內政部國土測繪中心

資訊安全管理系統政策文件

文件編號： ISMS-01000000

版　　次： V2.94

文件日期： 110 年 7 月 12 日

機密等級： 普通

National Land Surveying and Mapping Center

文件制/修訂紀錄

制/修訂 版次	制/修訂 日期	制/修訂 說明	作 者	備 註
1.0	961116	初版發行	ISMS 工作小組	
2.0	971014	增列「角色及責任」、「人員審查」、「考核獎懲」及「資通安全教育訓練」等事項對應程序文件之說明並配合 ISO 17799 及 CNS 17799 之廢止與 ISO 27002 及 CNS27002 之訂頒，修正依據標準。	ISMS 工作小組	
2.1	980213	依據程序文件名稱變更修訂。	ISMS 工作小組	
2.2	1001013	修正 ISMS 目標及電腦機房名稱。	ISMS 工作小組	
2.3	1031024	1. 前言，增加考量組織全景內容。 2. 修正二~四階程序文件之核定，依 100 年 11 月 8 日簽奉核可知授權人員核定。	蔡汶諭	
2.4	1041014	文字修正 1. ISO27001 標準要求事項第 4 節至第 8 節修正為 10 節 2. 一般要求修正內外部議題與關注方(interested party)，以及法令、法規及義務之要求 3. 事故修正為事件	蔡汶諭	
2.5	1060213	增加 ISMS 目標中的機房「電力及空調服務」，核心系統之可用性目標。	陳建男	
2.6	1061016	增加核心資訊系統等文字	陳建男	
2.7	1080412	因應資通安全管理法修正相關敘述及增列依據。	陳建男	
V2.08	1080927	修正版次敘述及組織名稱	蕭宇辰	
V2.09	1081219	修正「資訊系統」為「資通系統」	蕭宇辰	
V2.10	1090120	1. 修改適用範圍將各測量隊及所屬辦公室納入。 2. 資訊系統修改為資通系統。	蕭宇辰	

V2.90	1090416	1. 調整版次敘述。 2. 依據 ISO27001 標準辦理年度檢視，並修正部分內容。	蕭宇辰	
V2.91	1090708	修正「資訊安全」為「資通安全」	蕭宇辰	
V2.92	1091014	新增非上班時間之相關規定	蕭宇辰	
V2.93	1100505	1. ISMS 適用範圍為全機關，配合修正相關文字。 2. 修正誤植文字。	蕭宇辰	
V2.94	1100712	針對上移至內政部之系統服務，新增相關規定。	蕭宇辰	

目　　錄

壹、 ISMS 政策與目標

一、 前言

內政部國土測繪中心(以下簡稱本中心)致力於辦理國家基礎測繪工作，建立全國性測繪成果，以提供各界之參考應用，並配合 e 化世紀的生活，提供迅速、便捷、精確的服務，型塑優質的測繪服務品質，深獲社會大眾之好評與信賴。

有鑑於資訊科技之快速發展，各項服務及日常運作日益仰賴資通系統提供服務，如何確保資通安全已成為當今重要之議題，因此本中心(96 年 11 月 16 日改制前為內政部土地測量局)除已於 92 年 12 月 23 日發布「資通安全政策」，希望全體同仁共同遵循外，為強化資通系統核心之電腦機房安全管理及核心資通系統持續維運，特考量組織運作全景，針對本中心「電腦機房安全管理及核心資通系統」訂定本資訊安全管理系統(以下簡稱本系統或 ISMS)政策與目標，並建立系統與紀律化之流程制度，提供各相關單位之作業依據，以提昇資通安全管理與應變能力。

內政部國土測繪中心「資訊安全管理系統政策文件」(以下簡稱本政策文件)說明本中心資訊安全管理系統之整體概觀，以提供社會大眾及同仁對本中心整體資通安全管理制度之瞭解。

二、 ISMS 政策

確保本中心電腦機房設備、網路及核心資通系統之安全，以避免當發生人為疏失、蓄意破壞或自然災害時，遭致資產不當使用、洩漏、竄改、毀損、遺失等情事，影響本中心作業或損及民眾權益。

三、 ISMS 目標

(一) 目標

1. 通過並維持 ISO27001/CNS27001 驗證。
2. 確保本中心電腦機房之網路、電力及空調服務，因意外或操作錯誤造成無法使用，上班時間持續達 4 小時以上或非上班時間持續達 12 小時以上之次數，每年不得高於 2 次。
3. 確保本中心電腦機房因資通安全事件造成機密等級以上資料外洩，每年不得有 1 件。
4. 確保核心資通系統之可用性，因意外或操作錯誤造成無法使用，上班時間持續達 4 小時以上或非上班時間持續達 12 小時以上之次數，每年不得高於 4 次。

(二) 目標的執行

本中心相關單位主管應督導部屬達成本中心「電腦機房安全管理及核心資通系統」ISMS 目標。

(三) 目標的達成

由本中心資訊安全管理系統工作小組針對 ISMS 目標每年達成情況進行評估，並陳報本中心資通安全推行小組。

四、 適用範圍

適用於本中心全機關電腦之網路設備(如核心交換器、路由器、交換器及光纖配接盒)、網路基礎設施(如防火牆、DNS 伺服器、防毒閘道伺服器及個人電腦防毒伺服器)、環境控制設備、機房空間及實體基礎設施(如 UPS、機櫃、空調系統、消防設備等)及資通系統與資料庫之開發、日常維運與變更管理作業。

五、 驗證範圍

(一) 本中心核心資通系統：測繪資訊課國土測繪圖資 e 商城及控制測量課 e-GNSS 即時動態定位系統之 ISMS 維運。

(二) 本中心電腦機房包含至善樓電腦機房及地籍資料庫電腦機房，範圍涵蓋機房內之各項設備及網路安全等：

1. 至善樓機房(至善樓 5 樓)

   地址：臺中市南屯區黎明路 2 段 497 號 5 樓。

2. 地籍資料庫機房(地籍資料庫 4 樓)

   地址：臺中市南屯區博愛街 80 巷 51 號 4 樓。

六、 依據標準

本中心 ISMS 係依據以下標準制定：

(一) 本中心資通安全政策。

(二) 國家標準：CNS27001/ CNS 27002。

(三) 國際標準：ISO27001/ ISO27002。

(四) 相關法規：

1. 資通安全管理法。
2. 資通安全管理法施行細則。
3. 資通安全責任等級分級辦法。
4. 資通安全事件通報及應變辦法。
5. 資通安全情資分享辦法。
6. 公務機關所屬人員資通安全事項獎懲辦法。
7. 行政院及所屬各機關資通安全管理要點。
8. 行政院及所屬各機關資通安全管理規範。

貳、 資訊安全管理系統(ISMS)

ISMS 係依據 ISO27001/CNS27001 標準要求事項第 4 節至第 10 節之各項要求來進行管理系統之建立、實作、運作、監視、審查、維持與改進，詳述於後。

一、 一般要求

依據本中心內外部議題與關注方(interested party)，以及法令、法規及義務之要求，規劃整體營運活動與所面臨的風險，建立、實作、運作、監視、審查、維持與改進 ISMS。ISMS 採用之過程如下圖 2-1 所示之 PDCA(Plan, Do, Check, Act)模型為基礎。

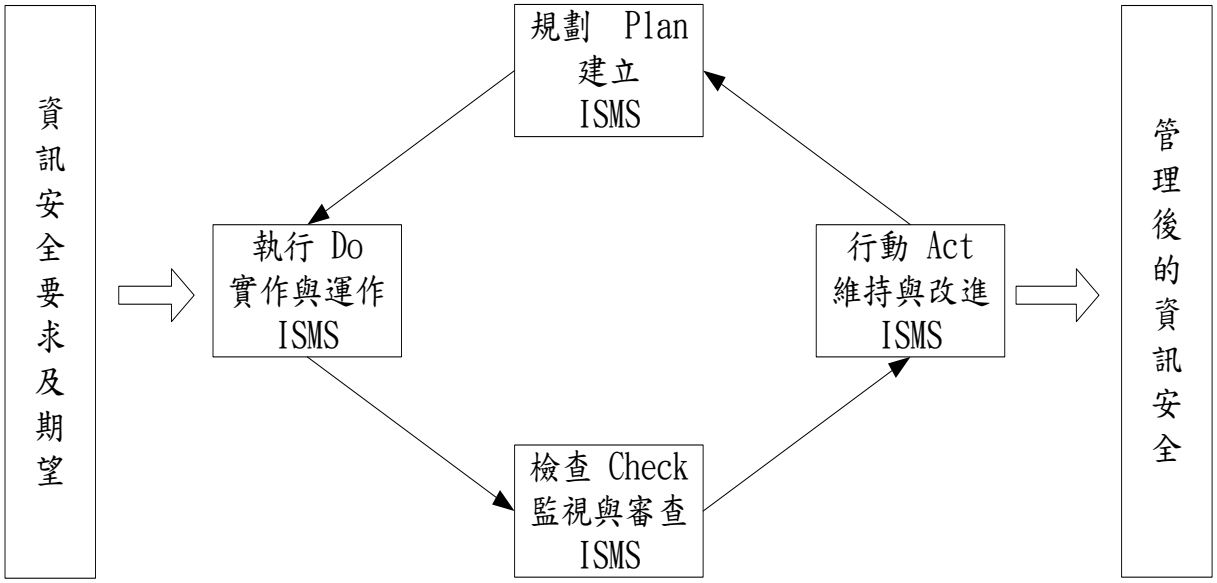

圖 2-1：ISMS 持續改善之 PDCA 模型

二、 ISMS 之建立與管理

(一) 為統籌本中心資通安全相關業務之整體規劃、評估、督導、協調、推動及資安事件處理等事項，特設置跨單位之「資通安全推行小組」，並於推行小組下設立「資訊安全管理系統工作小組」，以執行資訊安全管理系統之維運作業，詳見「資訊安全管理系統組織管理程序」。

(二) 建立本中心 ISMS，含風險評鑑、識別風險、分析及評估各項風險、風險處理、剩餘風險的核准、管理階層之授權、適用性聲明。

(三) 實作與運作本中心 ISMS，含風險處理計畫擬定、量測評鑑控制措施的有效性、實作訓練與認知計畫、管理 ISMS 運作及資源。

(四) 監視與審查本中心 ISMS，含執行監視與審查程序、定期審查 ISMS 有效性、量測控制措施的有效性、審查風險評鑑及剩餘風險的等級與已識別的可接受風險、維持與改進 ISMS。

(五) 本中心針對資訊業務的資通安全以及法規規定，以科學的方法進行風險評鑑，並依據風險評鑑結果進行風險處理計畫，詳見「資訊安全管理系統風險評鑑與管理程序」。

(六) 本中心對於 ISMS 必要之項目訂定控制措施並據以實施。

(七) ISMS 於執行上之問題，其所對應之各項矯正與預防措施處理，詳見「資訊安全管理系統稽核程序」之矯正及預防措施處理。

(八) 確保資通安全事件與弱點，能夠及時發現並採用一致且有效的作法管理資通安全事故，並建立有效且快速之通報系統，以期快速回復至正常狀態，詳見「資訊安全管理系統事故管理程序」。

(九) 在「電腦機房」的安全區域內，必須防範核心業務資訊，不遭受未授權的存取、破壞及干擾。另各資產於建置、調整或停用前，應納入安全需求，辦理資產安全規格分析、維護及保護，防止資產的遺

失、損害、竊盜或破解，防止組織活動之中斷，詳見「資訊安全管理系統實體與環境安全管理程序」。

(一〇) 為確保核心資通系統，於開發作業時安全評估及管理機制，訂定相關管理規範，詳見「資訊安全管理系統資通系統開發管理程序」。

(一一) 為確保網路服務及正確與安全地操作資訊處理設施、容量規劃與檢視、安全防護措施及管理機制，訂定相關管理規範，詳見「資訊安全管理系統網路安全管理程序」以及「資訊安全管理系統通訊與操作管理程序」。

(一二) 為避免資通系統因未授權之存取而使機密性或敏感性資料遭不當使用，應考量人員職務授予相關權限，必要時得施行加解密及身分鑑別機制，以加強資料之安全，達到較高安全防護的目標。資通系統的存取控制詳見「資訊安全管理系統存取控制管理程序」。

(一三) 有關資通安全之安全需求規劃、委外合約資通安全規範、資通系統異動上線管理等，詳見「資訊安全管理系統供應商管理程序」及「資訊安全管理系統資通系統上線管理程序」。

(一四) 營運持續需求須完整規劃，以支援相關資通系統，詳見「資訊安全管理系統資訊業務營運持續管理程序」。

(一五) 為確保相關同仁能瞭解所負資通安全責任及違反安全政策的後果，有關人員「角色及責任」、「人員審查」、「考核獎懲」及「資通安全教育訓練」等事項，詳見「資訊安全管理系統人員安全管理程序」。

(一六) 本中心配合內政部辦理資訊向上集中作業，放置於內政部內政資料中心或其機房環境等資通訊服務，應依內政部資通安全相關規定辦理。

三、 ISMS 文件架構

本 ISMS 文件,係為管制本中心資通安全各項管理性及支援性作業而建立之必要程序，文件架構如下頁圖 2-2 所示，包含以下各類制度文件：

(一) 一階文件

包含本 ISMS 政策文件及適用性聲明文件，提供本中心資訊安全管理系統一個整體性的描述,說明本中心 ISMS 實施之範圍、ISMS 政策、相關程序與文件、並描述本中心各項流程間之交互關係。所有 ISMS 相關之人員，均應熟悉本政策文件之政策及執行目標，並將其運用為各種程序、方法及工作規範之指導原則。

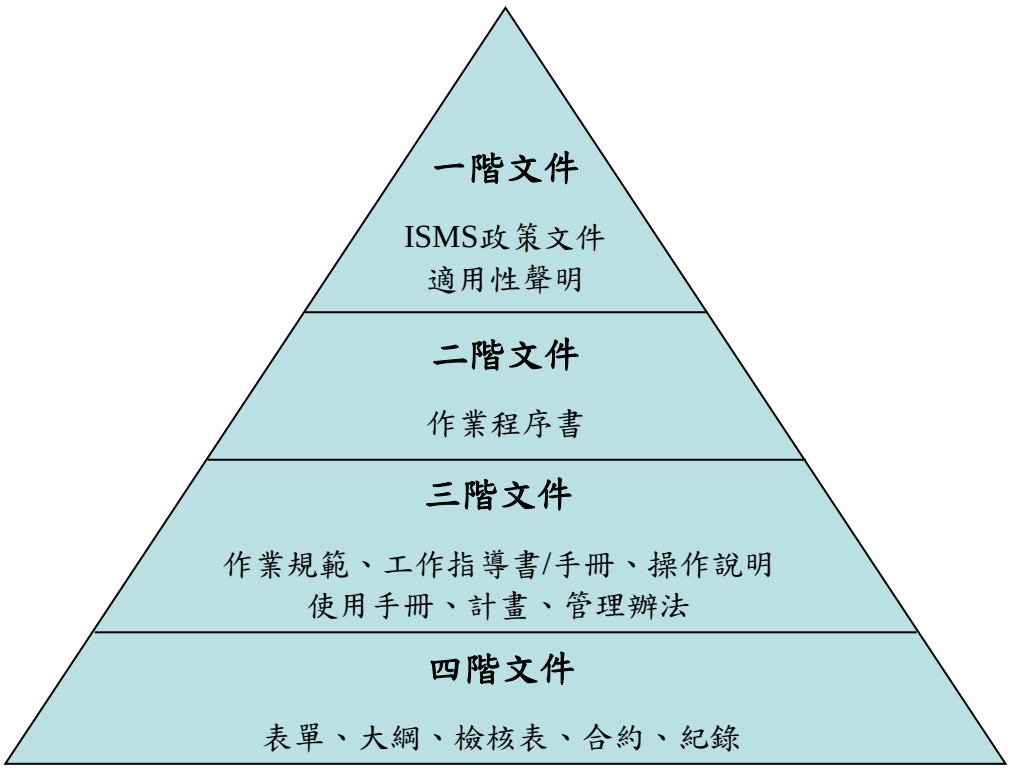

圖 2-2：ISMS 文件架構圖

(二) 二階文件

依據 ISMS 政策及 ISO27001/CNS27001 標準之管理原則，所制定之各項程序文件，規劃及發展資通安全相關之各項活動與服務所

需之組織運作流程，並詳述於各程序文件中。

每一流程可能包含數項相關之作業，每一份流程作業程序書中將再依其作業特性，建立一到數份之程序，以分別說明每一作業之執行程序。

(三) 三階文件

為確保本政策文件中各項資通安全規劃、維運及支援作業(Operation Support)工作於必要時能有適當之指引，本中心針對流程中之關鍵技術或作業另訂說明文件，如作業指導書(或手冊)、作業規範、操作說明(或使用手冊)、計畫、管理辦法等，以作為相關作業執行時之指導。

(四) 四階文件

為利於落實本中心各項作業，並達到制度化與一致化之目的，對於 ISMS 之各項要求，於流程執行過程中提供細部之表單、大綱、及檢核表等，以利相關人員依照規定之表單及資料執行各項作業，並記錄作業執行結果。此類表單，可以採用電子媒體方式處理，但仍必須保留該表單必要之資料。

(五) 文件化

ISMS 之一、二、三、四階文件應加以文件化，並注意適時更新，讓有需要的使用者均可隨時取得。

(六) 文件與紀錄管制

建立符合 ISMS 有效運作之文件與紀錄管控，詳見「資訊安全管理系統文件與紀錄管理程序」。

參、 ISMS 內部稽核

ISMS 工作小組應規劃內部稽核作業，將稽核範圍、準則、項目、方法及前次稽核的結果納入考量，每年至少辦理一次內部稽核，以判定 ISMS 控制目標、控制措施、過程及程序是否符合下列要求：

一、 符合 ISO27001/CNS27001 及相關外部、內部法規及相關規範。

二、 符合已知的資通安全要求。

三、 選用之控制措施確實執行與維護。

四、 依照預定時程落實執行。

稽核時所發現不符合項目，須填寫「資通安全矯正及預防措施處理表」，受稽核單位應進行改善措施並如期完成，ISMS 工作小組應持續追蹤控管改善措施之落實，詳見「資訊安全管理系統稽核程序」。

肆、 ISMS 之改進

一、 依「資訊安全管理系統組織管理程序」對所量測及監控之控制措施的有效性進行審查及判定。

二、 依「資訊安全管理系統稽核程序」辦理內部稽核作業，針對 ISMS 所產生的異常狀況或潛在問題，採取適當處理及研擬改善措施，持續精進本中心 ISMS 作業。

三、 依「資訊安全管理系統資訊業務營運持續管理程序」及「資訊安全管理系統事件管理程序」確保本中心如發生資通安全事件能及時採取適當應變措施，降低資通安全事件影響範圍及對本中心營運帶來之風險。

四、 依「資訊安全管理系統組織管理程序」實施管理審查，以確保 ISMS 之政策和目標的適宜性和有效性。

五、 依「資訊安全管理系統法規適用性管理程序」避免違反任何法律、行政命令、契約、標準、安全技術等規範。

六、 ISMS 各項控制措施之對應程序文件，詳見「適用性聲明(SOA)」。

伍、 ISMS 文件之制定

一、 一階文件之制定，係按資通安全推行小組所提出資通安全政策方向與目標後，由 ISMS 工作小組研提，經資通安全推行小組審查，簽奉主任核定後實施，修訂時亦同。

二、 二、三、四階文件之制定，由資通安全推行小組授權 ISMS 工作小組各分組研訂，經 ISMS 工作小組審查，第二階文件簽奉 ISMS 工作小組召集人核定後實施，三、四階文件由業務單位主管核定，修訂時亦同。

陸、 參考文件

無

柒、 相關表單文件

一、 ISMS-01000001 組織全景。

附件一、 附錄：詞彙介紹

一、 資產（asset）：對組織有價值的任何事物。

二、 可用性（availability）：經授權個體因應需求之可存取及可使用的性質。

三、 機密性（confidentiality）：使資訊不可用或不揭露給未經授權之個人、個體或過程的性質。

四、 資通安全（information security）：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。

五、 資通安全事件（information security event）：指系統、服務或網路狀態經鑑別而顯示可能有違反資通安全政策或保護措施失效之狀態發生，影響資通系統機能運作，構成資通安全政策之威脅。

六、 資通安全事故（information security incident）：單一或一連串有顯著機率可能危害營運作業與威脅資通安全之非所欲或非預期的資通安全事件。

七、 資訊安全管理系統（Information Security Management System, ISMS）：整體管理系統的一部份，以營運風險導向（作法）為基礎，用以建立、實作、運作、監視、審查、維持及改進資通安全。

八、 完整性（integrity）：保護資產的準確度(accuracy)和完全性(completeness)的性質。

九、 剩餘風險（residual risk）：風險處理後所剩餘的風險。

十、 風險接受（risk acceptance）：決定接受某風險。

十一、風險分析（risk analysis）：系統性的使用資訊，以識別緣由與估計

風險。

十二、風險評鑑（risk assessment）：風險分析與風險評估的整個過程。

十三、風險評估（risk evaluation）：把預估的風險和已知的風險準則進行比較的過程，以決定風險的顯著性。

十四、風險管理（risk management）：藉由協調各項活動以指導與控管組織之有關風險。

十五、風險處理（risk treatment）：選擇與實作措施的過程藉以修正風險。

十六、適用性聲明（statement of applicability）：描述與組織之 ISMS 相關且對其適用之各項控制目標與控制措施的已文件化聲明。

十七、核心資通系統：支持本中心關鍵基礎設施(CI)及核心業務運作之資通系統，並依據「資通安全責任等級分級辦法」附表九所定資通系統防護需求分級原則完成資通系統分級後，等級為「高」者。