法務部及所屬機關資訊安全政策

法務部

95 年 12 月 04 日函頒

目　錄

一、目的

法務部(以下簡稱本部)為推動本部及所屬各機關強化資訊安全管理，建立安全及可信賴之法務體系資訊環境，確保資料、系統、設備及網路安全，保障民眾權益，特訂定本政策。

二、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」等有關法令，及ISO27001資訊安全管理系統標準，考量本部業務需求，訂定資訊安全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。

三、資訊安全方針

資訊安全，人人有責。

四、資訊安全定義

所謂資訊安全係將管理程序及安全防護技術應用於各項資訊作業，包含作業執行時所使用之各項資訊系統軟、硬體設備、存放各種資訊及資料之檔案媒體及經由列表機所列印之各式報表，以確保資訊蒐集、處理、傳送、儲存及流通之安全。

五、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。

六、資訊安全目標

(一)保障資訊之機密性及防止非法使用

非法存取資訊之事件，各機關每年發生次數不得超過5次。

(二)確保資產之可用性、完整性

因資安事件導致服務停頓，各機關每半年小於3次(含)以下，每次不得超過36小時。

(三)確保業務運作之有效性及持續性

每年至少需執行2次「營運持續管理計畫」之情境演練，並於2年內完成業務持續運作計畫內所有情境之演練。所屬機關每年至少執行1次演練。

(四)確保同仁對資訊安全有一定認知

每人每年至少應接受4小時以上的資訊安全教育訓練。

(五)確保資安措施符合政策及法令要求

本部每年至少進行2次內部稽核。所屬機關則每年至少進行1次內部稽核。

七、資訊安全組織

(一)本部成立「法務部資通安全會報」(以下簡稱資安會報)為本部及所屬機關最高資訊安全管理組織，本會報負責制定、定期評估本部資訊安全政策，並統籌資訊安全計畫、資源調度等事項之協調、研議。由次長擔任召集人、主任秘書擔任副召集人、資訊處處長兼任執行秘書、各司處主管為委員，資訊處負責相關幕僚與行政文書作業。

(二)本部成立「法務部資通安全處理小組」(以下簡稱資安處理小組)，負責督導各機關執行資通安全預防及危機通報、緊急應變處理等相關工作。由本部資訊處處長、副處長分別擔任小組召集人、副召集人，成員包括本部資訊處各科主管及相關負責人員，共有三個分組：安全預防分組、危機處理分組、稽核分組。所屬機關成立資訊安全執行小組。

八、資訊安全分工原則

(一)資訊安全政策、計畫、措施、技術規範之研議及安全技術之研究、建置、評估相關事項由資訊處負責辦理。

(二)資料及資訊系統之安全需求研議、使用管理及保護等事項，由各業務單位負責辦理。

(三)執行各項資訊作業時，應依「行政院及所屬各機關資訊安全管理要點」、「行政院所屬各機關資訊安全管理規範」、「電腦處理個人資料保護法」及相關法令規定辦理，並遵守本部各項規範。

(四)資訊安全教育訓練，由資訊處統籌規劃或協同其他單位共同辦理。

(五)本部稽核作業，由資訊處及政風司負責辦理。各機關內部稽核作業，由

各機關之資訊單位及政風單位負責辦理；外部稽核作業，由資訊單位會同政風單位及相關業務單位辦理。

(六)本部之資訊及網路系統因遭受破壞、不當使用所造成危安或重大災害事件，應依本部「營運持續管理計畫」辦理，資安處理小組應在最短期間內訂定應採行應變措施，並將處理情形記錄備查。

(七)本部人員違反資訊安全規定者，依「法務部及所屬各機關人員共同獎懲標準表」辦理。有「公務員懲戒法」第 2 條所定情事，應付懲戒者，依該法第 19 條規定辦理；有觸犯「刑法」之嫌疑者，應予移送司法機關調查；有涉及國家賠償事件者，應依「國家賠償法」等相關法律追究損害賠償責任。非本部人員違反資訊安全規定時，亦應依相關法律規定追究民刑事責任。

九、資產分類、等級及評鑑原則

(一)分類

依據各項作業內容特性，將資產分為資訊資產、實體資產、軟體資產、服務、書面文件及人員 6 大類。

(二)等級

依照各類資產所具有之機密性、完整性及可用性評估該資產反應出之價值。

(三)評鑑

根據資產本身之弱點、威脅及衝擊，評鑑其風險等級。經分級與評鑑後，依其所具備之價值，施以適當程度之安全控管。

十、不可接受風險等級

執行風險評鑑後，將資產區分為不同風險等級，其中位於「不可接受風險值以上」之資產，應訂定「風險改善計畫」據以監督控管，並落實執行追蹤控制。

十一、適用性聲明書

本部依據 ISO27001 標準要求產出適用性聲明書，以書面方式列舉資產是否適用其標準所列之控制措施，及其不適用之原因。當組織架構、人員、設備、實體環境等變動時，資安會報應重新定義控制措施之適用性。