限閱

資通安全維護計畫

高雄市前鎮區衛生所

114 年 8 月

修 訂 紀 錄

版次	修訂日期	修訂內容摘要	修訂者	修訂單位
1.0	108 年 1 月 23 日	初版發行	吳貞慧	第二組
1.1	111 年 7 月 21 日	2 版發行	陳姿月	第二組
2.0	114 年 8 月 l 日	共通版發行	吳貞慧	第二組

目錄

壹、 依據及目的

依據資通安全管理法第 10 條、資通安全管理法施行細則第 6 條及高雄市各衛生所組織規程，訂定資通安全維護計畫（以下簡稱本計畫），作為高雄市前鎮區衛生所（以下簡稱本所）資訊安全推動與降低資安風險，並符合法令法規之依循。

貳、 適用範圍

本計畫適用範圍涵蓋本所全機關。

參、 核心業務及重要性

一、 核心業務及作業

（請依是否辦理醫療業務進行勾選）

□本所為**辦理醫療業務**之衛生所

高雄市各衛生所組織規程第四條 衛生所設兩組，分別掌理各有關事項：

（一）防疫、保健、照護、精神衛生、衛生教育、門診醫療、巡迴醫療及緊急救護等事項。

（二）食品衛生、營業與職業衛生、衛生統計及醫藥管理等事項。

■本所為**未辦理醫療業務**之衛生所

高雄市各衛生所組織規程第四條 衛生所設兩組，分別掌理各有關事項：

（一）防疫、保健、照護、精神衛生、衛生教育及緊急救護

等事項。

（二）食品衛生、營業與職業衛生、衛生統計及醫藥管理等事項。

二、 核心資通系統

（請依是否辦理醫療業務進行勾選）

□本所為**辦理醫療業務**之衛生所，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
門診醫療、巡迴醫療等事項。	高雄榮總微型門診系統（共用性系統）	為本所依組織法執掌，足認為重要者	財務損失：可能造成門診收費錯誤(500 元以內)。 民眾生命財產損失：就診民眾多繳費。 違反法遵義務：依個人資料保護法，應善盡個人資料保護責任，如外洩恐造成他人損害，進而單位受罰。 機關信譽：影響當日看診流程造成民怨。	8 小時
掌理防疫、保健、照護、精神衛生、衛生教育、緊急救護、食品衛生、營業與職業衛生、衛生統計及醫藥管理等事項。	無	為本所依組織法執掌，足認為重要者	民眾生命財產損失：可能造成民眾受罰。 機關信譽：未即時登陸可能造成民眾受罰，進而影響機關信譽。	24 小時

■本所為**未辦理醫療業務**之衛生所，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
掌理防疫、保健、照護、精神衛生、衛生教育、食品衛生、營業與職業衛生、衛生統計及醫藥管理等事項。	無	為本所依組織法執掌，足認為重要者	民眾生命財產損失：可能造成民眾受罰。 機關信譽：未即時登陸可能造成民眾受罰，進而影響機關信譽。	24 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。

三、 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
公文交換暨小型檔案管理系統	電子公文無法即時送達機關，影響機關行政效率	24 小時
電子郵件系統	電子郵件無法即時送達機關，影響機關行政效率	24 小時
人事差勤系統	出勤資料無法即時記錄，影響員工權利。	24 小時
全國性預防接種資訊管理系統（共用性系統）	未即時登錄可能造成民眾受罰，進而影響機關信譽。	24 小時

出生通報系統（衛生福利部國民健康署）	未即時登錄可能造成民眾受罰，進而影響機關信譽。	24 小時
照顧服務管理資訊平台（衛生福利部社會及家庭署）	未即時登錄可能造成民眾受罰，進而影響機關信譽。	24 小時
精神照護管理系統（衛生福利部心理及口腔健康司）	未即時登錄可能造成民眾受罰，進而影響機關信譽。	24 小時
志願服務資訊整合系統（衛生福利部）	未即時登錄可能造成民眾受罰，進而影響機關信譽。	24 小時
產品通路管理資訊系統（衛生福利部食品藥物管理署）	未即時登錄可能造成民眾受罰，進而影響機關信譽。	24 小時
營業衛生系統(高雄市政府衛生局)	未即時登錄可能造成民眾受罰，進而影響機關信譽。	24 小時
職業衛生系統(高雄市政府衛生局)	未即時登錄可能造成民眾受罰，進而影響機關信譽。	24 小時
醫事管理系統（衛生福利部）	未即時登錄可能造成民眾受罰，進而影響機關信譽。	24 小時
菸害防制法稽查處分通報及個案管理資訊系統（衛生福利部國民健康署）	未即時登錄可能造成民眾受罰，進而影響機關信譽。	24 小時

各欄位定義：

1. 業務名稱：公務機關之非核心業務至少應包含輔助單位之業務名稱，如差勤服務、郵件服務、用戶端服務等。(請依機關實際情形列出)
2. 作業名稱：該項業務內各項作業程序的名稱。
3. 說明：說明該業務之內容。
4. 最大可容忍中斷時間單位以小時計。

四、 獨立上網線路

（請依是否有獨立上網線路進行勾選）

□本所 **無** 獨立上網線路

■本所 **有** 獨立上網線路，清查後列表如下：

線路供應商	IP 位址範圍	承辦人	連絡電話	e-mail	線路用途	線路實體位置
中華電信(Hinet)	117.56.245.57~58	吳貞慧	07-8414687#23	wu5121@kcg.gov.tw	疫苗溫控警示與保全服務	2樓資訊機房

填寫說明：

獨立上網線路是指這條線路可以「上網」，且不走市府、衛生局的骨幹網路（例如，保全系統專用線路、衛福部離島偏鄉專案上網線路…等）。以下線路不用填報：

1. 機關自行申請的 iTaiwan 無線網路。
2. 機關跟中央介接的 VPN 線路，例如中央的戶役政系統專線、財政系統專線、衛福部專線、健保屬專線、警政署專線等。
3. 機關介接回市府、衛生局的 GSN VPN 線路（KHIN 網）也不用回報。

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：

（一）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。

（二）應強固核心資通系統之韌性，確保機關業務持續營運。

（三）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。

（四）針對辦理資通安全業務有功人員應進行獎勵。

（五）勿開啟來路不明或無法明確辨識寄件人之電子郵件。

（六）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%。

３、每人每年接受三小時以上一般資通安全教育訓練。

（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。

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專責人員簽陳資通安全長核定。

四、 資通安全政策及目標之宣導

（一）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，向所內公佈欄張貼本所資訊安全政策，提供所內所有同仁、約聘僱人員、臨時人員（含替代役、工讀生等）、接觸所內各項資訊之委外服務廠商及協力廠商之人員閱讀知悉，並檢視執行成效。

（二）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，本所訂定所長為資通安全長，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、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，為推動本所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組長/代理人以上之人員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，本所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，本所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、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。

６、資通安全技術之研究、建置及評估相關事項。

７、資通安全相關規章與程序、制度之執行。

８、資訊及資通系統之盤點及風險評估。

９、資料及資通系統之安全防護事項之執行。

１０、資通安全事件之通報及應變機制之執行。

１１、其他資通安全事項之辦理與推動。

１２、辦理資通安全內部稽核。

１３、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

（一）1.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，應設置資通安全專責人員進行資

通安全推動業務，其分工如下，本所現有資通安全專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及驗證、內部資通安全稽核、機關資安治理成熟度評估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、資通安全管理法法遵事項業務1人，負責本所對所屬公務務機關或所管特定非公務機關之法遵義務執行事宜。

（二）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。

（三）本所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、支援服務資產

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、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。

（三）本所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。

（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。

（五）各單位管理之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

本所自行辦理資通業務，未維運自行或委外設置、開發之資通系統者，資通安全責任等級為 D 級。

捌、　資通安全風險評估

一、　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）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。

（三）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

（請依是否辦理醫療業務進行勾選，最大可容忍中斷時間以小時計）

□本所為**辦理醫療業務**之衛生所

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
高雄榮總微型門診系統（共用性系統）	1. 防火牆 Fortigate 40F　1 台。 2. 網路交換器 型號 __台。 3. 個人電腦 型號 ___台。（僅填寫掛號、門診、藥局、批價使用之電腦數量）	8 小時	提供民眾就醫看診服務

■本所為**未辦理醫療業務**之衛生所

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
無	無	無	無

玖、　資通安全防護及控制措施

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、本所同仁使用資訊及資通系統前應經其管理人授權。

2、本所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、本所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、非本所同仁使用本所之資訊及資通系統，應確實遵守本所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。

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。

３、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、本所之網路區域劃分如下：

（１）外部網路：對外網路區域，連接外部廣域網路(Wide Area Network, WAN)。

（２）非軍事區(DMZ)：放置機關對外服務伺服器之區段。

（３）內部區域網路 (Local Area Network, LAN) ：機關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、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。

4、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。

5、本所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；禁止攜帶私人桌上型或筆記型電腦至辦公室連接辦公室網路使用。

6、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。

7、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。

8、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。

9、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。

（５）禁止未經核准私自裝設無線網路設備。

（６）所內電腦禁止私自使用任何無線網路產品連接外部網路。

（二）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，並不與前 3 次密碼重複。

２、使用者使用資通系統前應經授權，採一人一帳(證)制度使用唯一之使用者 ID，不可共用或借給他人使用，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。

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）每週盤點所有電腦是否已安裝防毒軟體，確認病毒碼是否每日持續更新。

（２）每月盤點所有電腦之作業系統更新與應用軟體系

統如 Office、Adobe 等更新（微軟公司約每月提供一次更新)，是否已更新至最新版，並不得自行於網路下載安裝各類軟體。

（３）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。

（４）確實執行網頁惡意軟體掃描。

（５）供醫師、掛號、藥局及繳費等醫療使用之電腦，不可任意直接插入外接儲存設備(含隨身碟或手機)，需預先於其他台電腦以防毒軟體進行掃描確認沒有病毒才可使用。

（６）放置於大廳提供志工、替代役或民眾使用之電腦，應將 USB 接口封閉不得使用。

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，禁止使用遠端連線工具連接至所內電腦進行遠距工作。

（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。

（四）確保實體與環境安全措施

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紀錄。

２、電腦機房或集中式機櫃之環境控制

（１）注意電腦機房或集中式機櫃運作的溫度及電力，必要時應建立恆時空調及備援措施。

（２）注意電腦機房或集中式機櫃消防安全防護措施，以減少環境不安全引發之危險。

（３）注意電腦機房或集中式機櫃之門禁管制；無法實施門禁管制之機櫃應隨時上鎖。實體接觸紀錄（或門禁紀錄）應詳實並定期陳核。

（４）各項安全措施應定期檢查、維修，發現不安全因子應檢討排除。

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。

（７）放置防火牆及數據機(小烏龜)之網路機櫃，建議放置於獨立房間並上鎖。

（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。

（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、所內電腦若有使用已產品支援終止(EOS)版本之Windows 作業系統，則不得連網使用。

４、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。

５、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。

６、非上班或例假日期間，非 24 小時運作之電腦設備，落實下班時應關閉電腦及螢幕電源。

７、如發現資安問題，應主動循機關之通報程序通報。

８、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

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、　系統獲取、開發及維護

（一）本所之資通系統應依「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，並檢討執行情形。

五、 業務持續運作演練

若有辦理醫療業務之衛生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。

六、 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

（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 1 小時內立即通知委託機關及採行之補救措施。

（二）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。

（三）受託者應採取之其他資通安全相關維護措施。

（四）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

（一）本所依資通安全責任等級分級屬 D 級，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）本所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，應使其充分瞭解本所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、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前 14 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、本所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

（一）本所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。

（二）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：

（1）資通安全政策及目標之實施情形。

（2）資通安全人力及資源之配置之實施情形。

（3）資通安全防護及控制措施之實施情形。

（４）內外部稽核結果。

（５）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，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

本所依據本法第 12 條之規定，應於上級或監督機關要求時，提出資通安全維護計畫實施情形，使其得瞭解本所之年度資通安全計畫實施情形。

壹拾柒、 限制使用危害國家資通安全產品

一、 法令依據

依據「各機關對危害國家資通安全產品限制使用原則」辦理。

二、 資通訊產品使用原則

（一）各機關辦理採購時，考量資安疑慮，應確實於招標文件規定不允許大陸地區廠商及陸籍人士參與，並不得採購及使用大陸廠牌資通訊產品。

（二）公務設備不得下載安裝大陸地軟體(含 App)，公務活動不得使用大陸地所提供之平臺或服務。

（三）機關應對同仁宣導量避免購買或使用大陸廠牌資通訊

產品，並落實要求大陸廠牌資通訊產品一律禁止處理公務事務或介接公務環境。

（四）督導汰換作業推動：本機關資安長應負起督導之責，推動落實汰換作業。

壹拾捌、 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）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）無線網路安全參考指引

（十）網路架構規劃參考指引

（十一）行政裝置資安防護參考指引

（十二）政府行動化安全防護規劃報告

（十三）安全軟體發展流程指引

（十四）安全軟體設計指引

（十五）安全軟體測試指引

（十六）資訊作業委外安全參考指引

（十七）本所資通安全事件通報及應變程序

（十八）基層醫療院所資安防護參考指引

（十九）微型診間系統終端電腦資安加強防護指引

二、 附件表單

（一）資通安全推動小組成員及分工表

（二）資通安全保密同意書

（三）資通安全需求申請單

（四）資訊及資通系統資產清冊

（五）風險評估表

（六）風險類型暨風險對策參考表

（七）管制區域人員進出登記表

（八）委外廠商執行人員保密切結書、保密同意書

（九）委外廠商查核項目表

（十）年度資通安全教育訓練計畫

（十一）資通安全認知宣導及教育訓練簽到表

（十二）資通安全維護計畫實施情形

（十三）資通安全稽核計畫

（十四）稽核項目紀錄表

（十五）稽核結果紀錄表

（十六）稽核委員聘任同意保密切結書

（十七）稽核結果及改善報告

（十八）改善績效追蹤報告