

內政部消防署暨所屬機關存取控制程序規範

一、目的

為建立內政部消防署（以下簡稱本署）暨所屬機關存取控制管理制度，以防止未經授權使用資訊系統，特訂定本規範。

二、依據

- （一）行政院及所屬各機關資訊安全管理要點。
- （二）行政院及所屬各機關資訊安全管理規範。
- （三）行政院所屬機關電腦設備安全暨資訊機密維護準則。
- （四）本署暨所屬機關資通安全政策及管理要點。

三、存取控制方針

- （一）資料之存取應與業務相關範圍為主，任何人未經授權不得存取業務範圍外之資訊系統、設備或資料。
- （二）使用者不得將帳號借予他人使用或盜用他人帳號。
- （三）被賦予系統最高權限人員、掌理重要技術及作業控制之特定人員應審慎授權評估。
- （四）資料之存取應符合個人資料保護法、電子簽章法及智慧財產權相關法令、法規、或契約對資料保護及資料存取使用控管規定。
- （五）對可能竄越作業系統（OS）或應用系統（AP）安全控管措施之特權公用程式應限制或嚴密控管，並禁止一般使用者使用該等公用程式。
- （六）各式電腦應設定螢幕保護程式鎖定，避免被未經授權之存取使用。

四、帳號與密碼管理

- （一）新購置之應用軟體或系統，安裝完成後應立即更新預設密碼，並刪除或關閉不必要之帳號。
- （二）系統管理者應避免共用帳號。
- （三）資訊系統伺服器主機管理者帳號及個人電腦使用者帳號或一般系統使用者帳號密碼長度及複雜度應符合政府組態基準（GCB）並週期性變更密碼。

五、系統存取控制

- （一）系統應避免於帳號登入過程，以明碼顯示密碼資訊。
- （二）應視需求設定登入系統時間限制，如果在未經許可之作業時間，或連線超過 4 小時未操作系統，系統將自動中斷連線，以防止未經授權之存取系統。
- （三）系統登入、登出應留存電腦稽核紀錄。

六、遠端存取限制

- （一）非經授權禁止於辦公處所外，遠端存取系統。
- （二）遠端連線必須經過加密之安全通道，例如：SSL-VPN。

七、資料庫存取控制

- (一) 資料庫之存取之身份驗證機制需由系統內部安全機制提供，由作業系統及資料庫同步執行身份識別。
- (二) 資料庫之帳號登入管理機制應留存紀錄備查。

八、附則

- (一) 本署所屬機關得視本身業務之個別需求，依據本規範另訂相關規範，報署核備後實施。
- (二) 本規範自核定後實施，修正者亦同。