107年12月22日高市法局秘字第10730963500號函簽准訂定 版本號：1.0

113年1月15日高市法局秘字第11330074500號函簽准訂定 版本號：2.0

113年8月29日高市法局秘字第11330653400號函簽准訂定 版本號：2.1

114年11月5日高市法局秘字第11430846000號函簽准訂定 版本號：2.2

高雄市政府法制局
資通安全維護計畫

發行日期：114年11月5日

資通安全維護計畫

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、非核心資通系統及說明： 4
肆、資通安全政策及目標 5
一、資通安全政策 5
二、資通安全目標 5
三、資通安全政策及目標之核定程序 5
四、資通安全政策及目標之宣導 5
五、資通安全政策及目標定期檢討程序 6
伍、資通安全推動組織 6
一、資通安全長 6
二、資通安全推動小組 6
陸、專職人力及經費配置 7
一、專職人力及資源之配置 7
二、經費之配置 8
柒、資訊及資通系統之盤點 8
一、資訊及資通系統盤點 8
二、機關資通安全責任等級分級 8
捌、資通安全風險評估 9
一、資通安全風險評估 9
二、核心資通系統及最大可容忍中斷時間 9
玖、資通安全防護及控制措施 9
一、資訊及資通系統之管理 9
二、存取控制與加密機制管理 10

三、作業與通訊安全管理 12
四、系統獲取、開發及維護 16
拾、資通安全事件通報、應變及演練相關機制 16
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 17
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 18
二、監督受託者資通安全維護情形應注意事項 18
拾參、資通安全教育訓練 19
一、資通安全教育訓練要求 19
二、資通安全教育訓練辦理方式 19
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 19
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
拾陸、資通安全維護計畫實施情形之提出 21
拾柒、相關法規 21

壹、依據及目的

本計畫依據下列法規訂定：

一、 資通安全管理法第10條及施行細則第6條。

二、 高雄市政府法制局組織規程。

貳、適用範圍

本計畫適用範圍涵蓋高雄市政府法制局（以下簡稱本局）全機關。

參、核心業務及重要性

一、核心業務及重要性：

本局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
訴願審議	無	為本局依組織法執掌，足認為重要者。	影響人民提起訴願之權利及機關信譽。	不適用
國家賠償審議	無	為本局依組織法執掌，足認為重要者。	影響人民申請國家賠償之權利及機關信譽。	不適用
法規審查	無	為本局依組織法執掌，足認為重要者。	影響各局處法規研擬、解釋、審議及諮詢等法制事項。	不適用
法制行政業務	無	為本局依組織法執掌，足認為重要者。	影響本局法制行政業務運作。	不適用

二、非核心資通系統及說明：

本局之非核心資通系統及說明如下表：

非核心資通系統	業務失效影響說明	最大可容忍中斷時間
本局官網	民眾無法查詢本局官網相關資料，影響本局為民服務。	24 小時
法制資料服務中心	影響本局同仁登錄、查詢或檢索訴願、國家賠償及各局處會簽會辦案	72 小時以上

	件。	

肆、資通安全政策及目標

一、資通安全政策

為使本局業務順利運作，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，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)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)因應資通安全威脅情勢變化，辦理資通安全教育訓練，以提高本局同仁之資通安全意識，本局同仁亦應確實參與訓練。

(三)針對辦理資通安全業務有功人員應進行獎勵。

(四)勿開啟來路不明或無法明確辨識寄件人之電子郵件。

(五)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，能於規定時間內完成通報、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，以確保資通系統或資訊之機密性、完整性及可用性。
2. 達成資通安全責任等級分級之要求，以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

由本局秘書室簽陳資通安全長核定。

四、資通安全政策及目標之宣導

每年透過教育訓練、內部會議、電子郵件等方式，向本局所有人員進行宣導。

五、資通安全政策及目標定期檢討程序

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，本局訂定副局長為資通安全長，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

為推動本局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成立資通安全推動小組，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.其他重要資通安全事項之協調研議。

(二)職掌

本局之資通安全推動小組依資通安全長之指示負責下列事項，名單應列冊，並適時更新：

1.研議並傳達本局資通安全政策及目標。

2. 訂定並執行本局資通安全相關規章與程序、制度，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局年度工作計畫。

4. 資訊及資通系統之盤點及風險評估。

5. 資料及資通系統之安全防護事項之執行。

6. 資通安全事件之通報及應變機制之執行。

7. 辦理資通安全內部稽核。

8. 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。

9. 其他資通安全事項之規劃、辦理與推動。

陸、專職人力及經費配置

一、專職人力及資源之配置

(一)本局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，最低應設置資通安全專職人員１人，其工作如下，本局現有資通安全專職人員名單及職掌應列冊，並適時更新。

1. 管理面業務，負責資通系統分級及防護基準、資訊安全管理系統之導入、內部資通安全稽核及業務持續運作演練等業務之推動。

2. 技術面業務，負責安全性檢測、資通安全健診、資通安全弱點通報機制之導入及資通安全防護等業務之推動。

3. 認知與訓練業務，負責資通安全教育訓練業務之推動，並取得資通安全專業證照及職能訓練證書各一張以上。

(二)本局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。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。

(三)本局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，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，建立人力備援制度。

(四)本局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

(一)資通安全推動小組於規劃配置相關經費及資源時，應考量本局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)資通安全經費、資源之配置情形每年定期檢討，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)本局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、實體資產等。

(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、作業程序、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：電腦硬體(含虛擬機)及通訊設備、可攜式設備及資通系統相關之設備等。

(三)本局每年度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」，欄位包含：資產名稱、資產類別、擁有者(負責人)、管理者(保管人)、使用者、存放位置、防護需求等級。

(四)資訊及資通系統資產以標籤標示於設備明顯處，並載明財產編號、保管人、規格等資訊。

二、機關資通安全責任等級分級

本局維運委外設置、開發之資通系統，為資通安全責任等級C

級機關。

捌、資通安全風險評估

一、資通安全風險評估

(一)每年針對資訊及資通系統資產進行風險評估。

(二)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」，並依資通安全維護計畫附件中之風險評鑑方式進行風險評估之工作。

(三)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

本局無核心資通系統。

玖、資通安全防護及控制措施

本局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、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。
4. 資訊及資通系統之日誌保存期限應達6個月。

(二)資訊及資通系統之使用

1. 本局同仁使用資訊及資通系統前應經其管理人授權。
2. 本局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. 本局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. 非本局同仁使用本局之資訊及資通系統，應確實遵守本局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)資訊及資通系統之維修

1. 資訊及資通系統委由外部廠商維修時，相關儲存裝置(如：硬碟、隨身碟等)不得直接攜出，應卸除保管於本局管理範圍內或先將裝置執行格式化，避免資訊遭外部人員取得。(加連同硬碟攜出需簽保密切結)。

(四)資訊及資通系統之刪除或汰除

2. 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。

3. 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。

4. 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. 本局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) 非軍事區(DMZ)：放置本局對外服務伺服器之區段。

(3) 內部區域網路 (Local Area Network, LAN) ：本局內部單位人員及內部伺服器使用之網路區段。

2. 外部網路、非軍事區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. 本局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. 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。

5. 網域名稱系統(DNS)防護

(1) 一般伺服器應關閉 DNS 服務，防火牆政策亦應針對 DNS 進行控管，關閉不需要的 DNS 服務存取。

(2) DNS 伺服器應經常性進行弱點漏洞管理與修補、落實存取管控機制。

(3) DNS 伺服器應設定指向 GSN Cache DNS。

(4) 內部主機位置查詢應指向機關內部 DNS 伺服器。

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。

7. 資通安全弱點通報機制（VANS）作業

(1) 本局應配合市府資訊中心導入資通安全弱點通報機制，並完成平台填報與管理、弱點改善（如：作業系統安全性更新、套裝軟體安裝或版本升級與更新）等工作。

(2) VANS系統管理員應每個月定期上傳1次資訊資產盤點資料，針對高風險以上之弱點，應於一週內至VANS系統填寫相關弱點處置方式。

(3) VANS系統管理員每月完成弱點處置後，查核人員應於當月查核資訊資產盤點資料及高風險以上之弱點處理情形。

(二)資通系統權限管理

1. 本局之資通系統應設置密碼管理，密碼之要求需滿足：

(1) 密碼長度 12 碼以上。

(2) 密碼複雜度應包含英文大寫小寫、特殊符號及數字三種以上。

(3)使用者每 90 天應更換一次密碼。

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。

(三)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。

(四)加密管理

1. 本局之機密資訊於儲存或傳輸時應進行加密。

2. 本局之加密保護措施應遵守下列規定：

(1)避免留存解密資訊。

(2)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. 本局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，管理者並應每年定

期針對管理之設備進行軟體抽查。

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. 本局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. 資通安全推動小組應定期審查已授權之遠距工作需求是否適當。

3. 針對遠距工作之連線應採適當之防護措施(並包含伺服器端之集中過濾機制檢查使用者之授權)，並且記錄其登入情形。

4. 提供適當通訊設備，並指定含有加密機制的遠端存取方式。

5. 提供虛擬桌面存取，以防止於私有設備上處理及儲存資訊。

6. 進行遠距工作時之安全監視。

7. 遠距工作終止時之存取權限撤銷，並應返還相關設備。

8. 如連線之標的(伺服器、主機等)置於本府資訊中心機房內，應依照本府資訊中心之要求執行。

(三)電子郵件安全管理

1. 本局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. 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。

(四)確保實體與環境安全措施(配合本府資訊中心辦理)

1. 資料中心及電腦機房之門禁管理

(1) 資料中心及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資料中心及電腦機房，資料中心及電腦機房管理者並應定期檢視授權人員之名單。

(3) 人員進入管制區應配載身分識別之標示，並隨時注意身分不明或可疑人員。

(4) 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。

(5) 人員及設備進出資料中心及電腦機房應留存記錄。

2. 資料中心及電腦機房之環境控制(本局系統存放於本府資訊中心機房之虛擬機器平台)

(1) 資料中心及電腦機房之空調、電力應建立備援措施。

(2) 資料中心及電腦機房應安裝之安全偵測及防護措施，包括熱度及煙霧偵測設備、火災警報設備、溫濕度監控設備、漏水偵測設備、入侵者偵測系統，以減少環境不安全引發之危險。

(3) 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. 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. 本局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。

(六)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。

(七)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。

(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。

四、系統獲取、開發及維護

本局之資通系統應依「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：

(一)開發過程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」。

(二)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。

(三)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。

(四)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，並檢討執行情形。

拾、資通安全事件通報、應變及演練相關機制

本局依「各機關資通安全事件通報及應變處理作業程序」及「資通安全事件通報及應變辦法」相關規定即時通報及應變，迅速完成損害控制或復原作業，降低資通安全事件對本局業務之衝擊影

響，並確保資通安全事件發生時之跡證保存。

拾壹、資通安全情資之評估及因應

本局接獲資通安全情資，應評估該情資之內容，並視其對本局之影響、本局可接受之風險及本局之資源，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

本局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、特定網頁內容不當、特定網頁發生個資外洩、特定系統遭受入侵、特定系統進行網路攻擊活動等，證據明確，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、國民身分證統一編號、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、涉及關鍵基礎設施維運之核心業務運作等內容，屬涉及核心業務之情資。

二、資通安全情資之因應措施

本局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)涉及核心業務之情資

資通安全推動小組應就涉及核心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。

拾貳、資通系統或服務委外辦理之管理

本局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

(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)本局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。

拾參、資通安全教育訓練

一、資通安全教育訓練要求

(一)本局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。

(二)本局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

(一)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)本局資通安全認知宣導及教育訓練之內容包含：

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. 資通安全法令規定及作業內容。

(三)員工報到時，應使其充分瞭解本局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。

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

本局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，及本局各相關規定辦理之。

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，使本局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，應與本局之資通安全政策、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紀錄。

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

本局每年執行1次資訊安全內部稽核，並於對資訊安全有疑慮或對所採取之矯正措施，需進一步檢查評估時，不定期進行資訊安全內部稽核，藉以適時發現、糾正、消除並預防不符合程序之作業發生，以期各項活動都能有效達成既定資訊安全目標。

（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

（一）本局之資通安全推動小組應於12月前(每年至少1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。

（二）管理審查議題包含下列討論事項：

1. 過往管理審查議案之處理狀態。
2. 資通安全維護計畫內容之適切性。

3. 資通安全政策及目標之實施情形。
4. 內外部稽核結果。
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。

（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，以作為管理審查執行之證據。

拾陸、資通安全維護計畫實施情形之提出

本局依據資通安全管理法第12條之規定，須應上級或監督機關要求，提出資通安全維護計畫實施情形，使其得瞭解本局之年度資通安全計畫實施情形。

拾柒、相關法規

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、各機關資通安全事件通報及應變處理作業程序