

法務部及所屬機關資訊資產管理規範

安全分級： 公開 一般 限閱

文件編號：20801

版次：1.1

施行日期：中華民國 104 年 11 月 15 日

目 錄

一、 目的	3
二、 適用範圍	3
三、 資訊資產分類	3
四、 資訊資產管理責任	3
五、 資訊資產分級及標示	4
六、 資訊資產安全管制	4

一、目的

為有效管理法務部(以下簡稱本部)及所屬機關資訊資產之安全性,特訂定本規範。

二、適用範圍

本部及所屬機關資訊安全管理系統範圍內之資訊資產。

三、資訊資產分類

依據各項作業內容特性,將資訊資產分為下列6大類:

(一)資訊類資產(Information Assets):

1. 系統資料,例如:資料庫、應用程式及備份資料等。
2. 電子化儲存之文件檔案,例如:系統或軟體使用手冊及教育訓練教材等。

(二)實體類資產(Physical Assets):

1. 電腦設備,例如:伺服器、主機、螢幕、筆記型電腦、個人電腦及印表機等。
2. 通訊設備,例如:路由器、網路交換器、數據機、傳真機等。
3. 儲存媒體,例如:磁帶、磁帶機、磁帶櫃、光碟片及光碟機等。
4. 其他技術設備,例如:不斷電系統及機房用發電機等。

(三)軟體類資產(Software Assets):

套裝軟體,例如:系統軟體、應用軟體、公用軟體、網路軟體等。

(四)服務類資產(Services):

1. 區域網路及通訊服務。
2. 一般服務,例如:電力系統、空調系統等。

(五)書面文件類資產(Paper Documents):

1. 書面管理文件,例如:系統文件、使用手冊、各種程序及指引辦法等。
2. 書面紀錄,例如:申請表單及採購/維護合約等。

(六)人員類資產(People):

包含所有員工(依職等職務分)、承包商、顧問、維修人員等。

四、資訊資產管理責任

- (一)藉由定期進行之風險評鑑作業,鑑別需進行詳細風險評鑑作業之業務流程,建立相關資訊資產清冊。

- (二) 資訊資產均須指派人員負責管理事宜。
- (三) 人員異動或離職前，須確實移交所保管之相關資訊資產。
- (四) 資訊資產報廢時，應依資產類別循相關安全程序辦理銷毀。

五、資訊資產分級及標示

- (一) 為確保資訊資產得到最妥適之處理，應建立資訊資產清冊，並於清冊中標示各項資訊資產之機密性 (Confidentiality)、完整性 (Integrity) 及可用性 (Availability) 分級。
- (二) 重要實體類資訊資產應依可用性等級 (可接受中斷時間) 或緊急應變處理作業需求進行標示，以利緊急處理。

六、資訊資產安全管制

(一) 資訊類資產

- 1、限機關內部人員存取之資訊類資產，機關以外人員非經授權不得存取。
- 2、具機敏性資訊資產應設密碼保護，經過授權後方可存取。
- 3、應採用儲存媒體 (如磁帶、光碟片、硬碟) 進行備份，並應妥為保管，機敏性資訊之備份媒體應置於上鎖櫃內。
- 4、如須廢棄時，非屬公開資訊者應確保不被復原，磁片或硬碟等儲存媒體需格式化或消磁，必要時，須採用實體破壞。

(二) 實體類資產

- 1、應考量其設置環境，並應有適當之保護。
- 2、應評量其電力使用安全，纜線應有適當保護。
- 3、應定期進行保養及維護，必要時，應進行測試。
- 4、於報廢時應將資訊清除。

(三) 軟體類資產

- 1、軟體使用應符合版權要求。
- 2、不明來源之軟體或從網路下載之軟體應先進行掃毒或測試。

(四) 服務類資產

- 1、應有即時監控機制，確保正常運作。
- 2、應定期進行保養及測試。
- 3、應確保其服務水準。

(五) 書面文件類資產

- 1、限機關內部人員查閱運用之書面文件，機關以外人員非經授權不得查閱及運用。
- 2、具機敏性之書面文件，應保存於上鎖櫃內，經授權方得以查閱及運用。
- 3、如須廢棄時，非屬公開文件者應以碎紙機銷毀或燒毀，具機敏性文件並需由相關人員監督其過程。

(六) 人員類資產

- 1、人員應進行資訊安全基本認知及定期教育訓練。
- 2、應對接觸機敏性資訊及業務之人員或重要職務工作者之背景及工作能力進行篩選。
- 3、人員於調離職時應進行權限變更並辦理資訊資產移交。

(七) 各類資訊資產之安全管制措施，除遵循上述原則性規範外，另依各資訊資產類別相關之管理規範、程序辦理。