管理系統文件

文 件 類 別	第 一 階 文 件	
文 件 編 號	ISMS-M-001	
文 件 名 稱	資通安全管理政策	
發 行 單 位	資通安全處理小組	
發 行 日 期	113 年 08 月 23 日	
版　　次	2A	
訂修廢單位	審　　查	核　　准

（原版簽名頁保存於資通安全處理小組）

訂　　修　　廢　　記　　錄		
版次	發行日期	訂 修 廢 內 容 摘 要
A	104/09/16	初版發行
B	108/10/25	因應資通安全管理法施行及配合法規用詞，將「資訊」一詞修改為「資通」。
C	112/08/14	增修訂 6.2.3.9 變更規劃
2A	113/08/23	配合 ISO/IEC27001:2022 進行全新改版。

1. 目的

1.1. 本資通安全管理政策作為本院資訊安全管理制度(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. 全面導入 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. 確保本院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，以保障本院所屬利害關係人之權益。

2. 適用範圍

2.1. 本政策適用於本院所有資訊資產及相關的資訊處理活動，包括但不限於電子、紙本、口頭或其他形式的資訊。此政策涵蓋所有本院成員，包括員工、委外廠商以及其他合作夥伴，應用於所有位置及資訊處理場所。

2.2. 資訊安全管理控制措施涵蓋 4 項控制領域，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，對本院帶來各種可能之風險及危害。控制領域如下：

2.2.1. 組織面控制措施。

2.2.2. 人員面控制措施。

2.2.3. 實體面控制措施。

2.2.4. 技術面控制措施。

2.3. 資通安全管理政策宜將考量下列事項之要求：

2.3.1. 營運策略及要求事項。

2.3.2. 法規、法律及契約。

2.3.3. 目前及預想之資訊安全風險及威脅。

2.4. 資通安全管理政策宜考量下列事項相關之聲明

2.4.1. 資訊安全之定義。

2.4.2. 資通安全目標或。

2.4.3. 引導與資訊安全相關之所有活動的原則。

2.4.4. 對滿足與資訊安全相關之適用要求事項的承諾。

2.4.5. 對資訊安全管理系統持續改善之承諾。

2.4.6. 資訊安全管理之責任指派。

2.4.7. 處理例外之程序。

2.5. 資通安全政策所對應之程序要求應包含：

2.5.1. 存取控制。

2.5.2. 實體及環境安全。

2.5.3. 資產管理。

2.5.4. 資訊傳送。

2.5.5. 端點裝置之安全組態及處置。

2.5.6. 網路安全。

2.5.7. 資通安全事件管理。

2.5.8. 系統及資料備份。

2.5.9. 密碼技術及金鑰管理。

2.5.10. 資訊分類分級及處理。

2.5.11. 技術脆弱性管理。

2.5.12. 安全系統開發。

2.6. 宜考量相關人員權限及能力，制定、審查及核可資通安全政策的責任。審查包括改善本院資通安全政策及管理程序之機會，並考量以下機會變更：

2.7. 本院的營運策略。

2.8. 本院之技術環境。

2.9. 法規及契約要求。

2.10. 資通安全風險。

2.11. 預想之資訊安全威脅環境。

2.12. 從資通安全事件中學習。

3. 資通安全管理政策

為了促使本院 ISMS 能貫徹執行、有效運作、監督管理、持續進行，藉由維護本院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，特頒佈資通安全管理政策。本政策為最高領導原則，旨在讓同仁於日常工作時有一明確指導原則，所有同仁及委外廠商皆有義務積極參與推動資通安全管理政策，以確保本院所有同仁之資料、資訊系統、設備及網路之安全維運，並期許所有人均能了解、實施與維持，以達資訊持續營運的目標。

3.1. 落實資通安全，強化服務品質

由全體同仁貫徹執行 ISMS，所有資訊作業相關措施，應確保業務資料之機密性、完整性及可用性，免於因外在之威脅或內部人員不當的管理，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持續進行監控、審查及稽核資訊安全制度的工作，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工作，每年持續進行適當的資通安全教育訓練，建立「資訊安全，人人有責」的觀念，促使同仁瞭解資通安全之重要性，促其遵守資通安全規定，藉此提

高資通安全智能及緊急應變能力，降低資訊安全風險，達成資通安全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

訂定重要資訊資產及關鍵性業務核心資通系統之緊急應變計畫及災害復原計畫，每半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，確保關鍵性業務核心資通系統持續運作，使本院主要業務順利執行。

3.4. 合理利用個資、防範個人資料外洩

對個人資料進行分類和評估，以確定保護的需求和措施。建立存取控制機制，於個資傳輸及共享方面採用加密與安全措施，定期評估委外廠商的遵守能力，並與委外廠商簽訂合約和協議以確保個資安全。強化員工教育訓練，增強個資保護意識。建立監控和審查機制，持續監視個資的使用、存取和傳輸，並及時檢測和應對異常活動或安全事件。確保不再需要時，個資能夠被安全且永久地刪除。

4. 組織背景

4.1. 了解組織及其背景

本院應依據「ISMS-P-019 組織全景評鑑管理程序書」之要求決定與其目的有關且影響達成其資訊安全管理系統預期成果能力者之內部及外部議題。

4.2. 了解利害關係者的需求跟期望

本院應依據「ISMS-P-019 組織全景評鑑管理程序書」之要求確定：

4.2.1. 與本院資訊安全管理系統相關的利害關係者。

4.2.2. 這些利害關係者的相關需求與期望。

4.2.3. 將如何經由資訊安全管理系統滿足前述相關要求。

4.3. 決定資訊安全管理系統的範圍

本院應決定資訊安全管理系統之邊界及適用性，以建立其範圍。在決定此範圍時應考慮：

4.3.1. 4.1 中提到的內部和外部議題。

4.3.2. 4.2 中提到的要求事項。

4.3.3. 本院履行之活動與其他組織履行之活動間的介面及相依性。

4.3.4. 範圍應記載於「ISMS-M-002 適用性聲明書」(SOA，Statement of applicability）中以文件化資訊提供。

4.4. 資訊安全管理系統

本院應根據本政策之要求建立、實施、維護和持續改進資訊安全管理系統。

5. 管理階層責任

5.1. 管理階層承諾

院部長官應通過下列方式展現對資訊安全管理系統的領導能力和承諾：

5.1.1. 確保資通安全政策和資通安全目標的建立並與本院的策略方向相容。

5.1.2. 確保將資訊安全管理系統要求事項整合到本院之各項過程中。

5.1.3. 確保資訊安全管理系統所需的資源可取得。

5.1.4. 傳達有效資訊安全管理的重要性，及符合資訊安全管理系統要求的重要性。

5.1.5. 確保資訊安全管理系統達成其預期的成果。

5.1.6. 指導和支援人員以促進資訊安全管理系統之有效性。

5.1.7. 宣導持續改進。

5.1.8. 當適用其他相關管理角色之責任範圍時，加以支持以展現其領導權。

5.2. 政策

院部長官應建立包含下列事項之資通安全政策：

5.2.1. 適合本院的目的。

5.2.2. 包括資通安全目標(見 6.2)或提供設定資通安全目標的框架。

5.2.3. 包括承諾滿足與資通安全相關的適用要求。

5.2.4. 包括對持續改進資訊安全管理系統的承諾。

5.2.5. 以文件化資訊提供。

5.2.6. 在本院內進行傳達。

5.2.7. 適用時，提供給關注方。

5.3. 組織角色、責任和權限

為確保資訊安全相關角色之責任及權限已於本院內指派並傳達，應遵循「ISMS-P-002 資通安全組織與權責管理程序書」等相關規定辦理。院部長官應指派下列責任及權限：

5.3.1. 確保資訊安全管理系統符合本文件之要求事項。

5.3.2. 向院部長官報告資訊安全管理系統之績效。

6. 規劃

6.1. 風險與機會的應對措施

6.1.1. 一般要求

6.1.1.1. 於規劃資訊安全管理系統時，本院應考量 4.1 所提及之議題及 4.2 所提及的要求事項，並決定需因應的風險及機會：

6.1.1.1.1. 確保資訊安全管理系統達成其預期成果。

6.1.1.1.2. 預防或減少非想要之影響。

6.1.1.1.3. 達成持續改善。

6.1.1.2. 本院應規劃下列事項：

6.1.1.2.1. 因應此等風險及機會之行動。

6.1.1.2.2. 執行下列事項之方法：

A. 將各項行動整合及實作於其資訊安全管理系統過程之中。

B. 評估這些行動之有效性。

6.1.2. 資訊安全風險評鑑

本院應於「ISMS-P-004 資訊安全風險管理程序書」定義及應用資訊安全風險評鑑過程：

6.1.2.1. 建立及維持資訊安全風險準則，包括：

6.1.2.1.1. 風險接受準則。

6.1.2.1.2. 執行資訊安全風險評鑑之準則。

6.1.2.2. 確保重複之資訊安全風險評鑑產生一致、有效及可比較之結果。

6.1.2.3. 識別資訊安全風險。

6.1.2.3.1. 應用資訊安全風險評鑑過程，以識別資訊安全管理系統範圍內資訊之機密性、完整性及可用性損害有關的風險。

6.1.2.3.2. 識別風險擁有者。

6.1.2.4. 分析資訊安全風險。

6.1.2.4.1. 評鑑若 6.1.2.3.1 中所識別之風險實現時，可能導致之潛在後果。

6.1.2.4.2. 評鑑 6.1.2.3.1 中所識別之風險發生的實際可能性。

6.1.2.4.3. 決定風險等級。

6.1.2.5. 評估資訊安全風險。

6.1.2.5.1. 以 6.1.2.1 中所建立之風險準則，比較風險分析結果。

6.1.2.5.2. 訂定已分析風險之風險處理優先序。

本院應保存關於資訊安全風險評鑑過程之文件化資訊。

6.1.3. 資訊安全風險處理

本院應於「ISMS-P-004 資訊安全風險管理程序書」定義並應用資訊安全風險處理流程，藉以：

6.1.3.1. 考慮風險評鑑結果，選擇適當的資訊安全風險處理選項。

6.1.3.2. 對所選定資訊安全風險處理選項，決定所有必須實作之控制措施。

6.1.3.3. 比較上述 6.1.3.2 中所決定之控制措施與 ISO27001 附錄 A 中者，並查證未忽略必要之控制措施。

6.1.3.4. 產生「ISMS-M-002 適用性聲明書」並包含以下內容：
- 必要的控制措施(見 6.1.3.2 和 6.3.3.3)。
- 將其納入的理由。
- 是否實施了必要的控制措施。
- 排除任何附錄 A 控制措施的理由。

6.1.3.5. 制定資訊安全風險處理計畫。

6.1.3.6. 取得風險擁有者對資訊安全風險處理計畫之核可，以及接受殘餘的資訊安全風險。

本院應依「ISMS-P-004 資訊安全風險管理程序書」辦理風險評鑑作業，並保存關於資訊安全風險處理過程之文件化資訊。

6.2. 資通安全目標和實現目標的規劃

本院應依循「ISMS-P-005 資通安全目標管理程序書」之要求在相關部門及層級建立資通安全目標。資通安全目標應：

6.2.1. 與資通安全政策保持一致。

6.2.2. 可以量測(若可行時)。

6.2.3. 考慮適用的資通安全要求，以及風險評鑑和風險處理的結果。

6.2.4. 受到監控。

6.2.5. 經過溝通。

6.2.6. 適當時進行更新。

6.2.7. 本院應保存資通安全目標之文件化資訊。

6.2.8. 於規劃如何達成資通安全目標時，本院應決定下列事項：

6.2.8.1. 要做什麼。

6.2.8.2. 需要哪些資源。

6.2.8.3. 由誰負責。

6.2.8.4. 何時完成。

6.2.8.5. 如何評估結果。

6.3. 變更管理

當確定需要對資訊安全管理體系進行變更時，應以預先規劃的方式進行變更；有關各項作業之變更管理，請參照本院各項作業之程序書辦理。

7. 支援

7.1. 資源

本院應決定並提供建立、實施、維護和持續改進資訊安全管理系統所需的資源。

7.2. 能力

本院宜依據「ISMS-P-010 人力資源安全管理程序書」之要求採取下列措施：

7.2.1. 決定於本院控制下執行工作，影響其資通安全績效人員之必要能力。

7.2.2. 確保此等人員於適當教育、訓練或經驗之基礎上能勝任。

7.2.3. 於適當時，採取取得必要能力之行動，並評估所採取行動之有效性。

7.2.4. 保存適切之文件化資訊，作為勝任之證據。

7.3. 認知

本院控制下執行工作之人員，應認知下列事項：

7.3.1. 資通安全政策。

7.3.2. 其對資訊安全管理系統有效性之貢獻，包括改善之資訊安全績效的益處。

7.3.3. 未遵循資訊安全管理系統要求事項之可能影響。

7.4. 溝通

本院應於「ISMS-P-002 資通安全組織與權責管理程序書」規範相關於資訊安全管理系統之內外部溝通或傳達的需要，包括下列事項。

7.4.1. 溝通什麼。

7.4.2. 何時溝通。

7.4.3. 和誰溝通。

7.4.4. 如何溝通。

7.5. 文件化資訊

7.5.1. 一般要求

本院之資訊安全管理系統應包括下列內容：

7.5.1.1. 本文件要求之文件化資訊。

7.5.1.2. 由本院所決定對資訊安全管理系統有效性，必要之文件化資訊。

7.5.1.2.1. 組織規模，以及其活動、過程、產品及服務之類型。

7.5.1.2.2. 各過程及其互動之複雜度。

7.5.1.2.3. 人員之能力。

7.5.2. 制訂和更新

於制訂及更新文件化資訊時，應依循「ISMS-P-001 文件與紀錄管理程序書」之要求，確保適切之下列項目：

7.5.2.1. 識別和描述（例如標題、日期、作者或索引號碼）。

7.5.2.2. 格式（例如語言、軟體版本、圖形）和媒體（例如紙本、電子）。

7.5.2.3. 適切性及充分性之審查及核准。

7.5.3. 文件化資訊之控制

應控制資訊安全管理系統及本文件要求之文件化資訊，以確保下列事項：

7.5.3.1. 其於需要處及需要時為可用及適用。

7.5.3.2. 其受適切保護(例：防止漏失機密性、不當使用或完整性漏失)。

為管制文件化資訊，本院應於適當時，闡明下列活動。

7.5.3.3. 派送、存取、檢索及使用。

7.5.3.4. 儲存及保存，包括可讀性之保存。

7.5.3.5. 變更之控制(例：版本控制)。

7.5.3.6. 留存及屆期處置。

於適當時，應依循「ISMS-P-001 文件與紀錄管理程序書」之要求識別及控制由本院所決定對資訊安全管理系統之規劃及運作為必要之外部來源的文件化資訊(外來文件)。

8. 運作

8.1. 運作之規劃及控制

本院應策劃、實施和控制滿足要求所需的過程，並通過以下方式實施第 6 章確定的措施。
—建立過程之準則。
—根據準則實施過程之控制措施。

本院應保存文件化資訊，其程度必須具有足以達成其過程已依規劃執行之信心。

本院應控制所規劃之變更，並審查非預期變更之後果，必要時採取行動以減輕任何不利影響。

本院應依「ISMS-P-018 委外作業管理程序書」辦理委外作業以確保有關資訊安全管理系統之外部提供的過程、產品或服務受到控制。

8.2. 資訊安全風險評鑑

本院應依規劃之期間，或當重大變更被提出或發生時，依「ISMS-P-004 資訊安全風險管理程序書」之規範，執行資訊安全風

險評鑑。
本院應保存資訊安全風險評鑑結果之文件化資訊。

8.3. 資訊安全風險處理
本院應依「ISMS-P-004 資訊安全風險管理程序書」之規範實作資訊安全風險處理計畫。
本院應保存資訊安全風險處理結果之文件化資訊。

9. 績效評估

9.1. 監控、量測、分析和評估
本院應決定下列事項：

9.1.1. 需要監督及量測之事項，包括資訊安全過程及控制措施。

9.1.2. 監督、量測、分析及評估之適用方法，以確保有效的結果，所選擇的方法應產生可比較且可重現的結果才被視為有效。

9.1.3. 何時執行監督及量測。

9.1.4. 應由誰監督及量測。

9.1.5. 監督及量測結果應核實被分析及評估。

9.1.6. 應由誰分析及評估這些結果。

9.1.7. 應保存適切之文件化資訊，作為監督及量測結果的證據。

9.1.8. 應評估資訊安全管理系統之資訊安全績效及有效性。

9.2. 內部稽核

9.2.1. 一般要求
本院應依「ISMS-P-007 資訊安全稽核管理程序書」至少每半年定期執行一次內部稽核，以提供資訊安全管理系統之下列資訊：

9.2.1.1. 是否符合下列事項：

9.2.1.1.1. 本院對其資訊安全管理系統之要求事項。

9.2.1.1.2. 本文件之要求事項。

9.2.1.2. 得到有效實施及維持。

9.2.2. 內部稽核方案

本院應依「ISMS-P-007 資訊安全稽核管理程序書」之要求規劃、建立、實施和維護稽核方案，包括頻率、方法、職責、計劃要求事項和報告。

在建立內部稽核計畫時，本院應考慮相關過程的重要性和先前稽核的結果。

執行內部稽核時應：

9.2.2.1. 定義每次稽核的標準和範圍。

9.2.2.2. 選擇稽核人員並進行稽核，以確保稽核過程的客觀性和公正性。

9.2.2.3. 確保將稽核結果報告給相關管理階層。

9.2.2.4. 保存文件化資訊作為稽核計畫及稽核結果之證據。

9.3. 管理審查

9.3.1. 一般要求

本院「資通安全暨個人資料保護管理會」至少每年召開一次管理審查會議，審查本院之資訊安全管理系統，以確保其持續的合宜性、適切性及有效性。

9.3.2. 管理審查輸入事項

管理審查應包括對下列事項之考量：

9.3.2.1. 先前管理審查之措施的處理狀態。

9.3.2.2. 與資訊安全管理系統相關之內部及外部議題的變更。

9.3.2.3. 與資訊安全管理系統有關的利害關係方的需求和期望的變化。

9.3.2.4. 資訊安全績效之回饋，包括下列之趨勢：

9.3.2.4.1. 不符合事項與矯正措施之執行狀況。

9.3.2.4.2. 監督與量測結果。

9.3.2.4.3. 稽核的結果。

9.3.2.4.4. 資通安全目標的實現。

9.3.2.5. 資通安全維護計畫實施情形。

9.3.2.6. 利害相關團體的回饋。

9.3.2.7. 風險評鑑結果與風險處理計畫狀態。

9.3.2.8. 持續改善的機會。

9.3.3. 審查輸出

管理審查之輸出應包括與持續改善機會有關之決策，以及任何對資訊安全管理系統變更之需要。

本院應保存文件化資訊，以作為管理審查結果之證據。

10. 改善

10.1. 持續改進

本院應持續改善資訊安全管理系統之合宜性、適切性及有效性。

10.2. 不符合及矯正措施

不符合項目發生時，本院應依「ISMS-P-008 矯正及預防管理程序書」有下列作為：

10.2.1. 適用時，對不符合事項作出回應：

10.2.1.1. 採取措施管控並矯正之。

10.2.1.2. 處理其後果。

10.2.2. 評估消除不符合項目之原因所需採取的措施，使其不再發生且不於他處發生：

10.2.2.1. 審查不符合項目。

10.2.2.2. 決定不符合項目之原因。

10.2.2.3. 判定是否有類似或潛在之不符合事項存在。

10.2.3. 實作所有所需行動。

10.2.4. 審查所有所採取矯正措施之有效性。

10.2.5. 必要時，對資訊安全管理系統進行變更。

10.2.5.1. 矯正措施應切合所遇到之不符合項目之影響。

10.2.5.2. 本院應保存文件化資訊，以作為下列事項之證據。

10.2.6. 不符合項目之本質及後續採取之所有行動。

10.2.7. 任何矯正措施之結果。

11. 審查

11.1. 本政策每年應至少評估檢討一次，以反映本院資通安全需求、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. 資通安全管理政策及特定主題政策之審查，宜將管理審查及稽核的結果納入考量。

11.3. 變更政策時宜維持一致性時，並考量其他相關政策之審查及更新。

11.4. 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院所屬職員及與本院連線作業之有關機關（構）、委外廠商，修正時亦同。