



文件編號	ISMS-P-013	文件名稱	帳號密碼及存取控制管理程序書		
機密等級	內部使用	版次	2.5	頁次	1 / 11

管理系統文件

文件類別	第二階文件	
文件編號	ISMS-P-013	
文件名稱	帳號密碼及存取控制管理程序書	
發行單位	文件管制小組	
發行日期	111年02月17日	
版次	2.5	
訂修廢單位	審查	核准
資通安全處理小組		

(原版簽名頁保存於資通安全處理小組)



文件編號	ISMS-P-013	文件名稱	帳號密碼及存取控制管理程序書		
機密等級	內部使用	版次	2.5	頁次	3 / 11

1. 目的

為促使本校資通系統帳號、密碼及存取權限之申請、異動之管理有一明確規範，確保任何存取行為皆經適當的授權與管理，防止不當之資訊存取及避免重要資料外洩，特制定本程序書。

2. 適用範圍

凡本校提供服務所需之內部作業相關資通設施與網路，包括作業平台、資料庫、應用系統、企業網路、遠距存取服務及各種網路設備（如：路由器、防火牆及交換器等）之帳號及密碼申請、權限管理，均適用本程序書。

3. 參考文件

3.1. ISMS-P-018 委外作業管理程序書。

3.2. ISMS-P-008 矯正及預防管理程序書。

4. 名詞定義

4.1. 各項資通系統服務申請：係指最新消息帳號申請、維修系統帳號申請、校務資通系統服務申請、電子公文系統服務申請...等，校內各項資通系統服務之申請。

4.2. 各式網路、主機帳號申請：係指本校所有教職員電子郵件帳號、學生社團 Web 網站、學系院 Web 網站、行政(學術)單位 Web 網站...等，各項網路帳號之申請。



文件編號	ISMS-P-013	文件名稱	帳號密碼及存取控制管理程序書		
機密等級	內部使用	版 次	2.5	頁次	4 / 11

5. 作業內容

5.1. 帳號密碼及存取控制管理流程圖

作業流程	權責單位	相關表單
<pre> graph TD A([提出帳號及權限申請]) --> B{審核} B -- No --> A B -- Yes --> C[設置帳號及權限] C --> D[帳號及權限使用] D --> E{存取控管查核} E -- No --> F[異常處理] E -- Yes --> G([紀錄保存]) F --> G </pre>	<p>各單位使用者</p> <p>使用單位主管 /圖書資訊處處長</p> <p>系統管理人員</p> <p>各單位使用者</p> <p>系統管理人員</p> <p>系統管理人員</p> <p>圖書資訊處</p>	<p>各式申請表單</p> <p>各式申請表單</p>



文件編號	ISMS-P-013	文件名稱	帳號密碼及存取控制管理程序書		
機密等級	內部使用	版次	2.5	頁次	5 / 11

5.2. 存取控制政策

- 5.2.1. 資訊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訊資產。
- 5.2.2. 應正確地使用資訊資產，以維護資訊資產之機密性、完整性與可用性。
- 5.2.3. 非因業務需求不得將系統存取帳號提供給外部人員，若因業務需要開放帳號予外部人員，應有適當安全控管措施，該安全控管措施應考量業務需求及資訊資產之機密性，授與適當之存取權限及有效日期。
- 5.2.4. 被賦予系統管理最高權限之人員、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。
- 5.2.5. 因處理系統當機與異常狀況需視狀況授與適當之存取權限，並避免共用帳號。
- 5.2.6. 可攜式電腦儲存媒體，例如：筆記型電腦、隨身碟、外接式硬碟、光碟、磁帶等，應採取適當之控管措施，以防止未經授權之資料、系統、網路存取或病毒傳播。
- 5.2.7. 資料之存取，必須符合「個人資料保護法」、「電子簽章法」及「智慧財產權」等相關法規、法令之規定，或契約對資料保護及資料存取使用控管之規定。
- 5.2.8. 系統主機公用程式路徑之存取權限應適當控管，應禁止一般使用者存取。
- 5.2.9. 針對無人看管的資訊資產設備，應有適當控管程序，以防未經授權之存取或濫用。
- 5.2.10. 個人桌上型電腦、可攜式電腦應設定於一定時間不使用或離開後，自動清除螢幕上的資訊並登出或鎖定系統，以避免被未經授權之存取，若因業務需要不在此限(如：攝影監視、環控系統等)。

5.3. 提出帳號及權限申請

使用者應依規定提出帳號及權限之申請。



文件編號	ISMS-P-013	文件名稱	帳號密碼及存取控制管理程序書		
機密等級	內部使用	版 次	2.5	頁次	6 / 11

申請項目	需使用之表單
電子郵件帳號申請	ISMS-P-013-01 E-mail 申請單
各系統使用帳號申請	ISMS-P-013-02 系統使用權限申請單
各系統管理帳號申請	ISMS-P-013-03 系統管理權限申請單

5.3.1. 各單位使用者若需資通系統之使用權限，應填寫「ISMS-P-013-02 系統使用權限申請單」，說明欲申請之資通系統帳號種類及相關細節，經申請單位主管核准後向圖書資訊處提出申請。

5.3.2. 圖書資訊處成員若需資通系統之管理權限，應填寫「ISMS-P-013-03 系統管理權限申請單」，向圖書資訊處提出申請。

5.4. 審核

5.4.1. 使用者帳號權限之審核

資通系統使用權限申請單需經申請單位權責主管核准後，並送往人事室確認，始可送交圖書資訊處辦理帳號、密碼及存取權限之註冊申請。

5.4.2. 管理者帳號權限之審核

管理者填妥系統管理權限申請表單需經圖書資訊處處長核准後，由該系統管理者辦理帳號、密碼及存取權限之註冊申請。

5.5. 設置帳號及權限

5.5.1. 完成帳號及存取權限申請與審核程序後，各系統管理者依使用者及管理者申請資料，進行帳號、密碼及存取權限之設定，存取權限之設定以員工工作所需之最小權限與最少資訊為原則。

5.5.2. 新購置之應用軟體或資通系統，安裝完成後應更新預設之通行



文件編號	ISMS-P-013	文件名稱	帳號密碼及存取控制管理程序書		
機密等級	內部使用	版 次	2.5	頁次	7 / 11

碼，並刪除或關閉不必要之帳號。

5.6. 帳號及權限之使用

5.6.1. 帳號及權限之異動

5.6.1.1. 使用者調職、離職、停職時帳號異動

使用者職務異動(調職、離職、停職)時，應重新檢核權限並提出權限異動申請，以符合最小權限要求。

5.6.1.2. 對於調、離職人員(含留職停薪人員)人事單位應通知相關單位人員離、調職之情形，相關單位於收到通知後，應依下列之規定辦理帳號異動(停用、註銷或變更)作業：

5.6.1.2.1. 圖書資訊處系統管理者應依據人事室有關使用者調職之郵件通知，於人事命令生效當日實施權限帳之移轉。

5.6.1.2.2. 使用者若離職停職，應立即通知圖書資訊處系統管理者註銷或停用其帳號及存取權限，電子郵件系統帳號保留，但予以停用。

5.6.1.3. 委外廠商駐點人員完成任務或離職時，應通知圖書資訊處，辦妥移交手續，繳回其所使用之資料、證件、設備與軟體，並填寫「ISMS-P-013-02 系統使用權限申請單」提出帳號刪除申請，由系統管理員註銷其提供服務所需各項作業權限。

5.6.2. 密碼使用管理原則

5.6.2.1. 使用者於第一次登錄系統時，應立即更改預設密碼，並妥善保管帳號與維持密碼之機密性。

5.6.2.2. 密碼長度設定

使用者及管理者密碼長度設定至少 8 碼，且應符合密碼設置原則。

5.6.2.3. 密碼內容設置原則

5.6.2.3.1. 密碼內容之設定，應參雜數字、英文字母大小寫及特殊符號，至少符合下列要求中之 2 項。

A. 內含至少 1 個大寫英文字母。



文件編號	ISMS-P-013	文件名稱	帳號密碼及存取控制管理程序書		
機密等級	內部使用	版次	2.5	頁次	8 / 11

B. 內含至少 1 個小寫英文字母。

C. 內含至少 1 個阿拉伯數字。

D. 內含至少 1 個特殊符號。

5.6.2.3.2. 密碼內容之設定，應儘量避免使用易猜測或公開資訊，如下說明：

A. 個人姓名、出生年月日、身分證字號。

B. 機關、單位名稱或是其他相關事項。

C. 使用者 ID、其他系統 ID。

D. 電腦主機名稱、作業系統名稱。

E. 電話號碼、空白、字典字彙（具有意義的英文單字，例如：flower、eagle、birthday 等）。

5.6.2.4. 系統管理者及使用者應至少六個月更換密碼一次，密碼變更時應避免使用與前一次相同的密碼。

5.6.2.5. 一般使用帳號為確保使用安全性，建議每隔六個月變更密碼一次(若屬功能限制或系統老舊無法提供此功能，待版本升級或更新系統時改善)。

5.6.2.6. 所有使用者須負帳號及密碼保管之責，不得對任何人透露或以任何形式公開自己帳號及密碼，以避免密碼外洩。

5.6.2.7. 使用者懷疑其密碼被他人知悉或發現密碼可能遭破解時，應立即更改密碼。

5.6.2.8. 使用者應避免將帳號、密碼記錄在書面上，或張貼在個人電腦、螢幕或其他未保護且容易洩漏秘密之處所。

5.6.2.9. 系統管理者應避免共用系統管理者帳號，系統管理者帳號與密碼應存放於安全之處。保存帳號、密碼之檔案應以加密或加密碼之方式保護。

5.6.2.10. 系統使用者禁止共用自己或他人的帳號及密碼。



文件編號	ISMS-P-013	文件名稱	帳號密碼及存取控制管理程序書		
機密等級	內部使用	版 次	2.5	頁次	9 / 11

5.6.2.11. 使用者忘記密碼時，應經系統管理者確認身分後，重新設定新密碼。

5.6.2.12. 使用者每次存取系統時應輸入密碼登入系統，避免使用記錄密碼功能，導致開機時自動登入系統。

5.6.2.13. 使用者帳號之存取應保留稽核紀錄 (Log)，系統管理者不得擅自修改或刪除稽核紀錄 (Log) 內容。針對異常登入情況，系統管理者應隨時監控並採取適當防護措施。

5.6.3. 使用者存取管理

5.6.3.1. 特殊權限之使用者必須與一般權限之使用者區分管理，針對特殊權限帳號，應妥善管理。

5.6.3.2. 特殊權限之授權管理，必須依執行業務系統別之需求（例如作業系統、資料庫管理系統、網路服務系統、監控管理系統等）賦予系統存取特殊權限的授權，且以執行業務及職務所必要的最低資源存取授權為限。

5.6.3.3. 系統相關作業人員需經正式授權存取業務相關之資訊資產，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。

5.6.3.4. 重要系統稽核紀錄 (Log) 應定期審核，系統管理者不得新增、刪除或修改稽核紀錄 (Log)，審查週期不得超過 6 個月。

5.6.3.5. 各系統主機之管理者帳號，由系統管理者持有，委外廠商如需使用管理者帳號，應向各系統管理者提出申請並經核准後始得使用。

5.6.3.6. 系統管理者於委外廠商完成各項維護管理作業後，得停用該管理帳號或變更密碼。

5.6.3.7. 外單位資訊存取應依據「ISMS-P-018 委外作業管理程序書」之規定辦理。

5.6.4. 作業系統存取控制

5.6.4.1. 系統設定應避免於登入程序中以明碼方式顯示通行碼相關



文件編號	ISMS-P-013	文件名稱	帳號密碼及存取控制管理程序書		
機密等級	內部使用	版 次	2.5	頁次	10 / 11

資訊。

- 5.6.4.2. 只有在完成所有的登入資料輸入後，系統才開始查驗登入資訊的正確性；若登入發生錯誤，系統不應顯示錯誤發生之原因。
- 5.6.4.3. 系統登入被拒絕後，應立即中斷登入程序，並不得給予任何的協助。
- 5.6.4.4. 應設有系統登入程序時間及次數之限制，如超出時間及次數限制時，系統將自動中斷登入。
- 5.6.4.5. 使用者帳號避免顯示任何足以辨識使用者特別權限的訊息，例如：顯示其為管理者或監督者。
- 5.6.4.6. 系統管理人員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。
- 5.6.4.7. 系統之存取使用應留存查核紀錄。

5.6.5. 應用系統之存取控制

5.6.5.1. 資訊存取之限制

- 5.6.5.1.1. 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。例如：新增、刪除或執行等。
- 5.6.5.1.2. 應用系統之敏感與機密性資訊，應與一般資訊作適當區隔，並加強權限控管措施。

5.6.5.2. 原始程式資源之存取控制

- 5.6.5.2.1. 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。應用程式之異動須經適當管控。
- 5.6.5.2.2. 開發中之原始程式碼，應與線上程式碼分開放置與管控。
- 5.6.5.2.3. 舊版的原始程式應妥慎保管，並詳細記錄使用的明確時間，以備新版程式失敗時回復使用。
- 5.6.5.2.4. 應用程式管理人員，應檢視程式目錄清單，如有異常情



文件編號	ISMS-P-013	文件名稱	帳號密碼及存取控制管理程序書		
機密等級	內部使用	版 次	2.5	頁次	11 / 11

形，應即查明原因及處理。

5.7. 存取控管查核

- 5.7.1. 各系統管理者每年應審查所有系統使用者及管理者帳號一次，以確保所有帳號及存取權限之合法使用，以確保所有帳號之合法使用。
- 5.7.2. 各系統管理者每年應將各項伺服器主機、網路通訊設備、資通安全設備、門禁系統及監控系統等帳號權限設定資料印出或填寫於「ISMS-P-013-04 系統帳號審查紀錄單」，進行帳號權限清查，並將查核結果呈權責主管審閱。
- 5.7.3. 各系統管理者每年應將各項伺服器主機、網路通訊設備或其他有安裝憑證的設備之憑證核發內容及有效期印出或填寫於「ISMS-P-013-04 系統帳號審查紀錄單」，進行憑證狀態清查。

5.8. 異常處理

經查核結果若發生異常，由系統負責人依據「ISMS-P-008 矯正及預防管理程序書」之相關規定執行矯正與預防措施，進行問題矯正及風險預防的作業。

5.9. 紀錄保存

相關業務承辦人員應參照如下規範，妥善保存各項紀錄。

編號	表單名稱	保存地點	保存期限
1	E-MAIL 申請單	圖書資訊處	至少 1 年
2	系統使用權限申請單	圖書資訊處	至少 1 年
3	系統管理權限申請單	圖書資訊處	至少 1 年
4	系統帳號審查紀錄單	圖書資訊處	至少 1 年

6. 附件

- 6.1. ISMS-P-013-01 E-MAIL 申請單。
- 6.2. ISMS-P-013-02 系統使用權限申請單。
- 6.3. ISMS-P-013-03 系統管理權限申請單。
- 6.4. ISMS-P-013-04 系統帳號審查紀錄單。



開 南 大 學

K A I N A N U n i v e r s i t y

E - m a i l 帳 號 申 請 單

單位名稱		申請日期	年 月 日
申請人姓名		校內分機	
行動電話			
身 份 別	<input type="checkbox"/> 專任教師 <input type="checkbox"/> 兼任教師 <input type="checkbox"/> 職員 <input type="checkbox"/> 社團 <input type="checkbox"/> 其它_____		
申請帳號	1.	2.	3.
信箱位址	@mail.knu.edu.tw		
密碼	請勿填寫(密碼以電話告知)		
圖書資訊處 承辦人員		承辦日期	
說 明	<p>1.電子郵件主機設定如下: POP3 伺服器: mail.knu.edu.tw SMTP 伺服器: mail.knu.edu.tw</p> <p>2.如個人密碼忘記,請攜帶附相片之證件親洽圖書資訊處辦理變更或洽校內分機:1925。</p>		
注意事項	<p>1.申請帳號請填寫小寫之英文或數字,英文與數字可混合(例: john、john123 皆可,但不可全部為數字)。</p> <p>2.申請之帳號,最少為4個字元,至多12個字元。</p> <p>3.申請之帳號以第一組為優先考量,若所申請之帳號與他人重複,將由第二、三組帳號依序設定。</p> <p>4.若未填寫完整申請帳號欄位,則圖書資訊處以隨機方式設定帳號,申請人不得事後申請更改。</p> <p>5.如有任何疑問,請洽圖書資訊處分機:1925。</p>		



開南大學

K A I N A N U n i v e r s i t y

系統使用權限申請單

日期： 年 月 日

申請人姓名		服務單位	
電話		E-mail	

申請權限 註銷權限

本人願遵守以下規定：

1. 除本單位之系統外，若需系統使用權限，務必詳述原因，並以有使用到才申請為原則。
2. 若因電腦處理資料業務而知悉或持有他人個人資料者，不得無故洩漏。並應遵守電腦處理個人資料保護法相關規定。

遵守本校資訊安全管理制度等相關資安規定。

申請原因			
操作管理方式	<input type="checkbox"/> 實機操作 <input type="checkbox"/> SSH <input type="checkbox"/> 網頁操作 <input type="checkbox"/> Telnet <input type="checkbox"/> FTP <input type="checkbox"/> 遠端桌面 <small>(預設勾選)</small>		
申請資訊服務	<input type="checkbox"/> 人事系統 <input type="checkbox"/> 電子公文系統 經 <u>秘書室核章</u> 核准 <input type="checkbox"/> 通過 <input type="checkbox"/> 教務系統 <input type="checkbox"/> 會計系統 <input type="checkbox"/> 未通過 <input type="checkbox"/> 學務系統 <input type="checkbox"/> 教務系統群組發信(單位帳號用) <input type="checkbox"/> 電子郵件系統 <input type="checkbox"/> 其它 _____ <input type="checkbox"/> 校園虛擬私有網路 _____		
申請帳號	<input type="checkbox"/> 同 E-mail 帳號(如已有校內信箱者勾選) <input type="checkbox"/> 新帳號 (1) (2) (3)		
申請人員		申請單位	
	(申請人簽名)	主 管	
人事室	(教職員須經人事室核章後受理)		
核准帳號		核准密碼	請勿填寫(密碼以電話告知)
	(此欄位由本單位填寫)		
圖書資訊處 承辦人		圖書資訊處 單位主管	



開 南 大 學

K A I N A N U n i v e r s i t y

系 統 管 理 權 限 申 請 單

日期： 年 月 日

申請人姓名		服務單位	
電 話		E-mail	

 申請權限 註銷權限**本人願遵守以下規定：**

1. 除本單位之系統外，若需系統管理權限，務必詳述原因。
2. 若因電腦處理資料業務而知悉或持有他人個人資料者，不得無故洩漏。並應遵守電腦處理個人資料保護法相關規定。
3. 遵守本校資訊安全管理制等相關資安規定。

申請原因	
操作及管理方式	
維護之資通系統 (主機)	
申請帳號	

核准帳號		核准密碼	請勿填寫(於系統線上輸入密碼)	
承辦人員	單位主管		圖書資訊處 處長	



開南大學
K A I N A N U n i v e r s i t y

系統帳號審查紀錄單

系統(主機)名稱			
帳號類別		<input type="checkbox"/> 作業系統(OS) <input type="checkbox"/> 應用系統(AP) <input type="checkbox"/> 資料庫(Data Base) <input type="checkbox"/> 資安防護系統 <input type="checkbox"/> 其他_____	
清查人員		清查日期	
帳號名稱	權限/角色	使用單位/使用人員	備註
部門主管		圖書資訊處 處長	