

# 司法院

## 資訊安全政策

機密等級：普通

文件編號：IS-1-1

版 本：2.0

發行日期：96.11.29



文件編號	IS-1-1	機密等級	普通	版本	2.0
------	--------	------	----	----	-----

## 目錄

一、 依據.....	1
二、 目的.....	1
三、 適用範圍.....	1
四、 政策.....	1
五、 目標.....	1
六、 責任.....	1
七、 審查.....	2
八、 實施.....	2

文件編號	IS-1-1	機密等級	普通	版本	2.0
------	--------	------	----	----	-----

## 司法院資訊安全政策

### 一、依據

- (一) 國家機密保護法。
- (二) 電腦處理個人資料保護法。
- (三) 司法院及所屬各機關資訊安全管理要點。

### 二、目的

司法院(以下簡稱本院)為強化資訊安全管理，提供可靠之資訊服務，確保資訊資產可用性、完整性與機密性，並符合相關法令之要求，訂定本政策。

### 三、適用範圍

本政策適用於本院對外網站，為符合本政策所採行之資訊安全措施，應考量下列事項：

- (一) 資訊安全政策訂定及評估
- (二) 組織資訊安全與分工
- (三) 資產管理
- (四) 人力資源安全
- (五) 實體與環境安全
- (六) 通訊與作業管理
- (七) 存取控制
- (八) 資訊系統取得、開發及維護
- (九) 資訊安全事故管理
- (十) 營運持續管理
- (十一) 遵循性

### 四、政策

維護對外網站之可用性、完整性與機密性。

### 五、目標

- (一) 各資訊服務，除因例行性維護或水、電、網路 ISP 等服務中斷者外，應保持 99.5% 以上之可用性；服務中斷，每次不得超過 1 工作日。
- (二) 發現資訊內容遭外力不當修改，應於接獲通知或發現之時起，1 工作日內修正完成。
- (三) 發生 A 級重大資訊安全事件之次數，每年不得超過 0 次。

### 六、責任

- (一) 管理階層應建立及審查本政策。
- (二) 資訊安全管理人員應透過適當的標準和程序以實施本政策。

文件編號	IS-1-1	機密等級	普通	版本	2.0
------	--------	------	----	----	-----

- (三) 系統管理人員、資料維護人員與提供資訊服務之廠商（於契約要求），應依規定程序及指定措施辦理資訊業務，以維護本政策。
- (四) 本院所有人員及提供資訊服務之廠商應透過適當通報機制，報告資訊安全事件及資訊安全弱點。
- (五) 任何危害資訊安全之行為人，視情節輕重追究其民事、刑事及行政責任。

#### 七、審查

本政策每年至少應評估一次，以反映相關法令、技術及業務等最新發展現況，確保維持營運和提供服務的能力。

#### 八、實施

本政策經核定後實施，並應通知員工、與本院連線作業之有關機關（構）及提供資訊服務之廠商，修正時亦同。