：

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。

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%。

（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

資通安全政策由本所資通安全長核定。

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，向機關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

依本法第11條之規定，本所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「連江縣南竿鄉公所個人資料保護暨資通安全推動小組」(簡稱：本小

組)，本小組成員由本所行政課、民政課、社會課、財經課、環保課等各課主管擔任。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. 個資稽核組：

(1) 成員：由人事管理員擔任。

(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. 資通維護組

(1) 成員：由事務管理人員擔任資安專責人員、人事管理員擔任個資專員。

(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. 協助資通安全長綜理本小組有關業務，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。

(3) 個資專員職責

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。
 - 4. 預計於今年5-6月召開資通安全審查會議。

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「C級」。為利推展資通安全及個人資料保護工作，應設置資通安全專責人員及個資專人，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系統之管理、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系統時，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、軟體、實體及支援服務資產等四類。
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) 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：相關基礎設施及其他機關內部之支援服務，如電力、消防等。
2. 資訊及資通系統應界定其可容忍之故障發生至修復正常運轉所需時間 (Recovery Time Object, RTO) 及復原之時間點 (Recovery Point Object, RPO)。(分級辦法附表中僅要求針對核心資通系統進行營運持續演練，惟判定資通安全事件等級時，仍需判斷非核心資通系統可容忍中斷時間，故要求在資訊及資通系統盤點後，應即訂出資通系統之RTO及RPO)。
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、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. 各單位管理之資訊或資通系統如有異動，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

本所因有維運自行或委外開發之資通系統者，其資通安全責任等級為C級。

捌、資通安全風險評估

一、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. 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。

二、核心資通系統及最大可容忍中斷時間

核心資通系統	資訊資產	最大可容忍中斷時間	核心資通系統主要功能
連江縣公文整合資訊系統	由縣府統一管理硬體及軟體	24 小時	相關文書檔案業務

最大可容忍中斷時間以小時計。

玖、資通安全防護及控制措施

一、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。

二、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。

三、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。

四、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. 使用者不得私自使用已知或有嫌疑惡意之網站。
 3. 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

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。

(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。
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。

五、確保實體與環境安全措施

1. 監視器系統及網路機房之門禁管理

- (1) 監視器系統及網路機房應進行人員進出管控。
- (2) 監視器系統及網路機房進入之鑰匙由資安專責人員保管

2. 監視器系統及網路機房之環境控制

- (1) 監視器系統及網路機房之空調、電力應建立備援措施。
- (2) 監視器系統及網路機房之溫度管控範圍為：26-28度。
- (3) 監視器系統及網路機房應安裝之安全偵測及防護措施，包括火災警報設備、溫濕度監控設備、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
- (3) 機密性及敏感性資訊，不使用或下班時應該上鎖。內。
- (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。

六、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。

七、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。

八、電腦使用之安全管理

1. 電腦、業務系統或自然人憑證，若超過三十分鐘不使用時，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，如無特殊需求，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。

九、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

十、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。

十一、業務持續運作演練

本所應針對核心資通系統制定業務持續運作計畫，並每二年辦理一次核心資通系統持續運作演練。

十二、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。

十三、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。

十四、系統獲取、開發及維護

1. 本機關之資通系統應依「資通安全責任等級分級辦法」附表九之規定完成系統防護需求分級，依分級之結果，完成附表十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，

24
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所之資源，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，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。

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。

壹拾叁、資通安全教育訓練

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。
 - (1) 資通安全法令規定。
 - (2) 資通安全作業內容。
 - (3) 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. 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。
2. 稽核結果應對相關管理階層報告，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。
3. 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。

壹拾陸、相關法規、程序及表單

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