107 年 12 月 25 日高市社秘字第 10741352300 號簽准訂定
108 年 1 月 29 日高市社秘字第 10831324700 號修正
109 年 3 月 9 日高市社秘字第 10932258000 號修正
109 年 11 月 19 日高市社秘字第 10940450700 號修正
110 年 4 月 15 日高市社秘字第 11033202100 號修正
111 年 5 月 31 日高市社秘字第 11134782000 號修正
111 年 7 月 19 日高市社秘字第 11135938100 號修正
112 年 7 月 10 日高市社秘字第 11235853600 號修正
112 年 8 月 7 日高市社秘字第 11236640200 號修正

高雄市政府社會局

資通安全維護計畫

發行日期：112 年 8 月 7 日

文件制/修訂紀錄

制/修訂版次	制/修訂日期	簽准文號	制/修訂說明	承辦單位
V1.0	107.12.25	高市社秘字第10741352300號	因應行政院定自108年1月1日施行「資通安全管理法」	秘書室
V2.0	108.1.29	高市社秘字第10831324700號	修訂為C級機關	秘書室
V3.0	109.3.9	高市社秘字第10932258000號	增列資安推動小組成員職級	秘書室
V3.1	109.11.19	高市社秘字第10940450700號	修訂核心業務及重要性	秘書室
V4.0	110.4.15	高市社秘字第11033202100號	增列早療管理系統為非核心業務	秘書室
V5.0	111.5.31	高市社秘字第11134782000號	增列仁家個案管理系統為非核心系統	秘書室
V5.1	111.7.19	高市社秘字第11135938100號	增列上級機關系統為非核心業務	秘書室
V6.0	112.7.10	高市社秘字第11235853600號	1.新增核心業務重要性說明 2.修訂資通安全政策及目標	秘書室
V6.1	112.8.7	高市社秘字第11236640200號	修訂資通安全政策及目標文字	秘書室

目　　錄

高雄市政府社會局資通安全維護計畫(修正草案)

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 條及其施行細則第 6 條。

二、高雄市政府社會局組織規程。

貳、適用範圍

本計畫適用範圍涵蓋高雄市政府社會局（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：

本局核心業務及其重要性如下表：

核心業務	權責單位	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
社政	本局秘書室	高雄市社會福利平台	為本局依組織法執掌之重要業務，且涉及民眾個人資料。	本市各區公所社政業務運作受阻，影響民眾福利身分證明及民眾申請生活補助權益，進而影響機關信譽。	12 小時

二、非核心業務及說明：

本局十九項非核心業務及其說明如下表：

非核心業務	權責單位	資通系統名稱	業務失效影響說明	最大可容忍中斷時間
(一)身心障礙福利資訊	衛生福利部社會及家庭署	衛生福利部社會及家庭署全國身心障礙福利資訊整合平台(上級機關維運)	機關信譽：造成無法查詢民眾資格及開立身心障礙證明，相關訪視紀錄也無法上傳，可能影響民眾權益，進而影響機關信譽。	72 小時
(二)照顧服務管理	衛生福利部長期照顧司	衛生福利部照顧服務管理資訊平台(上級機關維運)	機關信譽：資料無法查詢、建檔及派案，造成各區訪視人員無法掌握進度，可能影響民眾權益，進而影響機關信	72 小時

			譽。	
(三)托育人員(保母)登記管理	衛生福利部社會及家庭署	衛生福利部社會及家庭署托育人員(保母)登記管理資訊系統(上級機關維運)	機關信譽：無法媒合申請托育保母服務及記錄相關托育資料，亦造成撥款延遲等情事，可能影響民眾權益，進而影響機關信譽。	72 小時
(四)脆弱家庭個案管理	衛生福利部社會及家庭署	衛生福利部脆弱家庭個案管理平台(上級機關維運)	影響其他機關業務運作(相依性)：中央或地方通報家庭案件無法即時分析及派案處置，可能引發民眾生活困苦。 機關信譽：因機關無法掌握個案狀況，造成民眾權益受損，進而影響機關信譽。	72 小時
(五)社福津貼給付資料	衛生福利部社會及家庭署	衛生福利部全國社福津貼給付資料比對資訊系統(上級機關維運)	機關信譽：無法時即查詢民眾個資，民眾自行至戶政事務所申請檢附個資，影響時效及不便民。	72 小時
(六)社會福利資源整合	衛生福利部社會社會救助及社工司	衛生福利部全國社會福利資源整合系統(上級機關維運)	機關信譽：無法即時查詢、建立社會救助案件，亦造成撥款延遲等情事，可能影響民眾權益，進而影響機關信譽。	72 小時
(七)兒童及少年未來教育與發展帳戶管理	衛生福利部社會社會救助及社工司	衛生福利部兒童及少年未來教育與發展帳戶管理系統(上級機關維運)	機關信譽：無法即時查詢個案儲蓄現況及基本資料，可能影響服務成效，進而影響機關信譽。	72 小時
(八)社福個案管理	本局社會工作科	高雄市社福個案管理系統	無法即時查詢個案資料與社工員訪視紀錄及派案工作，影響社工員行政效率及個案處遇計畫之執行。	72 小時

(九)未滿二歲兒童托育準公共化服務	本局兒童及少年福利科	高雄市未滿二歲兒童托育準公共化線上申請系統	本市保母無法上網填報登記資料，影響時效及不便民。	72 小時
(十)福利地圖系統	本局秘書室	福利地圖系統	民眾無法即時查詢福利據點位置，需自行上網查詢，不便民。	72 小時
(十一)福利諮詢	本局秘書室	福利專家諮詢系統	民眾無法即時試算相關福利資格，需自行上網查詢或至公所洽詢，不便民。	72 小時
(十二)資料比對	本局秘書室	高雄市政府資料比對系統	國中小學學校承辦人員無法即時比對學生福利身份，需民眾自行至區公所申請檢附相關證明書，影響時效及不便民。	24 小時
(十三)坐月子到宅服務	本局婦女及保護服務科	高雄市坐月子到宅服務系統	無法時即查詢民眾個資，民眾自行至戶政事務所申請檢附個資，影響時效及不便民。	24 小時
(十四)官方網站	本局秘書室	社會局官方網站	民眾無法查詢相關福利資訊，且影響機關行政效率。	24 小時
(十五)報名暨場地租借	本局秘書室	線上報名暨場地租借系統	民眾無法報名或查詢相關課程及場地租借情形，且影響機關行政效率。	48 小時
(十六)內部場地租借及派車	本局秘書室	場地租借及派車系統	無法即時瞭解本局內部場地借用及車輛出勤狀況，影響機關行政效率。	24 小時
(十七)影像檔案管理	本局秘書室	影像檔案管理平台	無法調閱影像掃描檔案，影響檔案申請閱覽之行政效率。	72 小時
(十八)發展遲緩兒童早期療育通報及個案管理	本局秘書室	高雄市發展遲緩兒童早期療育通報及個案管理系統	早期療育個案之通報、派案及個案紀錄無法即時查詢及登錄，影響案件處理時效。	48 小時

(十九)住民個案管理	本局秘書室	個案管理系統(仁愛之家)	無法即時記錄家民狀況及申請派車、設備維護。	72 小時

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，已導入資訊安全管理系統，並訂定資訊安全管理手冊，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：

(一)建立並維持可靠之資訊與通訊作業環境。本局之資訊系統、電腦及網路，係為提供本局公務與為民服務之目的而存在，相關人員應依照前述之目的，正當使用本局之資訊系統、電腦及網路，各單位主管對於該單位所屬員工使用本局之資訊系統、電腦及網路之行為，負有監督之責；委外服務廠商及協力廠商人員使用本局之資訊系統、電腦及網路之行為，應由實際負責該項業務之單位，指派專人負責監督；訪客使用本局之資訊系統、電腦及網路之行為，則由實際負責接待之單位，指派專人負責監督。

(二)為確保本局相關應用系統及資料庫之安全，本局採行各項網路隔離與防護措施，未經許可不得擅自新增或變更網路設備，亦不得擅自移除電腦中之網路監控防護機制。

(三)為確保本局資訊資產之機密性，本局之資訊資產依其機密性區分為限定使用、內部使用及公開使用三個等級之資訊分級標示與保護。相關人員應確實依照上述機密等級，對資訊資產進行標示，並於使用、保存、複製、傳輸時，依照該資訊資產之機密等級，採取保護措施。資訊資產包括資訊機房、核心資通系統、網路、個人電腦、行動裝置與前述項目所處理、傳輸與儲存之資訊。

(四)各項系統及網路服務之使用權限之分配應符合僅授予工作所需必要權限之原則。相關人員使用本局資訊系統與網路前，應事先提出申請，經所屬單位主管審核確為工作上所

必須，再由系統管理人員進行權限之設定。

(五)應妥善保管帳號密碼，避免遭他人利用進行不當存取。所使用之密碼長度應為 8 碼以上，包含英文大寫、小寫、特殊符號或數字三種以上。至少 90 天更換一次密碼並不與前 3 次密碼有重複。

(六)進出因安全理由實施門禁管制之區域，應遵守人員與物品管制之規定，配合執行各項登記與檢查。

(七)經手限定使用資料者，應於離開座位時將限定使用之書面資料置於已上鎖空間內，並對尚在使用中的電腦，啟動其螢幕保護裝置。

(八)本局所有同仁應共同努力保護智慧財產權，且避免本局遭受病毒、駭客及資訊外洩之威脅，且不得於公務用途之電腦中安裝未經許可的軟體，或自網路下載與工作無關之程式、文件與影音資料。

(九)為維護相關應用系統及資料庫之網路安全，連接本局網路應事先提出申請，並經評估其風險後開放使用。透過公眾網路或遠距存取本局之內部網路或對相關伺服器與網路設備進行管理維護時，應加強身分認證並採取加密措施；與本局之網路連線結束後，應立即中斷連線。

(十)不得於辦公室內私裝電腦及網路通訊等相關設備。

(十一) 為保護民眾個人資料之安全性，除因執行法定職務之必要，不得將含有個人資料之檔案，自資訊系統下載並儲存於可攜式儲存裝置中，亦不得將含有民眾個人資料之檔案經由網路對外傳輸。

(十二) 因應資通安全威脅情勢變化，辦理資通安全教育訓練及新進人員資安宣導，本機關同仁亦應確實參與訓練以提高員工之資通安全意識，並依照資通安全宣導內容，於使用電腦與網路時，實施必要之資通安全防護措施，以防止遭受惡意軟體、社交工程、身分盜用、資訊竊取等攻擊。

(十三) 公務電子郵件信箱，僅供傳遞與公務有關訊息，並使用純文字模式瀏覽，避免讀取來歷不明之郵件。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。

（十四）相關人員在發現可能對本局之資料、系統與網路造成危害的事件、弱點與錯誤時，應立即通報秘書室。相關人員於接獲社交工程演練與資通安全事件通報及應變演練通知時，應依演練要求與時限配合辦理。

（十五）違反資訊安全規定情節嚴重者先送資通安全推動小組開會討論，決議後再提報本局局務會議研議。

（十六）本政策每年至少評估一次，以反映政府政策、法令、技術及機關業務之最新狀況，確保本局資訊安全政策之適切性。

二、資通安全目標

（一）量化型目標

1. 核心資通系統可用性達 99.97%以上。(中斷時數/總運作時數≤0.03%)。

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%。

4. 每年辦理資通安全教育訓練至少 1 次。

5. 每 2 年辦理滲透測試及弱點掃瞄作業 1 次。

(二)質化型目標：

1. 機密性目標：確保敏感資訊僅限於授權人員使用。

2. 完整性目標：確保資訊處理過程之正確與完整。

3. 可用性目標：確保系統、服務或資源能夠持續運作，並提供正常的功能性。

4. 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。

5. 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

(一)本局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，向本局內所有人員進行宣導，並檢視執行成效。

(二)本局應每年向利害關係人(例如資訊服務供應商、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

依資通安全管理法第 11 條之規定，本局首長指派主任秘書為資通安全長，負責督導機關資通安全相關事項。

二、資通安全推動小組

(一)本局設置「資通安全推動小組」負責本局整體資訊安全工作之推動，由資通安全長任召集人，並為本局資安工作之資安管理代表，成員為本局各業務科股長級以上人員擔任。

(二)「資通安全推動小組」下設「策略規劃組」、「資安防護組」及「績效管理組」。

(三)分工及職掌

本局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，本局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。

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。

(四)「策略規劃組」、「資安防護組」及「績效管理組」及其它與本局資訊安全管理相關之人員名單，詳如資訊安全管理手冊附件 11 資訊安全人員清冊。

陸、專職(責)人力及經費配置

一、專職(責)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(責)人員 1 人，其分工如下，另現有資通安全專職(責)人員名單及職掌應列冊，並適時更新。

1.資通安全管理面業務 1 人，負責推動資通系統防護需求分級、資通安全管理系統導入、內部資通安全稽核及教育訓練等業務之推動。

2.資通系統安全管理業務 1 人，負責資通系統分級及防護基準、安全性檢測、業務持續運作演練等業務之推動。

3.資通安全防護業務 1 人，負責資通安全監控管理機制、政府

組態基準導入，資通安全防護設施建置及資通安全事件通報及應變業務之推動。

4. 資通安全管理法之法遵事項業務1人，負責本局對所屬公務機關之法遵義務執行事宜。

(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。本局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。

(三)資安專職人員專業職能之培養(如證書、證照、培訓紀錄等)，應依據資通安全責任等級分級辦法之規定。

1. 資安專職(責)人員總計應持有1張以上資通安全專業證照。

2. 資安專職(責)人員總計應持有1張以上資通安全職能評量證書。

(四)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。

(五)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。

(六)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)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，並經資通安全長核定後，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，分別為資料資產、文件資產、軟體資產、服務資產與人員資產等，資料類、文件類、軟體類與硬體類資訊資產依其機密程度分為公開使用、內部使用及限定使用等三級。資訊與資通系統資產盤點結果分別彙整為資訊資產清冊與資訊系統清冊。

(二)本局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。

(三)盤點作業程序、各類資訊資產保護資產、機密分級保護措施及各級資通系統防護規定，詳如資訊安全管理手冊「資訊資產管理」章節。

二、機關資通安全責任等級分級

本局無資通安全責任等級分級辦法第 5 條所列之情形，所維運之社會福利平台、官網、線上報名暨場地租借及派車系統之資通系統係委外（自行）開發，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)本局應每年針對整體資訊環境進行風險評鑑，包括就可能影響資訊安全管理目標達成之風險項目，參考內外在環境議題，並考量資通安全主管機關對於資通安全趨勢、新興威脅與防禦措施之分析與指引，鑑別可能影響本局資訊安全管理整體目標達成的情境；考量現有控制措施效果，分析風險情境發生可能性與衝擊；依風險準則，評估風險情

境之風險等級等作業。

(二)本局針對風險評鑑結果中風險等級 3（高風險）之風險情境採取風險管理措施，風險管理措施之設計，以能使風險等級 3 之風險情境其殘留風險低於風險等級 3 為原則。

(三)本局針對整體資訊環境，進行風險評鑑與風險管理之作業程序，詳如資訊安全管理手冊「風險評鑑與風險管理」章節。

二、核心資通系統及最大可容忍中斷時間

(一)本局於每年辦理資訊及資通系統資產盤點，一併進行資訊系統之營運衝擊分析，於可用性衝擊項度中，判定資訊系統之可忍受中斷時間與可忍受資料流失量，相關作業程序詳如資訊安全管理手冊「資訊資產管理」章節。

(二)核心資通系統(主機)管理員，應依照資訊安全管理手冊「營運持續管理」章節，對核心資通安全系統進行系統災害復原之規劃與應變，並每年進行系統災害復原演練。

玖、資通安全防護及控制措施

一、資訊及資通系統之管理

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核心資通系統之防護基準，採行相關之防護及控制措施，由於本局核心資通系統已導入資通安全管理系統，全局之防護及控制措施詳如資訊安全管理手冊「五、資訊安全管理作業要求」章節。

二、技術面應辦事項

(一)本局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。

(二)資通安全防護設備

1. 本局應建置防毒軟體、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。

(三)安全性檢測

1. 網站安全弱點檢測：全部核心資通系統每二年辦理一次。

2. 系統滲透測試：全部核心資通系統每二年辦理一次。

壹拾、資通安全事件通報、應變及演練相關機制

一、訂定資通安全事件通報

為即時掌控資通安全事件，並有效降低其所造成之損害，本局應訂定資通安全事件通報、應變及演練相關機制，詳如資

訊安全管理手冊「資通安全事件通報處理」章節。

二、通報訂定作業規範內容：

(一)判定事件等級之流程及權責。

(二)事件之影響範圍、損害程度及機關因應能力之評估。

(三)資通安全事件之內部通報流程。

(四)通知受資通安全事件影響之其他機關之時機及方式。

(五)前四款事項之演練。

(六)資通安全事件通報窗口及聯繫方式。

(七)其他資通安全事件通報相關事項。

三、應變作業規範內容：

(一)應變小組之組織。

(二)事件發生前之演練作業。

(三)事件發生時之損害控制，及向中央目的事業主管機關請求技術支援或其他必要協助之機制。

(四)事件發生後之復原、鑑識、調查及改善機制。

(五)事件相關紀錄之保全。

(六)其他資通安全事件應變相關事項。

壹拾壹、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(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及系統弱點修補作業，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，進行必要之系統弱點修補作業，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，選任適當之受託者及簽定保密切結，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。

(六)本局應每年針對核心資通系統之建置、維運或服務廠商進行稽核，執行本項稽核時應先進行書面稽核，經書面稽核後認為有必要時，再進行實地稽核。稽核程序比照本計畫「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」及「二、資通安全維護計畫實施情形之稽核機制」章節所述。

壹拾參、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，資通安全專職人員每年至少 1 名人員接受 12 小時以上之資通安全專業課程訓練或資通安全職能訓練。

(二)資通安全專職人員以外之資訊人員，每人每 2 年至少接受 3 小時以上之資通安全專業課程訓練或資通安全職能訓練，且每年接受 3 小時以上之資通安全通識教育訓練。

(三)本局之一般使用者與主管，每人每年接受 3 小時以上之資通安全通識教育訓練。

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（含參加人

員簽到表)。

(二)本局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。

4. 資通安全技術訓練。

(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。

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。

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

本局每年執行一次資訊安全內部稽核，並於對資訊安全有疑慮時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，相關作業程序，詳如資訊安全管理手冊「四、管理系統框架」章節中「(七)、內部稽核」。

(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)本局資通安全推動小組應每年至少召開一次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)管理審查議題與審查紀錄保存，詳如資訊安全管理手冊「四、管理系統框架」章節中「(八)、管理審查」。

壹拾陸、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。

壹拾柒、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、資訊系統風險評鑑參考指引

八、政府資訊作業委外安全參考指引

九、網路架構規劃參考指引

十、電子郵件安全參考指引

十一、電子資料保護參考指引