中央研究院

資訊科學研究所

存取控制作業說明書

機密等級：□公開 ■內部 □敏感

編　　號：B330-I309

版　　本：1.0

核准日期：115 年 4 月 24 日

文件制／修訂紀錄表

版次	修訂日期	修訂單位	修訂者	核准者	修訂內容
1.0					新擬訂文件

目錄

壹、目的

中央研究院資訊科學研究所（以下簡稱本所）為保護本所資通系統之正常運作，降低未經授權存取之風險，以達成本單位安全控管之目的，訂定存取控制作業說明書（以下簡稱本說明書）。

貳、依據

一、 中央研究院資通安全暨個人資料保護政策及規範

二、 中央研究院資通安全管理規範實施要點

參、範圍

適用於本所資通資產之存取控管。

肆、權責

因業務需求存取本所資通資產之相關人員應遵守本說明書之相關規定，以確保本所資通資產之安全。

伍、作業說明

一、 存取控制權限管理

(一)帳號應辦理分權作業，如管理者、一般使用者、特權帳號…等，權限設計以工作所需最小權限為原則。

(二)各類資通資產之存取應與本身業務相關之範圍為主，任何人未經授權不得存取業務範圍外之資通資產。

(三)非因業務需求不得將系統存取帳號提供他人，若因業務需要開放帳號予他人時，應有適當安全控管措施，該控管措施應考量業務需求及各類資通資產之機密性，授與適當之存取權限及有效日期。

(四)被賦予系統管理最高權限之人員及掌理重要技術及作業控制之特定人員，應經審慎之授權評估與建立業務代理機制。

(五)處理系統異常狀況時為避免紀錄混淆，應授與適當存取權限，不得使用共用帳號。

(六)可攜式電腦儲存媒體，例如：筆記型電腦、隨身碟、光碟、磁帶、行動裝置等，於傳送或使用時應採取適當管控措施，防止未經授權

資料、系統、網路存取或病毒傳播。

(七)對資料、資訊之存取，必須符合「個人資料保護法」及「智慧財產權」等相關法令規定，並遵循合約中有關資料保護及資料存取使用管控之規定。

(八)應用系統之程式路徑存取權限應適當控管，禁止一般使用者存取。

二、 使用者帳號管理

(一)使用者帳號申請，依本所「帳號管理規則」線上申請，經由其主管核准後，由系統管理者進行使用者帳號建立作業。

(二)系統相關作業人員需經正式授權存取業務相關之資通資產，其識別資料與帳號必須為唯一，禁止借用他人之帳號或共用帳號。

(三)單一使用者於單一系統上僅能申請及持有單一個人帳號，因業務或特殊原因需使用兩個以上帳號，應提出申請。

(四)帳號持有人個人資料如有變更時，職務異動、留職停薪或離職時應依本所「帳號管理規則」線上辦理帳號異動、延長、停用或註銷。

(五)帳號持有人應遵守下列原則：

1. 尊重他人隱私與使用權。
2. 不得擅自使用他人帳號或修改他人檔案、資料或通行碼(以下簡稱密碼)，亦不得置放或散布侵擾其他使用者之程式。
3. 不得侵入未經授權使用之電腦系統/應用系統。
4. 不得傳送或散布具恐嚇性、暴力性或猥褻性之資料，或謾罵、侮辱他人等不當言論。
5. 不得散布病毒、蠕蟲、木馬、後門等有害程式。
6. 遵守智慧財產權有關規定，不得重製、反編譯或散布侵害他人著作權之檔案。
7. 不得寄送垃圾或廣告郵件。
8. 不得有其他重大違規行為。

帳號持有人如有違反前項使用原則情事，系統管理者視情節得為通知改善、縮減使用權限、停止使用或其他必要之處置。

三、 特殊權限管理

(一)避免共用系統管理者帳號，定期變更密碼並覆核權限之授與是否適當。

(二)特殊帳號之管理，應依作業系統、應用系統或設備之安裝手冊或管理手冊內容，於安裝完成後，將系統管理權限賦予特定使用者帳號後，變更該特殊帳號密碼並封存之。

四、 密碼管理

(一)使用者首次使用系統時，應立即更改密碼設定，並妥善保管帳號與維持密碼之機密性。

(二)使用者應避免將密碼記錄在書面上，張貼在個人電腦或終端機螢幕或其他容易洩漏秘密之場所；離開個人資訊設備逾 15 分鐘應鎖定螢幕或登出系統，重新使用應輸入密碼；下班時應關閉個人資訊設備。

(三)使用者發現密碼可能遭破解時，應立即自行更改密碼或通知系統管理者更改密碼。

(四)使用者應於每次登入系統時輸入密碼，避免使用記錄密碼功能，導致開機時自動登入系統。

(五)使用者及應用系統密碼應至少 180 天更換一次，並禁止於 24 小時內更換，重複使用相同的密碼。

(六)密碼應符合密碼設置原則且至少 8 碼，避免使用易猜測或公開資訊，例如：

1. 個人姓名、出生年月日、身分證字號。

2. 機關、單位名稱或其他相關事項。

3. 使用者 ID、其他系統 ID。

4. 電腦主機名稱、作業系統名稱、電話號碼或空白。

5. 密碼複雜度原則如 K@tVs0wD（英文字母、大小寫、數字及特殊字元）。

五、 使用者存取權限

(一)各項系統資源使用權限應有適當之申請、註冊及註銷作業管理程

序，依申請紀錄於帳號系統，以備查核。

(二)系統之授權管理，必須依執行業務系統別之需求，例如資料庫管理系統、網路資源系統、監控管理系統、密或機密性報表系統等賦予系統存取權限，且以執行業務及職務所必要的最小資源存取授權為限。

(三)各項設備與系統相關之使用權限（例如使用者帳號、密碼，作業權限）應有記錄並妥善保管該項文件。

(四)定期辦理系統帳號權限盤點作業，系統管理者填寫「B330-I309-02帳號清查紀錄單」(包含網站前台、後台、資料庫)，若發現帳號不當使用或持有人不再符合申請資格，應停止或註銷該帳號。

(五)針對無人看管的資通資產設備，設備應上鎖或設定通行碼等，以防未經授權之存取或濫用。

(六)可攜式(BYOD)資訊設備需使用安全之連線，並限制檔案存取權限。

六、 作業系統存取控制

(一)系統設定應避免於登入程序中以明碼方式顯示密碼相關資訊。

(二)重要系統宜設定系統登入程序之時間限制，如果超出時間限制，啟動螢幕保護程式或系統將自動中斷登入。

(三)使用者帳號避免顯示任何足以辨識使用者特別權限之訊息，例如：登入顯示其為管理者或監督者；限制登入失敗次數，以 5 次為原則，超過次數應暫時鎖定帳號 15 分鐘。

(四)系統管理者結束系統維護作業後，應結束應用系統及網路連線，清除螢幕上的資訊，登出系統，並鎖定主控台螢幕。

(五)重要系統紀錄應限定由系統管理者及具讀取權限者存取，保留其系統記錄檔 (system log)至少六個月，檔案設定為唯讀並留存查核。

七、 應用系統存取控制

(一)應用系統資訊之使用，僅限業務相關之授權使用者，並應適當控制。

(二)除帳號、密碼外，應依業務需求考量是否採用其他適切之身分鑑別技術（如自然人憑證...等）。

(三)應用系統之機密性資訊，應與一般資訊作適當區隔，並加強權限控管措施。

(四)應用程式原始碼，應集中存放，並指定專人管理程式之增修作業。

(五)開發中之原始程式碼，應與線上程式碼分開放置與控管。

(六)應用系統應啟動系統紀錄功能，系統管理者應保存系統紀錄檔並定期備份；記錄事項參照「B330-I311 應用系統發展及維護安全管理作業說明書」電子形式軌跡資料(Log)。

八、 網路存取控制

(一)網路系統應依其性質之不同，區隔不同網段，各網段應以特定安全設施（如防火牆及網路閘道）加以保護，以降低可能之安全風險。

(二)網路管理者應定期檢視防火牆及網路閘道之存取紀錄，並留存查核記錄。

(三)對具機密或敏感性之系統，或具特殊權限之帳號，應加強連線管理。

(四)應限制或指定連線來源 IP 位址或帳號。

九、 資料庫存取控制

(一)資料庫使用者帳號之新增或異動需經正式申請填寫「B330-I309-01 資通系統帳號使用申請表」，所有資料庫使用者必須使用獨立之帳號及密碼登入。

(二)資料庫使用者之帳號密碼之身分驗證機制必須是由資料庫系統之內部安全機制所提供，而非僅使用作業系統之安全機制。

(三)資料庫使用者之帳號密碼設定必須符合本說明書及相關系統之帳號密碼管理規範之要求。

(四)資料庫公用程式路徑之存取權限應適當控管，禁止一般使用者存取；存取紀錄應留存並查核。

(五)資料庫最高權限帳號之存取應僅限於授權之人員；資料庫預設帳號應變更密碼，或是關閉使用。

(六)應留存資料庫異動紀錄，以供錯誤復原。

十、 系統存取及應用之監督

(一)事件紀錄

1. 系統管理者應保留其系統記錄檔 (system log) 至少六個月，以為日後稽核調查及監督之用。

2. 系統稽核軌跡宜包括下列事項：

(1) 使用者識別碼。

(2) 登入及登出系統之日期及時間 。

(3) 儘可能記錄端末機的識別資料或其位址。

3. 各系統時間應自動或手動與本院資服處鐘訊源進行同步。

4. 若作業平台本身所提供之系統記錄檔的資料不足以作為稽核之用，須另行開發或購置進階之管理工具，以確實作好系統稽核作業。

(二) 系統使用之監督

1. 各類系統之監督程序如次：

(1) 各應用系統負責人應將其所轄檔案之重要性，告知相關電腦系統管理者，並討論各檔案存取權限。

(2) 各電腦系統管理者依前項之結果，定期監控系統檔案之存取記錄（log）檔。

2. 系統使用監督應考量事項如下：

(1) 系統存取失敗情形。

(2) 檢查系統登入的模式，確定使用者識別碼是否有不正常使用或是被重新使用的情形。

(3) 查核系統存取特別權限的帳號使用情形及配置情形。

(4) 追蹤特定的系統交易處理事項。

(5) 敏感性資源的使用情形。

十一、 外部人員存取資訊之安全管理

(一)外部人員進行遠端作業存取單位資通設施，應於實際存取作業前，線上填寫「機器對外開放服務申請或異動(防火牆)」申請表，俟單位主管核准後始能提供存取服務。

(二)相關作業規範請參考 B330-I310 網路安全管理作業說明書。

陸、參考文件

一、 B330-I311 應用系統發展及維護安全管理作業說明書

二、 B330-I310 網路安全管理作業說明書。

三、 中央研究院資訊科學研究所帳號管理規則。

柒、使用表單

一、 B330-I309-01 資通系統帳號使用申請表

二、 B330-I309-02 帳號清查紀錄單

三、 帳號系統