法務部主管法規查詢系統

列印時間：113.03.29 03:46

列印 關閉視窗

法規內容

法規名稱：	法務部及所屬機關資訊系統存取控制管理規範
公發布日：	民國 96 年 03 月 09 日
修正日期：	民國 111 年 05 月 11 日
法規體系：	法務部部內各單位 > 資訊處
立法理由：	立法總說明 條文對照表.ODT

一、目的

為有效管理法務部（以下簡稱本部）及所屬機關資訊系統之存取安全，防止非法授權存取之事件，以維護資料之保密性，特訂定本規範。

二、適用範圍

本部及所屬機關資訊系統帳號、密碼、權限管理及存取紀錄等管理事宜。

三、帳號新增及異動管理

（一）帳號新增及異動須經申請並經權責主管核可後交由系統管理人員或帳號管理人員處理，並保留紀錄。

（二）帳號、密碼之通知過程，應有保護措施，防止被窺視竊取。

（三）每一使用者在同一系統上應以使用一個帳號為原則，同一使用者因業務或特殊需要有使用二個以上帳號之必要時，應提出申請核可。

（四）離職人員及留職停薪人員應辦理帳號異動程序，並由帳號管理人員立即鎖定帳號或停止系統權限；未依規定辦理者，帳號管理人員得逕行停止該帳號之使用。

（五）系統存取權限之配賦，應以執行公務必要者為限。

（六）原則禁止共用帳號，以區分安全責任。

四、系統登入作業管理

（一）重要系統應限制連續登入失敗之上限為五次，登入失敗次數達上限者，應暫時停止該帳戶一定時間之登入，或鎖定該帳戶直到系統管理人員（或帳號管理人員）確認該帳戶擁有人身分後應其要求解除鎖定。

（二）重要系統之登入程序應避免於登入畫面提供帳號、密碼之提示訊息；登入失敗之因應訊息亦不揭露系統設計相關資訊。

（三）重要系統使用者除採一般識別碼外，應依業務需求考量是否須採用其他適切之身分鑑別技術。

（四）重要系統於登入作業完成後，應以可顯示前一次登入成功或失敗之時間或相關訊息為原則。

（五）含有敏感性資訊之系統，應考量業務需求，設定可開放連線之時間或連線逾時自動登出之機制，以防止未經授權存取。

五、密碼安全管理

（一）除系統程式使用之帳號及系統採用多重身分認證方式外，一般靜態密碼之強度及使用應符合下列規定：

1.禁止使用空白密碼。

2.密碼長度至少為八個字元，管理者密碼至少為十個字元。

3.密碼變更時，新密碼不得與前三次密碼相同。

4.密碼設定應包括數字及英文字母，建議包括特殊字元。

5.重要系統之密碼以至少每六個月更換一次為原則。

6.避免使用與個人有關資料（如生日、身分證字號、單位簡稱、電話號碼等）作為密碼。

（二）使用者密碼須妥善保管，避免他人知悉。

六、使用存取權限管理

（一）使用者權限之申請，應由權責主管依照使用者執行職務需求及角色，以工作所需最小權限之原則核可後，交由系統管理人員或帳號管理人員執行相關設定。

（二）未經核可之申請，系統管理人員或帳號管理人員不得進行　授權作業設定。

（三）經授權之使用者方始得使用作業系統提供之公用程式。

（四）系統管理人員進行遠端維護時，應限制經由本部核可之遠端連線來源。

七、存取事件紀錄

（一）重要系統應啟動系統紀錄功能，系統管理人員不得刪除系統稽核檔案。

（二）系統紀錄檔應定期備份，並由專人負責保管。

（三）各重要系統應視其重要性及系統支援程度，在不影響日常作業之情況下，將以下事件列入紀錄：

1.系統管理人員及具備特殊權限帳號者之登入成功及失敗事件。

2.使用者帳號異動及對密碼檔案之讀取與變更。

3.程式原始碼及程式執行碼之變更。

4.以非應用程式功能對系統使用之資料庫資料所作之資料變更。

5.系統設定檔之存取及變更。

（四）存取事件紀錄應使用系統內部時鐘，並與國家時間同步。

八、存取控管作業查核

（一）系統管理人員應定期辦理帳號權限清查，檢視權限與職務對應之適切性及是否留存閒置帳號等。

（二）系統管理人員應不定期監控有無違反系統存取之安全事件，以維護系統存取安全。

（三）系統管理人員應針對存取行為進行查核，檢視各項紀錄，並分析其異常狀況。

（四）系統管理人員所存取之紀錄檔須另指派專人查核。

資料來源：法務部主管法規查詢系統