管理系統文件

文 件 類 別	第 二 階 文 件
文 件 編 號	IMS-P-013
文 件 名 稱	帳號密碼及存取控制管理程序書
發 行 單 位	國立虎尾科技大學
發 行 日 期	112 年 05 月 05 日
版　　次	2.2
適用單位/範圍	全校

訂修廢單位	審　　查	核　　准

（原版簽名頁保存於 IMS 推動小組）

訂　　修　　廢　　記　　錄		
版次	發行日期	訂 修 廢 內 容 摘 要
1.0	106/01/11	初版發行
1.1	107/05/23	修改條文 5.6.1.1
2.0	108/08/21	1.因應資通安全管理法施行及配合法規用詞，將「資訊」一詞修改為「資通」。 2.修訂 5.6.2 密碼使用管理原則。
2.1	110/03/29	(1) 刪除 3.參考文件「附錄 A 資通安全管理規範」，並增訂「國際標準資訊安全管理系統(ISO27001：2013)」。 (2) 修訂 5.6.2.1 為:”帳號密碼設置原則與使用規範參照本校「IMS-W-001 一般資通設備安全管理作業標準書」文件辦理，因 5.6.2.2~5.6.2.9 與 IMS-W-001 一般資通設備安全管理作業標準書內容相同，因此予以刪除。
2.2	112/05/05	條文 5.2.5、5.6.1.5 修正

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。

2. 適用範圍

   本校提供服務所需之內部作業相關資訊設施與網路，包括作業平台、資料庫、資通系統、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）之帳號密碼申請及權限之管理。

3. 參考文件

   3.1　國際標準資訊安全管理系統(ISO27001：2013)。

   3.2　教育體系資通安全暨個人資料管理規範。

   3.3　IMS-P-018 資訊業務委外作業管理程序書。

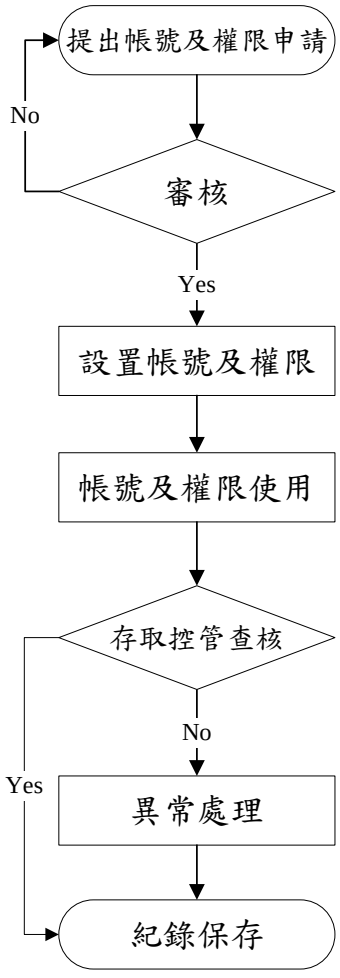
   3.4　IMS-P-008 矯正預防及持續改善管理程序書。

4. 名詞定義

   無。

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
	各單位使用者 權責主管 系統管理者 各單位使用者 系統管理者 系統管理者 權責主管 系統管理者 IMS 推動小組	資通系統使用權限申請單 資通系統管理權限申請單 學生信箱帳號密碼異動申請單 教職員工校園雲桌面帳號申請單 資通系統使用權限申請單 資通系統管理權限申請單 學生信箱帳號密碼異動申請單 教職員工校園雲桌面帳號申請單 資通系統使用權限申請單 系統帳號審查紀錄單

5.2　存取控制政策

5.2.1　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。

5.2.2　應正確地使用資通資產，以維護資通資產之機密性、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通資產之機密性，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，並應避免共用帳號。除系統功能限制(如：無法新增帳號)情況例外。

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　針對無人看管的資通資產設備，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。

5.3.1 各單位使用者若需資通系統之使用權限，應填寫「IMS-P-013-01 資通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承辦人員提出申請。

5.3.2 本校人員若需資通系統之管理權限，應填寫「IMS-P-013-02 資通系統管理權限申請單」，向單位權責主管提出申請。

5.3.3 本校教職員工若需要本校所提供之雲桌面服務，應填寫「IMS-P-013-01 資通系統使用權限申請單」，向單位權責主管提出申請。

5.3.4 本校各單位若需要申請校園雲端主機進行各項業務時，應填寫「IMS-P-013-05 校園雲端虛擬主機租用申請單」，向單位權責主管提出申請。

5.4 審核

5.4.1 使用者帳號權限之審核
使用者填妥帳號及權限申請表單，由業務直屬單位主管依業務需求審查其使用帳號及權限之適當性，經系統管理者單位主管核准後，始可由該系統管理者辦理使用帳號、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
管理者填妥帳號及權限申請表單，由業務直屬單位主管依業務需求審查其管理帳號及權限之適當性，經系統管理者單位主管核准後，始可由該系統管理者辦理管理帳號、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，存取權限之設定以人員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密碼，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 使用者離職時帳號異動

本校職員於完成離職作業流程時，由人事室於資通系統內設定離職狀態；本校學生於完成畢業、休學或轉學作業流程時，由教務處於資通系統內設定離校狀態；系統每日自動介接更新資料並刪除使用者帳號。職員完成離職作業流程時，須於一個月內刪除電子郵件帳號。本校人員退休續用校內信箱，須填寫「IMS-P-013-01 資通系統使用權限申請單」申請保留信箱。

5.6.1.2 使用者調職時帳號異動

使用者於調職時，須填寫「IMS-P-013-01 資通系統使用權限申請單」提出帳號刪除或變更申請，系統管理人員應於人員調職後二週內註銷使用者所有資通系統之使用帳號及存取權限。

5.6.1.3 管理者離（調）職時帳號異動

管理者於離（調）職時，須填寫「IMS-P-013-02 資通系統管理權限申請單」提出帳號刪除或變更申請，系統管理人員應於人員離（調）職後二週內註銷管理者所有資通系統之管理帳號及存取權限。

5.6.1.4 委外廠商駐點人員完成任務或離職時，應通知權責單位，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「IMS-P-013-01 資通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。

5.6.1.5 系統管理人員於帳號清查時進行之帳號異動

各資通系統管理人員依本程序書 5.7.1 每年進行帳號清查之「IMS-P-013-03 系統帳號審查紀錄單」審查結果，直接進行資通系統權限異動。

5.6.2 密碼使用管理原則

5.6.2.1 帳號密碼設置原則與使用規範參照本校「IMS-W-001 一般資通設備安全管理作業標準書」文件辦理。

5.6.2.2 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。

5.6.2.3 登入密碼錯誤次數限制：重要系統必須設定連續密碼登入錯誤次數限制，達五次錯誤後，應暫停該帳戶登入 30 分鐘或鎖定帳戶不能使用系統。如系統功能無法暫停或鎖定帳戶登入，應針對連續登入之錯誤事件加以記錄，並於內部查核時，查核是否有連續登入失敗的事件。

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。

5.6.3.4 應妥善管理久未登錄系統之帳戶，若超過 6 個月未曾登錄，則視需要清除或停用閒置帳號。

5.6.3.5 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 3 個月。

5.6.3.6 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。

5.6.3.7 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。

5.6.3.8 外單位資訊存取應依據「IMS-P-018 資訊業務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密碼相關資訊。

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 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。

5.6.4.4 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。

5.6.4.5 系統管理人員結束系統維護作業後，應結束資通系統及網路連線，清除螢幕上的資訊，登出系統，並鎖定主控台螢幕。

5.6.4.6 系統之存取使用應留存查核紀錄。

5.6.5 資通系統之存取控制

5.6.5.1 資訊存取之限制

5.6.5.1.1 資通系統資訊之使用，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 資通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

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，並將查核結果記錄於「IMS-P-013-03 系統帳號審查紀錄單」中備查。

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「IMS-P-013-03 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。

5.8　異常處理

經查核結果若發生異常，由系統負責人依據「IMS-P-008 矯正預防及持續改善管理程序」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	資通系統使用權限申請單	電子計算機中心	至少 3 年
2	資通系統管理權限申請單	電子計算機中心	至少 3 年
3	系統帳號審查紀錄單	電子計算機中心	至少 3 年
4	學生信箱帳號密碼異動申請單	電子計算機中心	至少 3 年
5	校園雲端虛擬主機租用申請單	電子計算機中心	至少 3 年

6. 附件

6.1　IMS-P-013-01 資通系統使用權限申請單。

6.2　IMS-P-013-02 資通系統管理權限申請單。

6.3　IMS-P-013-03 系統帳號審查紀錄單。

6.4　IMS-P-013-04 學生信箱帳號密碼異動申請單。

6.5　IMS-P-013-05 校園雲端虛擬主機租用申請單。