法務部調查局

資訊安全政策

安全分級：□ 機敏 □ 內部使用 ■ 公開

文件編號：MJIB-A-001

版次：V2.0

中華民國97年11月7日

文件修訂履歷

制/修版本	制/修日期	變更說明	制/修單位	制/修人員	核准人員
1.0	96/12/28	新版制訂	資訊室		ISMS 推動小組
2.0	97/11/7	資訊安全目標表	資訊室		ISMS 推動小組

目　次

壹、 目的 1
貳、 依據 1
參、 資訊安全方針 1
肆、 資訊安全範圍 1
伍、 資訊安全目標 2
陸、 組織權責 2
柒、 運作機制 3
捌、 文件系統 3
玖、 管理責任 3
壹拾、 內部稽核 5
壹拾壹、 管理審查 5
壹拾貳、 體系改進 6

壹、目的

本局為強化資訊安全管理，建立安全及可信賴之資訊環境，確保資料、系統、設備及網路安全，維護國家安全，保障民眾權益，特訂定本政策。

貳、依據

本政策係依據「行政院及所屬各機關資訊安全管理要點」，並參酌「行政院及所屬各機關資訊安全管理規範」、行政院頒「建立我國通資訊基礎建設安全機制計畫」、法務部頒「法務部及所屬機關資訊安全政策」等有關法令，及 ISO 27001 標準，考量本局業務需求，訂定法務部調查局資訊安全管理系統政策及相關標準作業程序，以建立資訊安全管理機制、強化資訊安全防護，提昇資訊安全之水準。

參、資訊安全方針

資訊安全，人人有責。

肆、資訊安全範圍

一、資訊安全權責分工。

二、人員管理及資訊安全教育訓練。

三、電腦系統安全管理。

四、網路安全管理。

五、系統存取管制。

六、系統發展及維護安全管理。

七、資訊資產安全管理。

八、實體及環境安全管理。

九、業務永續運作計畫管理。

十、資訊安全稽核。

十一、資訊安全事件通報管理。

伍、資訊安全目標

一、保障資訊之機密性及防止非法使用

二、確保資產之可用性、完整性

三、確保業務運作之有效性及持續性

四、確保同仁對資訊安全有一定認知

五、確保資安措施符合政策及法令要求

陸、組織權責

本局為確保資訊安全管理系統能有效運作與實踐，明訂相關組織及權責，以推動及維持資訊安全管理系統各類管理、執行與查核等工作之進行。

一、組織架構

本局設置「法務部調查局資訊安全管理系統推動小組」(以下簡稱本局 ISMS 推動小組)，由本局副局長擔任召集人，負責核定資訊安全管理系統相關之政策、目標與作業要點，並定期召開會議審查資訊安全管理系統推動情形。另由 ISMS 推動小組執行秘書兼任「法務部調查局推動資訊安全管理系統工作小組」(以下簡稱本局 ISMS 工作小組）組長，由資訊室主任擔任，負責擬定資訊安全管理系統相關之政策與作業要點草案後，陳本局 ISMS 推動小組審查通過並簽奉局長核可後公布實施。

二、權責

本局 ISMS 推動小組與 ISMS 工作小組之工作權責，請參考「法務部調

查局資訊安全管理組織作業要點」。

柒、運作機制

本局係依照 ISO 27001 標準，採用「規劃與建立、實施與運作、監督與查核、維護與改進」(Plan-Do-Check-Act, PDCA)之循環運作模式，建立資訊安全管理系統，並維繫其有效運作與持續改進。

一、規劃與建立(Plan)

依據本局整體策略與目標，建立資訊安全管理系統。

二、實施與運作(Do)

依據評估規劃之結果，建立或修正應有之管控機制。

三、監督與查核(Check)

監督資訊安全管理系統各項作業之落實執行，並查核其有效性。

四、維護與改進(Act)

根據監督查核之結果與建議，改進並維護系統運作。

捌、文件系統

一、文件管制

本局資訊安全管理系統相關文件之管制、核發與變更均應依文件管理相關規定辦理。

二、紀錄管制

本局資訊安全管理系統運作所產生之文件、表單或紀錄，應依相關規定妥善管理，並訂定保存期限與核閱權限以為管制。

玖、管理責任

一、管理階層承諾

(一)對於本局資訊安全管理系統與改進各項作業，管理階層具體展現其承諾如下：

1.訂定資訊安全政策

2.確認資訊安全控制目標與計畫之建立

3.訂定資訊安全之角色與職責

4.宣導遵守資訊安全政策與法令規章、達成資訊安全控制目標及持續改善之重要性

5.提供資訊安全管理系統各項作業充足之資源

6.決定風險可接受水準

7.執行資訊安全管理系統之管理審查作業

(二)以上由本局 ISMS 工作小組擬定草案，並陳本局 ISMS 推動小組審查通過並簽奉局長核可後公布實施。

二、資源管理

(一)確認並提供執行下列事項所需之資源

1.資訊安全管理系統之建立、實施、運作與維護

2.確認資訊安全管理系統文件可符合業務需求

3.闡明法令規章之要求與契約之安全義務

4.正確運用管制措施，以確實維護資訊安全

5.執行必要之審查，並對結果做適當之反應與處理

6.改善資訊安全管理系統之有效性

(二)確認參與資訊安全管理系統作業之人員均具備工作所需之相關職能

1.確立資訊安全管理系統運作相關人員必須具備之職能

2.評估職能訓練與相關措施之有效性

3.建立並維護教育訓練、技能、經驗與資格之相關紀錄

壹拾、內部稽核

資訊安全管理系統應定期進行安全稽核，以檢討管制目標、管制措施與程序是否遵循相關標準、法令規章或資訊安全需求，並依預期規劃有效執行與維持。內部稽核作業之規劃應考量稽核對象或範圍之重要性與現況，定義稽核之標準、範圍、頻率與方法，確認稽核人員之客觀與公正，並妥善保存相關紀錄。受稽核單位對於不符合事項應及時採行改善措施，並追蹤驗證其有效性。

壹拾壹、管理審查

本局資訊安全管理審查作業由 ISMS 推動小組執行，以持續確保資訊安全管理系統運作之適切、充足與有效，審查範圍包括資訊安全管理系統改進方案與變革需求之評估，審查結果應予詳實記錄並妥善保存。

一、管理審查輸入

(一)資訊安全管理系統稽核與審查之結果

(二)來自利害相關團體之回應與要求

(三)改進資訊安全管理系統績效技術或程序

(四)預防與矯正措施之執行狀況

(五)先前風險評鑑未適切提出之脆弱性或威脅

(六)有效性量測的結果

(七)先前管理階層審查之跟催措施

(八)可能影響資訊安全管理系統之任何變更

(九)改進之建議

二、管理審查輸出

(一)資訊安全管理系統有效性之改進

(二)風險評鑑與風險處理計畫之更新

(三)為因應可能影響資訊安全管理系統之內部或外部事件，必要時，影響資訊安全之流程應予修訂，包括

1.營運要求

2.安全要求

3.影響既有營運要求之營運過程

4.法令或法規要求

5.合約的義務

6.風險等級及/或風險可接受程度

(四)資源需求

(五)控制措施如何量測之改進

壹拾貳、體系改進

一、持續改善

透過資訊安全相關規範、查核結果、事件監控分析、矯正預防措施及管理審查等機制，持續增進資訊安全管理系統之有效性。

二、預防措施

採取適當的控管措施，以預防不符合事項之發生。預防措施之作業程序如下：

(一)指出潛在之不符合事項及其原因

(二)決定及確認所需執行之預防措施

(三)記錄預防措施之執行結果

(四)審查預防措施執行之結果

(五)分析風險變化情形，並特別注意明顯變化之風險

三、**矯正措施**

採取適當的控管措施，以減少資訊安全管理系統建置與運作過程中所發現之不符合事項，並防止再度發生。矯正措施之作業程序如下：

(一)指出資訊安全管理系統建置與運作之不符合事項

(二)確認不符合事項的原因

(三)評估為防範再發生所需採行之措施

(四)決定及實作所需之矯正措施

(五)記錄矯正措施之執行結果

(六)審查矯正措施之執行結果

四、**矯正措施之實行時機**

(一)違反國家政策與法令規範

(二)違反本政策規定

(三)內、外部稽核發現之不符合事項

(四)違反資訊安全目標與控制有效性量測標準

(五)發生資訊安全事故

(六)機敏資料或文件被未經授權存取