1. 目的

1.1 作為本所資訊安全管理制度(以下簡稱ISMS)相關管理辦法以及作業程序之參考依據。同時沿用國際標準組織(ISO)所訂定之持續改善 P.D.C.A.循環流程管理模式，整合及強化資通安全管理體系，建立制度化、文件化及系統化之管理機制，持續監督及審查管理績效，以落實資通安全管理及業務持續營運之理念，並達到以下之目標：

1.1.1 建立、落實及維護資通安全管理政策。

1.1.2 導入 ISMS。

1.1.3 培訓資訊人力在資訊及通訊領域之安全專業能力。

1.1.4 強化資通安全環境及資通安全應變能力。

1.1.5 達成資通安全管理政策量測指標。

1.2 確保本所所屬之資訊資產之機密性、完整性及可用性，並符合相關法令法規之要求，使其免於遭受內、外部的蓄意或意外之威脅，以保障本所所屬利害關係人之權益。

2. 適用範圍

2.1 本所 ISMS 所涵蓋範圍內皆適用之。

2.2 資通安全管理涵蓋 14 項管理事項，避免因人為疏失、蓄意或天然災害等因素，導致資料不當使用、洩漏、竄改、破壞等情事發生，對本所帶來各種可能之風險及危害。管理事項如下：

2.2.1 資通安全管理政策制定及評估。

2.2.2 資通安全組織之職責與分工。

2.2.3 人力資源安全。

2.2.4 資訊資產管理。

2.2.5 存取控制。

2.2.6 密碼控制。

2.2.7 實體與環境安全。

2.2.8 作業安全。

2.2.9 通訊安全。

2.2.10 資訊系統獲取、開發及維護。

2.2.11 供應商關係。

2.2.12 資通安全事故管理。

2.2.13 營運持續管理的資通安全層面。

2.2.14 遵循性。

3. 安全管理政策

為了使本所 ISMS（資訊安全管理系統）能切合實際需要，藉由維護本所重要資訊系統的機密性、完整性與可用性，以支持業務之順遂，特頒布資通安全管理政策。本政策為高階指導原則，所有同仁、委外廠商皆有義務積極參與推動資通安全管理政策，以確保所有資訊系統安全維運，並期許所有人均能了解、實施與維持，以達資訊持續營運配合本所業務遂行的目標。

3.1 落實資通安全，強化服務品質

貫徹執行 ISMS，所有資訊作業相關措施，應確保資料之機密性、完整性及可用性，免於因相關資訊安全威脅遭受洩密、破壞或遺失等風險，選擇適切的保護措施，將風險降至可接受程度進行監控、審查及稽核資訊安全管理制度的工作，以完善的資通安全強化服務品質，提升服務水準。

3.2 加強資安訓練，符合法令要求規範

加強資安訓練，督導全體同仁落實資通安全管理，持續進行適當的資通安全教育訓練，建立「資通安全，人人有責」的觀念，促使同仁瞭解資通安全相關法令要求之重要性，進而遵守法令及規定，藉此提高資通安全認知及能力，降低資通安全風險，達成資通安管理法及個人資料保護法等相關法令要求事項。

3.3 規劃持續營運，迅速完成災害復原

訂定關鍵性業務核心資訊系統之緊急應變計畫及災害復原計畫，每兩年執行一次緊急應變流程演練，以確保資訊系統失效或重大災害事件發生時，能迅速復原，保持

關鍵性核心資訊系統續運作，達成本所主要業務順利執行。

4. 資通安全管理目標

本所執行 ISMS 需達成之資通安全目標，應依據「ISMS-P-005 資通安全目標管理程序書」之相關規定辦理。

5. 資通安全責任

5.1 本所的管理階層負責建立及審查政策。

5.2 資通安全管理者透過適當的標準和程序以實施本政策。

5.3 所有人員與契約委外廠商均須依照程序以維護資通安全管理政策。

5.4 所有人員有責任通報安全事件和任何已鑑別出的弱點。

5.5 任何蓄意違反資通安全的行為將受到相關規範或法律行動。

6. 資訊安全管理制度(ISMS)

6.1 一般要求

本所因應 ISO 27001:2013 資訊安全管理標準之要求，特制訂本政策作為整體 ISMS 之建置開發、實施操作、監控審查及持續改善之規範，並依據本所業務活動與風險，以建立資通安全管理政策及管理目標。

6.2 組織全景之鑑別

6.2.1 本所應決定與本所營運目的相關，且會影響 ISMS 預期成果之內部與外部議題，鑑別出與本所所提供服務相關之利害關係者，以及這些利害關係者對本所的需求與期望，並讓資通安全長知悉以取得共識，用以客觀決定本所 ISMS 之範圍。

6.2.2 應制定組織全景鑑別管理作業程序，用以系統化地鑑別本所之核心業務與核心業務相關之利害關係者，以及這些利害關係者對本所核心業務之需求與期望，並判別若無法達到需求與期望會對本所造成何種程度之衝擊，並將上述評估及分析結果供資通安全長用以決策 ISMS 之導入及驗證範圍。

6.3 ISMS 之建置開發

6.3.1 建立 ISMS

6.3.1.1 過程簡要說明

本所係依照 ISO 27001:2013 標準之步驟建立 ISMS，其過程簡要說明如下：

(a) 依據標準建議與主管機關之要求，成立本所「資訊安全推動小組」，並經核准頒布。

(b) 本所 ISMS 以全機關為實施範圍，不因選擇之驗證範圍而有所差異。

(c) 頒布「資通安全管理政策」，以說明本所資通安全管理政策、管理目標與執行方式。

(d) 進行風險評估作業，發掘資產與組織之安全弱點及其威脅與影響，並評估其風險等級，彙整成「風險評鑑報告」後，執行及追蹤「風險處理計畫」。

(e) 依據資通安全管理政策與風險評估的結果，設定風險管理之實施範圍。

(f) 選擇適合實施之資通安全管制目標與措施，並檢討確認其可行性與有效性。

(g) 將所選定之安全管制目標、管制措施、選用原因等資料記載於「適用性聲明（Statement of applicability）」文件中。

(h) 為貫徹資通安全並持續改善，本所將依實際需求適時檢討上述步驟，並做必要之變更修正。

6.3.1.2

本所所有同仁與委外廠商派駐人員均須遵循本所資通安全管理政策與資通安全目標，恪守 ISMS 各項作業流程、管理規範及相關法令法規之要求。故意或過失違反者，將視其違反情節及所造成之衝擊，依人事規章或委外契約予以懲處。

6.3.1.3

委外廠商在執行本所委外業務時若有複委託之需求，應評估複委託業務相關之資安風險，並要求委外廠商依 ISMS 等相關規定對複委託委外廠

商進行適當之監督與管理。

6.3.1.4 對內部及外部專案管理的過程中，應明訂及陳述與專案相關之各項資通安全要求，並由風險評鑑之結果用以決定及實作資通安全控制措施，確保內部及外部專案資訊之機密性、完整性及可用性，降低機敏資訊（含個人資料）外洩及違反法令之風險。

6.3.1.5 應決定及建立與 ISMS 相關的內部與外部溝通之需求及準則，內容須包含：要溝通什麼、何時溝通、和誰溝通、應是誰溝通以及應實現哪種溝通過程，確保 ISMS 各項資安業務在內部適度的溝通與傳達，以利 ISMS 推動與管理。

6.3.1.6 應制定可攜式資訊設備（包含智慧型移動裝置）及可攜式儲存媒體之管理程序，要求同仁落實執行，並定期針對可攜式資訊設備（包含智慧型移動裝置）及可攜式儲存媒體進行風險評鑑，依據風險評鑑之結果選擇適切之控制措施，定期對同仁執行查核作業，確保使用可攜式資訊設備及儲存媒體之風險受到監控，降低機密資料外洩之風險。

6.3.2 ISMS 之實施操作

6.3.2.1 應制定風險處理計畫，有系統地鑑別及陳述適當的管理措施、權責及優先順序，以便管理資通安全風險。

6.3.2.2 實施風險處理計畫中所選定之控制措施，以對各項風險加以防禦與控制，包含實施既定管理計畫，以達到所設定之資通安全目標。

6.3.2.3 應擬定安全控制措施有效性之量測指標與使用方法，以判斷所選控制措施以達資安目標所要求之程度。

6.3.2.4 人員所需實施訓練與認知計畫參閱第 7.2.2 節。

6.3.2.5 各項作業需遵照作業規範與程序執行，並不定期檢視與管理各項作業執行之狀況。

6.3.2.6　須定時衡量各項計畫目標執行狀況，並依據衡量結果適時調整相關控制措施與目標。

6.3.2.7　執行時所需之各項資源管理參閱第 7.2 節。

6.3.2.8　課室主管利用不定期巡視、內外部稽核或是課室人員所提出之建議事項回報，加速偵知各種安全事件並予以回應處理。

6.3.3　ISMS 之監控審查

6.3.3.1　本所採用下列監控方式確保 ISMS 所涵蓋範圍皆能安全無虞：

(a) 人員應定期及不定期巡視檢查各項設備及環境是否皆屬正常狀態。

(b) 利用攝影機監視各個地區人員出入狀況並錄影存證。

(c) 應設定、定期檢查及紀錄各項監控指標，以協助判斷安全事件，預防及立即處理安全事故之發生。

(d) 課室主管應隨時注意各項通報事件或人員工作執行狀況，進而決定相應的控制措施，必要時可將人員職務進行短期調動，避免發生系統失效或人為破壞事件。

(e) 配合定期執行之內部稽核，確認各種安全措施及控制程序是否如預期般實施。

(f) 隨時注意本所所發生之資安事件，針對事件發生之成因及後果詳加評估，並配合矯正預防措施之執行，改善整體資安環境，降低資安事件發生之機率。

(g) 管理階層利用定期執行之「資訊安全推動小組」或內部會議，討論目前可能存在的安全漏洞，並決定解決之道。

6.3.3.2　於「資訊安全推動小組」中定期審查 ISMS 之有效性，並考慮安全稽核、事件、有效性量測及利害關係團體之建議及反映意見。

6.3.3.3 於「資訊安全推動小組」中審查資通安全風險、殘餘風險與可接受風險等級，並考慮組織、技術、課室營運目標及程序、已鑑別之威脅與外部事件（包括法令法規、契約義務及社會環境)之變化。

6.3.3.4 每年執行 1 次內部稽核，以確定是否有依據作業流程執行，且是否達到預期功能。

6.3.3.5 每年至少召開一次資通安全管理審查會議，執行正式的 ISMS 審查，以確保範圍適當及 ISMS 過程之各項改善措施均已鑑別與實施。

6.3.3.6 應依據監控審查結果，適時修訂資通安全維護計畫，以符合資安政策、資安目標與各項資通安全要求。

6.3.3.7 所有對 ISMS 有效性或績效有衝擊之活動與事件均須加以記錄。

6.3.4 ISMS 之持續改善

本所將定期進行下述工作：

6.3.4.1 利用風險評鑑及內外部稽核之結果進行整體資通安全環境之改善。

6.3.4.2 採取適當矯正及預防措施，採用從其他外部單位或內部發生事件之安全經驗汲取教訓。

6.3.4.3 與相關機構就結果及各項措施進行溝通並徵詢意見。

6.3.4.4 必要時修改 ISMS。

6.3.4.5 確保各項修改措施達到預期目標。

6.4 文件要求

6.4.1 一般要求

本所 ISMS 文件化包括下列各項：

6.4.1.1 資通安全管理政策與安全管理目標之書面聲明。

6.4.1.2 ISMS 適用範圍及各項作業程序。

6.4.1.3 風險評鑑報告。

6.4.1.4　風險處理計畫。

6.4.1.5　組織為確保有效規劃、操作及控制資通安全過程所需之文件。

6.4.1.6　ISO 27001 標準要求及上級主管單位要求之紀錄。

6.4.1.7　適用性聲明書。

6.4.2　文件管制

ISMS 所需之文件應受保護及管制。紀錄是文件之一種特殊型態，應依第 6.4.3 節所定的要求予以管制，並建立文件化程序，以界定所需之管制，用以：

6.4.2.1　在文件發行前核准其適切性。

6.4.2.2　必要時，審查與更新並重新核准文件。

6.4.2.3　確保文件之變更與最新改訂狀況已予鑑別。

6.4.2.4　確保在使用場所備妥適用文件之相關版本。

6.4.2.5　確保文件易於閱讀並容易識別。

6.4.2.6　確保文件於需使用時能隨時取用，並且於文件傳遞、保存及毀棄時皆能遵守文件管制規定辦理。

6.4.2.7　確保外來原始文件已加以鑑別。

6.4.2.8　確保文件分發有適當管制。

6.4.2.9　防止作廢（失效）文件被誤用，作廢文件為任何目的需保留時，應予以適當鑑別。

6.4.3　紀錄管制

6.4.3.1　為確保 ISMS 符合本所要求及提供有效運作之證據，應建立及維持執行 ISMS 各項作業程序之各項紀錄，並予以管制，並將相關法律法規及契約要求列入考量。

6.4.3.2　紀錄應清晰易讀，容易識別及檢索。紀錄之鑑別、儲存、保護、檢索、保存期限及作廢，應建立文件化程序，以界定所需之管制。

6.4.3.3　紀錄應妥善保存。

6.4.3.4 所需之紀錄及其範圍應由管理過程加以決定。該過程應記錄重大決定，並將紀錄之用途及缺少紀錄時相關之風險列入考量。

7. 管理階層責任

7.1 管理階層承諾

為使 ISMS 推動順利，管理階層應確實執行下列事項：

7.1.1 建立資通安全管理政策、資通安全目標及計畫。

7.1.2 成立「資訊安全推動小組」，以明訂及文件化資通安全之角色與責任。

7.1.3 定期召開 ISMS 之管理階層審查會議。

7.1.4 決定風險評鑑後之可接受風險等級。

7.1.5 定期執行 ISMS 之內部稽核作業。

7.1.6 提供充分資源，確保能建立、實施操作、監控審查及持續改善 ISMS。

7.1.7 各課室主管應儘量藉由各種內部公開會議或集會時，向所有人員宣達符合資通安全目標、法律及法規要求之重要性，以及持續改善之需求。

7.2 資源管理

7.2.1 資源提供

為確保 ISMS 執行無礙，應決定並提供下列工作之必要資源：

7.2.1.1 提供建置與維護 ISMS 時所需的人力與資源設備。

7.2.1.2 提供實施 ISMS 時必要之協助。

7.2.1.3 確定各項安全程序可配合營運需求。

7.2.1.4 鑑別並提出法律與法規的要求以及於各項契約上註明之安全義務。

7.2.1.5 正確應用所有實施的控制措施，以維持適當之安全。

7.2.1.6 當需要時，進行審查並針對審查結果作適當因應。

7.2.1.7　當必要時，改善 ISMS 之作業流程，以確保其有效性。

7.2.2　訓練、認知及能力

為確保所有同仁皆有能力執行所要求之工作與符合各項安全要求，應藉由各種途徑取得協助同仁執行教育訓練，包括下列方式：

7.2.2.1　提供各種能力訓練以滿足該需求。

7.2.2.2　藉由意見（滿意度）調查、測驗、繳交心得報告及證書取得等方式，評估所提供訓練之有效性。

7.2.2.3　確保同仁認知其所從事的活動之相關性及重要性，以及如何對資通安全目標之達成有所貢獻。

7.2.2.4　應留下教育訓練、技能、經驗及評定資格等紀錄，紀錄保存之要求參閱第 6.4.3 節。

7.3　有效溝通

應決定及建立與資訊安全管理制度（ISMS）相關的內部與外部溝通之需求及準則，內容須包含：要溝通什麼、何時溝通、和誰溝通、應是誰溝通以及應實現哪種溝通過程，確保資訊安全管理制度（ISMS）各項資安業務在內部適度的溝通與傳達，以利資訊安全管理制度（ISMS）之推動與管理。

8. 內部稽核

每 1 年定期執行 1 次內部稽核，確保 ISMS 的各項管制目標、控制措施、運作過程以及各項程序是否皆：

8.1　符合 ISO 27001 與相關法令或法規之要求。

8.2　符合本所所制定之資通安全目標及其他相關要求。

8.3　有效地實施與維持 ISMS。

8.4　符合上級單位的期待。

9. ISMS 之管理階層審查

9.1　概述

本所「資訊安全推動小組」至少每年召開一次會議，針對本所現行之 ISMS 進行審查，以確保相關程序的適用

性、適切性及有效性皆符合本所需求，並評估相關政策與目標的改善時機，或是其他的變更需求，且審查結果應留下相關文件與紀錄備查。

9.2 審查輸入（管理審查之範圍）

管理階層審查至少應包含下列項目：

9.2.1 先前管理審查決議事項之跟催狀況。

9.2.2 有關可能影響 ISMS 的外部與內部問題之變更。

9.2.3 資通安全的績效回饋，包含下列趨向：

9.2.3.1 不符合事項與矯正措施之執行狀況。

9.2.3.2 監督與量測結果。

9.2.3.3 內部稽核的結果。

9.2.3.4 資通安全目標的實現。

9.2.4 利害相關團體的回饋。

9.2.5 風險評鑑的結果與風險處理計畫的狀態。

9.2.6 持續改善的機會。

9.3 審查輸出

9.3.1 管理審查的產出應包含持續改善機會與 ISMS 的變更需求有關之決定。

9.3.2 管理階層審查之產出建議包含但不限於下列事項之任何決策與措施：

9.3.2.1 ISMS 有效性之改善。

9.3.2.2 風險評鑑與風險處理計畫之更新。

9.3.2.3 影響資通安全之程序與控制之必要時的修改，以回應可能衝擊 ISMS 之內部或外部事件，包括下列事項之變更：

(a) 各項營運要求。

(b) 各項安全要求。

(c) 影響既有各項營運要求之營運過程。

(d) 法律或法規各項要求。

(e) 契約的各項義務。

(f) 風險等級及/或風險接受準則。

9.3.2.4 資源需求。

9.3.2.5 控制措施的有效性如何量測之改善。

9.3.3 組織應保存文件化資訊及管理審查結果的證據。

10. ISMS 之改善

10.1 矯正措施

本所採取適當的控管措施，以減低 ISMS 在建置、操作及使用時所產生的不符合事項，以防止再度發生。矯正措施之內容應包含下列各項：

10.1.1 鑑別各項不符合資安要求之事項。

10.1.2 判定各項不符合事項發生之原因。

10.1.3 評估各項矯正措施之需求，以確保各項不符合事項不復發。

10.1.4 決定及實施所需之矯正措施。

10.1.5 需記錄所採矯正措施之結果，紀錄保存之要求參閱第 6.4.3 節。

10.1.6 審查所採取之矯正措施。

10.2 預防措施

本所應採取適當的控管措施，以預防及降低潛在不符合事項發生之機會，預防措施應能預防潛在問題所可能發生之影響。

10.2.1 鑑別潛在的各項不符合事項及其原因。

10.2.2 評估預防措施的需求，以防止不符合事項的發生。

10.2.3 決定及實施所需之預防措施。

10.2.4 記錄所採取措施之結果，紀錄保存之要求參閱第 6.4.3 節。

10.2.5 審查所採取之預防措施。

10.3 持續改善

本所經由資通安全管理政策、安全目標、內外部資通安全稽核結果、事件監控之分析、矯正與預防措施以及管理階層審查，由課室資通安全人員負責所有風險發生或不符合事項之監控，並追蹤相關業務承辦人之改善情形，以持續改善 ISMS 之有效性。

11. 審查

11.1 本政策每年應至少評估檢討一次，以反映本所資通安全需求、政府法令法規、外在網路環境變化及資通安全技術等最新發展現況，以確保其對於維持營運和提供適當服務的能力。

11.2 本政策如遇重大改變時應立即審查，以確保其適當性與有效性。必要時應告知相關課室/單位及委外廠商，以利共同遵守。

12. 發布實施

本政策經資通安全長核准，於公告日施行，並以書面、電子或其他方式通知本所所屬職員及與本所連線作業之有關機關（構）、委外廠商，修正時亦同。