

金融監督管理委員會資訊安全政策

- 一、 金融監督管理委員會（以下簡稱本會）為確保本會及所屬機關資料、資訊系統、設備及網路之安全，特訂定本政策。
- 二、 資訊安全之定義在避免因人為疏失、蓄意或自然災害等風險，運用適當之控制措施，來確保本會及所屬機關之資訊資產受到妥善之保護。
- 三、 資訊安全之整體目標在確保資訊之機密性、完整性及可用性，防範組織之營運受到資安事件之衝擊。重要系統應依此目標自行訂定量測方式。
- 四、 資訊安全政策之適用範圍包括人員、應用系統、硬體設備、機房及網路設施、資訊紀錄等五部分：
 - （一） 人員：本會及所屬機關正式人員、約聘雇人員及使用本會及所屬機關資訊資源之委外廠商人員。
 - （二） 應用系統：本會及所屬機關業務資訊系統。
 - （三） 硬體設備：本會及所屬機關各式主機、工作站、伺服器及個人電腦。
 - （四） 機房及網路設施：本會及所屬機關網路服務、空調、電力等。
 - （五） 資訊紀錄：本會及所屬機關各共同性系統、系統資料庫、

作業資料庫、系統規劃與設計文件、使用與操作手冊、制度文件及各式記錄等。

五、本會為統籌資訊安全管理等事項之協調及推動，成立跨部門之資通安全管理會報，其幕僚作業，由資訊服務處負責。

六、本會有關單位得就下列事項，訂定相關管理規範或實施計畫，提報本會資通安全管理會報審核通過後，再送本會業務會報核定，並定期評估實施成效：

(一) 資訊安全管理組織推動及權責。

(二) 人員安全管理及教育訓練。

(三) 電腦系統安全管理。

(四) 網路安全管理。

(五) 系統存取控制。

(六) 系統開發及維護之安全管理。

(七) 資訊資產之安全管理。

(八) 實體環境及環境安全管理。

(九) 營運持續管理之安全之準則。

支援前項相關管理規範或實施計畫所需之細部作業程序及表單等，由各有關單位研擬，簽報單位主管核定後實施。

七、資訊安全管理之分工原則：

- (一) 資訊安全政策、計畫及技術規範之研議、建置及評估等事項，由本會資訊單位負責辦理。
- (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) 資訊機密維護及資訊安全之稽核事項，由本會政風單位會同各業務相關單位辦理。

八、本會及所屬機關同仁應遵守維護公務機密之相關法令規定；在職及離退職後，均不得洩漏所知悉之業務機密，或為不當之使用。

九、為維業務正常運作，對資訊安全事件應建立緊急處理機制，在發生資訊安全事件時，應依規定之處理程序，立即向資訊單位或人員通報，採取反應措施，並聯繫檢警調單位協助偵查。

十、本政策應以書面或其他方式告知本會及所屬機關同仁及與本會連線作業之其他公私機關（構）及提供資訊服務之廠商，以利共同遵守。若違反本會資訊安全相關規定，得依情節輕重予以處分或追究其民、刑事責任。

十一、本政策應每年至少評估 1 次，或於發生重大變動時重新評估，以符合相關法令、技術及組織、營運之最新發展現況。