壹、目的

規範本院相關人員處理資通系統應遵循資通安全管理法暨相關子法等安全規定，以符合機密性、完整性、可用性及相關法規要求，有效風險管理並持續運作，提升確保資通系統服務品質、保障病人隱私及本院所屬利害關係人之權益。

貳、資通安全定義

係指防止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。並確保在遭受惡意攻擊、破壞或不當使用等資通安全事故發生時，企業組織能夠迅速執行必要應變處置，並在最短時間內回復正常運作，以降低資通安全事故可能影響及危害業務運作之損害程度。

參、資通安全目標

一、核心資通系統可用性達 99.9%以上（中斷時數 / 總運作時數 ≤0.1%）。

二、知悉資通安全事件發生，於確認資通安全事件 1 小時內 100%完成通報，並依資通安全事件通報及應變辦法執行緊急應變機制與災害復原作業。

三、依資通安全責任等級分級辦法應辦事項規定，一般使用者及主管每人每年接受三小時以上資通安全通識教育訓練。

肆、資通安全適用範圍與管理項目

一、資通安全適用範圍

1. 關鍵基礎設施資訊通訊機房與辦公環境、列管資通系統。
2. 本院所有正式員工、約聘僱人員、臨時人員。
3. 接觸本院各項資通系統之委外服務廠商及協力廠商之人員。
4. 接觸本院限定使用等級與內部使用等級資訊之訪客。

二、資通安全管理項目

沿用國際標準組織(ISO)所訂定資訊安全管理系統制度(ISMS)涵蓋控制管理事項，如下：

1. 組織控制
2. 人員控制
3. 實體控制
4. 技術控制

伍、資通安全管理

一、資通安全政策

- 保障資通系統隱私防止不當揭露
- 保護資通系統處理過程與結果的準確性及完整性
- 確保資通系統穩定服務並於可容忍時間恢復正常運作

資通安全政策應由具備專業技術與知識的內部稽核單位、獨立客觀的上級主管辦理，且每年至少評估一次，以反映政府政策、法令、技術及機關業務之最新狀況，確保本院資通安全政策之適切性。

二、資通安全組織

(一) 資通安全推動組織

本院「風險管理暨危機處理委員會」為內部最高資通安全組織，並設置「資通安全暨個資保護小組」推動本院資通安全相關政策，並由「資訊安全工作會議」落實執行相關資通安全工作與配套措施。

1. 風險管理暨危機處理委員會，任務如下：
   (1) 確立醫院風險與危機類別及權責單位。
   (2) 審定醫院風險管理計畫，建立全院危機管理之架構與機制。
   (3) 確立全院緊急應變指揮基本體系，建立共同之應變組織架構。
   (4) 督責權責單位依風險管理計畫，執行風險之預防及危機事件應變及復原。
2. 資通安全暨個資保護小組，任務如下：
   (1) 審議本院資通安全及個人資料保護制度。
   (2) 督導與稽核本院資通安全及個人資料保護管理機制之運作。
   (3) 督導本院資通安全及個人資料保護教育訓練之執行狀況。
   (4) 其他有關資通安全及個人資料保護之事項。
3. 資訊安全工作會議

   每月召開「資訊安全工作會議」並討論相關資通安全業務，例如：資通訊系統合約、資通安全工作行程、內外部關注議題、風險管理評估、資通安全通報追蹤、雲端服務資源報告、網路流量監控回報、資訊安全管理程序書更新、資通核心系統稽核作業等。

(二) 資通安全長與資通安全暨個資保護小組副召集人

1. 資通安全長 / 資通安全暨個資保護小組召集人 / 行政副院長

   依據本院「資通安全組織管理程序書」，由「行政副院長」擔任「資訊安全長」，負責督導本院整體資通(訊)安全工作。
2. 資通安全暨個資保護小組副召集人 / 資訊室主任

   由「資訊室主任」擔任「資通安全暨個資保護小組副召集人」，負責督導資通(訊)安全工作之推動。

(三) 資通安全事件通報及應變指揮架構

依據行政院「各機關資通安全事件通報及應變處理作業程序」規範，成立「資通安全事件通報及應變小組」，並編列各小組代表與分工作業規範。

三、人力資源安全管理

1. 各單位主管應督導可存取機密性與敏感性資訊或系統人員，應加強考核因工作需要配賦系統特別權限之人員，以防範不法及不當行為。
2. 本院定期舉辦資通安全相關教育訓練，促使同仁瞭解資通安全之重要性及各種可能的資通安全風險，以提高同仁資通安全意識，促其確實遵守資通安全規定。

3. 人員應依資通安全管理法及其子法規定，依其職務性質完成相關之資通安全訓練並取得教育訓練學分。
4. 人員於離職或職務調動時應辦理資通資產交接或歸還，並應立即辦理權限異動或帳號移除。
5. 人員資通安全相關作業要求，請參閱「員工保密暨資訊(通訊)安全規範切結書」，若違反資通安全相關規定，應依人事規章處理。

四、資通資產管理

(一) 規範資通資產分類定義與文件類、資料類資通資產機密等級劃分之標準，以及各類資產控管方式及備份需求，作為執行資通資產分類分級管理工作之依據，確保資通資產獲得適當之保護，摘要如下：

1. 資通資產應於每年定期或有大量異動時辦理清查作業。
2. 資通資產依據硬體、軟體、資料、人員、環境與服務等執行基本防護要求。
3. 資料文件類之資通資產機密分級為：公開使用、內部使用及限定使用，各類機密分級防護要求，參考「資通資產管理程序書」實施辦理。

(二) 其它未盡事宜，遵循本院 ISO27001 國際資訊安全管理制度規範辦理。

五、存取控制管理

(一) 規範本院資通系統之帳號、權限與密碼之管理方式，以確保院內資通系統不遭受未經授權之存取及不當使用，摘要如下：

1. 本院各資通系統使用者之識別碼（帳號）及通行碼（密碼），均應限制使用，並嚴禁轉知他人；若已為他人知悉者，應立即更新；因故被冒用致造成不良後果，應負洩密之責。
2. 使用者通行碼（密碼）應依規範執行更新並符合帳號密碼守則。
3. 系統權限以執行業務及職務所需為限，若使用者調整職務及離（休）職時，應儘速註銷該系統存取權限。

(二) 本項目參考本院「存取控制管理程序書」實施辦理。

六、加密管理

1. 如涉及重要資料之傳輸，應使用加密金鑰，加密金鑰應妥善保護。
2. 設定資訊系統帳號通行碼（密碼）複雜度並定期執行變更作業。
3. 其它未盡事宜，遵循本院 ISO27001 國際資訊安全管理制度規範辦理。

七、實體與環境安全管理

(一) 確保本院暨機房實體資通資產安全，避免機房與辦公環境遭受資通安全事件危害而中斷營運。

(二) 資訊機房實體環境管制原則：

1. 機房應保持整潔，地板應定期擦拭，但須避免用水洗。
2. 機房內禁止食用餐點、飲料或存放食物。
3. 機房應注意防鼠及防蟲，以免破壞設備。
4. 機房內嚴禁吸煙、存放易燃物、液體或使用未經核准之電器等。

5. 未經許可不得執行會產生火花與煙塵之作業。
6. 與作業無關之物品不得存放機房。
7. 各種物品應排列整齊，剩餘物品及廢棄物應儘速撤離機房。
8. 機房應有獨立專用之消防系統，消防感知器需均佈於機房區域之天花板及高架地板下方，並於適當之地點設置滅火系統。

(三) 資訊機房配置：空調、消防、門禁、UPS 斷電設備、錄影監視系統、環境監控系統等規範，或其它未盡事宜，參考本院「實體安全管理程序書」與 ISO27001 國際資訊安全管理制度規範實施辦理。

八、作業管理

1. 本院所有資訊系統與電腦設備（包含軟體、硬體、服務）必須符合工作之需要，避免使用於非公務用途，且未經資通安全暨個資保護小組副召集人(資訊室主任)授權不得隨意變更或移動。
2. 使用網際網路（Internet）時，避免遭受駭客攻擊、病毒攻擊或植入木馬程式，嚴禁連結與工作無關之網站，依 ISO27001 國際資訊安全「防火牆管理程序書」辦理。
3. 使用者不得使用資訊系統、電腦網路或電子郵件，傳送或散佈具恐嚇性、暴力性、違背善良風俗之資料，或謾罵、侮辱他人等不當言論。
4. 遵守帳號密碼規範，不得擅自盜用他人帳號或修改他人檔案、資料或密碼。
5. 不得非法侵入或企圖更改未經授權的資訊系統、電腦設備、網路系統，亦不得置放、散佈、侵擾其他使用者資料或程式，依 ISO27001 國際資訊安全「網路管理程序書」辦理。
6. 院內每一台公務資訊電腦設備皆配置固定通訊協定（IP）位址，禁止任意變更電腦通訊協定及（IP）位址，以避免造成網路通訊衝突而導致資訊系統或電腦設備發生異常。
7. 資訊系統與電腦設備設定作業系統安全性更新作業與防毒程式，嚴禁使用者自行變更或移除相關作業，避免遭受病毒攻擊而無法正常運作，依 ISO27001 國際資訊安全「技術弱點管理工作指導書」辦理。
8. 使用者欲升級或增加電腦工作站之軟硬體需求時，填寫「帳號密碼需求單」申請資訊軟體，填寫「請購單」申請硬體設備，經單位主管與資訊室審核通過，再由資材室購置，再通知資訊室人員進行安裝處理。
9. 因公務需求，欲使用私人或廠商提供之資訊程式或設備，必須填寫帳號密碼需求單，經單位主管許可，送資訊室審核通過列管後方能使用。
10. 使用者增加網路線路，必須填寫資訊維修單，經資訊室審核通過後，由專責人員施工處理，不得私自安裝網路設備或增加網點。
11. 連線使用院外機構之電腦與網路時，應遵守該機構之使用規範。
12. 尊重智慧財產權，本院各單位不接受委託任何拷貝、複製非法軟體或程式等行為。

13. 若違反上述相關規定，觸犯法律或造成院內損失，依造成傷害情節輕重，將依據員工獎懲辦法給予適度處罰，並自行肩負法律刑責。
14. 資訊電腦設備（包含：平板、筆電、All in one 等）係為醫院公務用途，依公共使用與配置為原則，各單位申請資訊電腦時，視實際業務需求程度評估，並經主管核准之後給予配置。
15. 員工攜帶私人電腦資訊設備，申請無線網路權限開放使用，必須遵守無線網路管理規範。
16. 電腦系統應與標準時鐘同步或定期對時，以確保系統時間之一致性。
17. 其它未盡事宜，遵循本院 ISO27001 國際資訊安全管理制度規範辦理。

九、通訊管理

1. 被授權的網路使用者，只能在授權範圍內存取網路資源，不得將自己的登入身份識別與登入網路的密碼交付他人使用。
2. 經由網際網路下載軟體或資料檔案，得視業務特性及需要，由使用單位事前測試及掃瞄，在確認安全無虞及不違反智慧財產權前提下，方得下載執行。
3. 對外開放的資訊系統中不得存放機密性及敏感性資料或文件。
4. 內部使用的瀏覽器，對下載的每一檔案應做電腦病毒的掃描。
5. 機密性資料或文件，使用電子郵件傳送應加密處理之。
6. 應考量網際網路新技術的可能安全弱點，並採取適當的防護措施以確保內部網路安全。
7. 網路系統中各主要主機伺服器應評量其對業務之急迫性設立備援主機，以備主要作業主機無法正常運作時之用。
8. 網路系統中各伺服器主機應定期（或異動時）做系統備份，包括完整系統備份，系統架構設定備份。
9. 伺服器主機應關閉非必要的服務程式，並隨時更新程式版本。
10. 本項目參考本院「網路管理程序書」實施辦理。

十、資通系統獲取、開發及維護管理

1. 應將系統發展測試作業及系統正式作業之軟體，分別在不同處理器或不同的目錄下作業，以便系統測試與正式作業分開處理，並避免作業軟體或資料遭意外竄改，或不當使用。
2. 各單位委託廠商開發或維護軟硬體設施時，應在單位相關人員監督及陪同下為之。
3. 自行或委外開發資通系統，應於系統發展生命週期規劃階段，將資通安全需求納入考量，依據本院「資通安全防護自我評量表」執行「資通系統防護需求等級評估表(附表九)」與「資通系統防護分級及防護基準(附表十)」法遵規範。
4. 資訊系統之維護、更新、上線執行及版本異動作業，應予安全管制，避免不當軟體、後門及電腦病毒等危害系統安全。

5. 重要業務系統，應建立例行性稽核制度，建立稽核軌跡。
6. 對系統服務廠商之軟硬體系統建置及維護人員，應規範及限制其可接觸之系統與資料範圍，並嚴禁核發長期性之系統帳號通行密碼。
7. 應注意系統開發環境安全，避免程式原始碼遭受不當污染。
8. 應使用安全的程式語法及程式元件開發，減低系統漏洞風險
9. 行動裝置應用程式安全提供行動裝置（係指包含但不限於智慧型手機、平板電腦等具通信及連網功能之隨身設備）服務應注意下列安全要點：
   (1) 應針對應用程式檢視系統所需最小權限，並進行存取控制。
   (2) 於行動裝置上如有必要儲存敏感資料，應採取加密等相關機制保護，以防範資料外洩。
   (3) 應針對應用程式進行原始碼掃描、黑箱測試或滲透測試，並針對中、高風險弱點及可影響敏感資料被竊取或竄改之弱點進行改善。
10. 本項目參考本院「應用系統獲取開發與維護管理程序書」實施辦理。

十一、供應關係管理

確保資訊通訊委外服務過程之資訊安全控制與服務水準符合資通安全管理法與相關子法規範，並依資通安全管理法第九條與資通安全管理法施行細則第四條辦理：

(一) 各機關依本法第九條規定委外辦理資通系統之建置、維運或資通服務之提供（以下簡稱受託業務），選任及監督受託者時，應注意下列事項：
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。
3. 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。
4. 受託業務涉及國家機密者，執行受託業務之相關人員應接受適任性查核，並依國家機密保護法之規定，管制其出境。
5. 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安全性檢測證明；該資通系統屬委託機關之核心資通系統，或委託金額達新臺幣一千萬元以上者，委託機關應自行或另行委託第三方進行安全性檢測；涉及利用非受託者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。
6. 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。
7. 委託關係終止或解除時，應確認受託者返還、移交、刪除或銷毀履行契約而持有之資料。
8. 受託者應採取之其他資通安全相關維護措施。
9. 委託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。

(二) 委託機關辦理前項第四款之適任性查核，應考量受託業務所涉及國家機密之機密等級及內容，就執行該業務之受託者所屬人員及可能接觸該國家機密之其他人員，於必要範圍內查核有無下列事項：

1. 曾犯洩密罪，或於動員戡亂時期終止後，犯內亂罪、外患罪，經判刑確定，或通緝有案尚未結案。
2. 曾任公務員，因違反相關安全保密規定受懲戒或記過以上行政懲處。
3. 曾受到外國政府、大陸地區、香港或澳門政府之利誘、脅迫，從事不利國家安全或重大利益情事。
4. 其他與國家機密保護相關之具體項目。

(三) 第一項第四款情形，應記載於招標公告、招標文件及契約；於辦理適任性查核前，並應經當事人書面同意。

(四) 本項目參考本院「資訊委外服務管理程序書」實施辦理，摘要如下：

1. 承攬廠商應簽署「資訊安全責任條款」，或於委外合約中包括「資訊安全責任條款」中之條款；本條款壹式兩份，由甲、乙雙方用印之後各自存檔保管。
2. 委外作業人員應簽署「資訊保密暨資通安全規範切結書」；委外作業人員因故更換時，應來函正式通知，替換之人員也應簽署「資訊保密暨資通安全規範切結書」。
3. 委外廠商發現資通安全異常事件而影響資通系統運作，應於法遵規範知悉一小時內透過電話或電子郵件通知本院窗口並進行緊急處置措施。
4. 委外契約或建議書徵求說明書應載明下列事項：
   (1) 廠商應遵循之資通安全、保密條款及作業相關之法規要求。
   (2) 各項資通安全控管要求，以明確告知委外廠商應遵循事項。
   (3) 相關資通資產之機密性、完整性、可用性及法規性要求。
   (4) 本院得保留對委外廠商進行資通安全稽核之權利。

(五) 委外廠商及其相關人員於契約期間出入本院辦公場所時，須佩戴識別證，以供人員安全控管及掌握。

(六) 委外廠商及其相關人員於非上班時間加班作業時，應事先取得相關單位同意，以利管控人員出入。

(七) 行政院宣導使用大陸廠牌資通訊產品規範：

1. 公務用之資通訊產品不得使用大陸廠牌，且不得安裝非公務用軟體。
2. 個人資通訊設備不得處理公務事務，亦不得與公務環境介接。
3. 各機關應就已使用或採購之大陸廠牌資通訊產品列冊管理，且不得與公務環境介接。
4. 各單位應配合盡速汰換所使用或採購大陸廠牌資通訊產品(含軟體、硬體及服務)。

(八) 其它未盡事宜，遵循本院 ISO27001 國際資訊安全管理制度規範辦理。

十二、資通安全事故管理

1. 本院（含供應關係上下游廠商）發生資通安全事故時，應立即通報，並由通安全暨個資保護小組窗口，依相關規定進行緊急應變處置。
2. 本院每年至少辦理一次資通安全事故通報暨災害復原演練。
3. 本項目參考本院「資通安全事故通報管理程序書」實施辦理

十三、業務持續營運管理

1. 本院針對核心資通系統（含資訊電腦主機伺服器、應用資訊系統、資料庫等）擬定資料備份、還原與異地儲存機制並確實辦理。
2. 建立跨部門核心資通系統業務持續運作程序並演練，以降低資通安全事故發生時的衝擊與威脅，使核心資通系統業務在發生事故時，仍可依備援方案持續運作。
3. 其它未盡事宜，遵循本院 ISO27001 國際資訊安全管理制度規範辦理。

十四、遵循性管理

(一) 法遵規範：禁止使用違反著作權、善良風俗或會妨害網路系統的正常運作之不法或不當的資訊。

(二) 資通安全稽核

1. 內部稽核：訂定稽核計畫並呈報核准後實施，得視狀況適時辦理修正。
2. 外部稽核：得定期或不定期對內外部關係實施稽核作業。
3. 實施稽核作業時，應詳實記錄查核情形，至少包括：實施對象、實施時程、實施範圍、人員配置與相關規範等，並撰寫稽核報告，呈報核閱。
4. 前項有關查核記錄與檢討報告，應由查核單位妥為保管，以供相關權責機關實施外部稽核時之參考。
5. 稽核報告之建議事項，應由受稽核之主辦單位負責辦理或改善。
6. 關於本項目之施行細節，由資通安全暨個資保護小組制定相關稽核計畫，於呈報核准後實施。

陸、附則

本院各權責單位得視個別業務需求，依據本實施要點另訂相關規範，呈報風險管理暨危機處理委員會核備後實施。

以下空白。