

宜蘭縣  
蘇澳鎮公所

資通安全維護計畫

v3.21

111年8月2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
一、核心業務及說明：.....	3
二、非核心業務及說明：.....	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.....	3
三、資通安全政策及目標之核定程序.....	3
伍、資通安全推動組織.....	4
陸、專責人力及經費配置.....	5
一、專責人力及資源之配置.....	5
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.....	6
捌、資通安全風險評估.....	6
玖、資通防護及控制措施.....	6
一、資訊及資通設備之管理.....	6
二、存取控制與加密機制管理.....	7
三、作業與通訊安全管理.....	9
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.....	12
壹拾壹、資通安全情資之評估及因應.....	12
一、資通安全情資之分類評估.....	12
二、資通安全情資之因應措施.....	13
壹拾貳、資通系統或服務委外辦理之管理.....	13
一、選任受託者應注意事項.....	13
二、監督受託者資通安全維護情形應注意事項.....	13
壹拾參、資通安全教育訓練.....	13
一、資通安全教育訓練要求.....	13
二、資通安全教育訓練辦理方式.....	13
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.....	14
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.....	14
一、資通安全維護計畫之實施.....	14
二、資通安全維護計畫實施情形之稽核機制.....	14

三、資通安全維護計畫之持續精進及績效管理.....	16
壹拾陸、資通安全維護計畫實施情形之提出.....	17
壹拾柒、相關法規、程序及表單.....	17
一、相關法規及參考文件.....	17
二、附件表單.....	17

## 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(以下簡稱本所)含本所各附屬單位。

## 參、核心業務及重要性

核心業務及說明：

核心業務	業務影響說明	提供單位	最大可容忍中斷時間
ECPA人事服務網、生活廢棄物質管理資訊系統、全國糧政跨區即時申辦服務作業平台、全國幼兒園幼生管理系統、全國身心障礙福利資訊整合平台	系統異常，影響機關行政效率	上級	24 小時

非核心業務及說明：

非核心業務	業務影響說明	提供單位	最大可容忍中斷時間
公文系統、差勤系統、員工業務網	系統異常，影響機關行政效率	上級	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，防止資訊或資通業務受未經授權之存取、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)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。

(二)針對各資料的機密性與完整性應妥善保護，避免資料遭竄改。

- (三)建立資通安全防護(如:防火牆、防毒軟體)。
- (四)辦理資通安全教育訓練(一般使用者與主管，每人每年三小時以上之一般資通安全教育訓練或自行取得線上學習相關認證三小時以上)，提升同仁資通安全意識。
- (五)禁止多人共用同一帳號。
- (六)落實資通安全通報機制。

## 二、資通安全目標

- (一)資安事件發生，於規定的時間完成通報、應變及復原作業。
- (二)全年度資安通報平臺之資安事件等級第1、2級發生件數少於3件(含)以下，等級第3、4級不得發生。
- (三)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、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。

## 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，其任務包括：

- (一)資通安全管理政策及目標之核定、核轉及督導。
- (二)資通安全責任之分配及協調。
- (三)資通安全資源分配。
- (四)資通安全防護措施之監督。
- (五)資通安全事件之檢討及監督。
- (六)資通安全相關規章與程序、制度文件核定。
- (七)資通安全管理年度工作計畫之核定
- (八)資通安全相關工作事項督導及績效管理。
- (九)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課室成立資通安全推動小組，其任務包括：

1. 本所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)分工及職掌本機關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組別內容，並適時更新之：
1. 人員名單：主任秘書(資通安全長)、所內各課室主管、研考課員、本所資訊人員。
  2. 策略規劃：
    - (1)資通安全政策及目標之研議。
    - (2)訂定機關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機關年度工作計畫。
    - (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。
  3. 資安防護：
    - (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。
  4. 績效管理組：
    - (1)配合宜蘭縣政府每年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)每年至少召開乙次以上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

- (一)依本法第 11 條之規定，本機關訂定副首長為資通安全長。
- (二)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。
- (三)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。
- (四)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。
- (五)專業人力資源之配置情形應每年檢討，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

- (一)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。
- (二)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。
- (三)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資通安全推動小組提出，由資通安全推動小組視整體資通安全資源進行分配，並經資通安全管理會議核定後，進行相關之建置。
- (四)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

- (一)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。
- (二)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：本所核心及非核心業務皆使用上級提供之軟體；無自行開發。
  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。
- (三)本所每年度應依資訊及資通系統盤點配合「神網電腦終端防護系統」輔助製作「電腦資產明細表」，欄位應包含：電腦基本資訊資訊及電腦名稱(使用者)、硬體內容。
- (四)資訊及資通系統資產應以標籤標示於設備明顯處，並載明財產分類編號、購買日期。

### 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、本所應每年針對資訊及資通系統資產進行風險評估。
- 二、本所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、資訊及資通設備之管理

#### (一) 資訊及資通設備之使用

1. 本所同仁使用資訊及資通設備須遵守宜蘭縣政府個人電腦資訊安全內部稽核自我審查表規範。
2. 本所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. 本所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. 非本所同仁使用本機關之資訊及資通設備，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。

#### (二) 存取控制與加密機制管理

1. 網路安全控管。
2. 本機關之防火牆由本機關自行管理，區域劃分如下：
  - (1) 外部網路：對外網路區域，連接外部廣網路 (WideAreaNetwork, WAN)。
  - (2) 內部區域網路 (LocalAreaNetwork, LAN)：機關內部單位人員使用。
  - (3) 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。
  - (4) 本機關應定期檢視防火牆政策是否適當。
  - (5) 使用者應依縣府規定之方式存取網路服務。
  - (6) 網路安全控管。
3. 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：依據宜蘭縣政府個人電腦資訊安全內部稽核規範辦理辦理。

(一)資通業務權限管理

1. 資訊及資通系統之使用

- (1)本機關同仁使用資訊及資通設備須遵守設備管理相關規範。
- (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。
- (6)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。
- (7)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。

2. 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

1. 網路安全控管

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(WideAreaNetwork, WAN)。
- (2)內部區域網路(LocalAreaNetwork, LAN)：機關內部單位人員及內部伺服器使用之網路區段。
- (3)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。
- (4)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。

- (5)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。
- (6)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。

## 2. 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)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。
  - (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。

## (四)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。

## (五)加密管理

1. 本機關之電腦皆應設 8 位數中英文混合開機密碼；電腦螢幕逾時十分鐘啟動螢幕保護裝置。

2. 本機關之機密資訊於儲存或傳輸時應進行加密。
3. 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，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. 績效管理組應定期清查已授權之遠距工作需求是否適當。

#### (三) 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。」

#### (四) 確保實體與環境安全措施

1. 電腦機房之門禁管理
  - (1) 電腦機房應進行實體隔離。
  - (2) 機關人員或來訪人員應申請及授權後方可進入電腦機房。
  - (3) 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。
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) 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. 各單位承辦人重要資料自行備份；如有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. 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、行動硬碟或光片等存放資料時，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資料，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. 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。

#### (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

#### (九)即時通訊軟體之安全管理

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

(一)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。

(二)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；並配合宜蘭縣政府每年辦理資通安全演練相關機制，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，並視其對本機關之影響、本機關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。

##### 1. 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。

##### 2. 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。

## 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

本所目前無委外辦理資通系統之建置、維運或資通服務；如有需求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

(一)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。

(二)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。

(三)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

- (一)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。
- (二)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。
- (三)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。
- (四)受託者應採取之其他資通安全相關維護措施。
- (五)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

- (一)本所依資通安全責任等級分級屬D級。
- (二)本所之一般使用者與主管，每人每年接受 3 小時以上或自行線上學習並取得三小時以上相關課程之一般資通安全教育訓練。

### 二、資通安全教育訓練辦理方式

- (一)考量管理、業務及資訊等不同工作類別之需求，評估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。
- (二)本機關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。
- (三)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。
- (四)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(配合政風室，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. 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

(一). 本機關之「推動小組」應於每年年底前(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。

(二). 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。
  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。
- (三). 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（參考「維護計畫表單 47-改善績效追蹤報告」格式），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，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

- (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)資訊系統風險評鑑參考指引
- (七)政府資訊作業委外安全參考指引
- (八)無線網路安全參考指引
- (九)網路架構規劃參考指引
- (十)行政裝置資安防護參考指引
- (十一)政府行動化安全防護規劃報告
- (十二)安全軟體發展流程指引
- (十三)安全軟體設計指引
- (十四)安全軟體測試指引
- (十五)資訊作業委外安全參考指引
- (十六)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
- (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)資通安全維護計畫實施情形自我審查表