德明財經科技大學

資訊安全存取管理規定

機密等級：一般

文件編號：Takming-ISMS-B-009

版　次：V 1.1

初版日期：107.12.25

修 訂 紀 錄

版次	修訂日期	修訂頁次	修訂者	修訂內容摘要
1.0	107.12.25	N/A	執行小組	初版
1.1	114.02.08	6	推動小組	變更「電算中心軟硬體需求服務申請表」為「網路連線服務申請表」

1. 目的

確保德明財經科技大學(以下簡稱本校)對資通系統的存取權限均經適當的授權及維護，以防止不當存取。

2. 適用範圍

本規定適用本校提供資訊服務存取所需之作業相關資通系統與網路，包括作業平台、資料庫、應用系統、校園網路、遠距存取服務及各種網路設備等。周遭環境及設備之安全管控，所有人員進出入機房皆需遵守本規定。

3. 名詞定義

3.1. 秘密鑑別資訊

3.1.1.係指用於確認使用者身分的機制，密碼/通行碼(password)為常見資訊，其他包含加密金鑰資訊(Cryptographic keys)，或存放在智慧卡(Smart card)等硬體符記(Hardware tokens)上的鑑別資訊等。

3.2. 靜態密碼

3.2.1.系統登入時所使用，以文字、數字或特殊字元組成由系統自動產生或人工設定之密碼。

3.3. 一次性密碼

3.3.1.密碼僅供一次登入或認證使用，由系統自動產生或人工設定下一次登入之密碼，密碼不能重複。

4. 權責

4.1. 主機/資料庫/應用系統管理者

4.1.1.負責主機群組、帳號管理作業。

4.1.2.定期審查主機使用者存取權限。

4.1.3.執行主機密碼管理作業。

4.2. 網路管理者

4.2.1.負責網路設備帳號及密碼管理作業。

4.2.2.定期審查網路設備使用者存取權限。

4.3. 資料擁有者(單位)

4.3.1.審查使用者存取權限。

4.3.2.公務資料之蒐集或利用，應尊重當事人之權益，依誠實及信用方法為之，不得逾越公務目的之必要範圍。

5. 要求事項

5.1. 存取控制政策

5.1.1.存取控制政策宜考量下列事項：

5.1.1.1.個別營運應用的安全要求。

5.1.1.2.所有與營運應用相關的資訊與該資訊所面臨的風險。

5.1.1.3.資訊傳播和授權政策，例如需知(need to know)原則，以及資訊的安全等級。

5.1.1.4.不同系統與網路間存取控制與資訊分類政策的一致性。

5.1.1.5.有關保護資料或服務存取的適當法規及所有的契約責任與義

務。

5.1.1.6.分散式和網路環境中存取權限的管理，其辨識所有可用的連接型式。

5.1.1.7.存取控制角色的區隔，例如：存取請求(request)、存取授權及存取管理。

5.1.1.8.存取權限正式授權的要求。

5.1.1.9.存取控制措施定期審查的要求。

5.1.2.存取控制可以角色為基準(Role-based Access Control)

5.1.2.1.各作業系統、應用系統、資料庫及網路設備之管理者應對其所管理之標的制定存取角色。

5.1.2.2.對於權限之申請以加入各種角色為原則，避免對個別使用者或帳號進行授權。

5.1.2.3.系統若無法以角色給予權限，則另列清單執行帳號、權限控管。

5.1.3.存取權限應以工作所需最小權限為主

5.1.3.1.各作業系統（含公用程式）、應用系統、資料庫系統及網路設備之使用需經過授權，且應有身份鑑別機制；資訊存取權限之設定以工作所需之最小權限與最少資訊為原則。

5.2. 使用者註冊與註銷

5.2.1.作業系統、應用系統、網路及資料庫使用者如需申請及註銷存取權限依據「資訊應用系統安全管理規定」、「網路安全管理規定」辦理，填寫相關申請單。

5.2.2.職務異動(例如：調、離職、留職停薪人員等)，依照本校相關法規辦理，於收到通知後，據以註銷或停用存取權限。

5.2.3.使用者申請及註銷應保留核准紀錄。

5.2.4.使用者需經由外部連線至本校使用非公開(屬內部使用)之資訊服務時，須於申請時特別說明，並經由評估後，授予權限。

5.2.5.本校帳號申請另外可依據「校園網路帳號申請表」申請。

5.3. 使用者存取權限之配置

5.3.1.系統存取權限之配賦，應以執行業務及職務所必需者為限，當使用者調整職務及離(休)職時，應儘速註銷其系統存取權限。

5.3.2.應依據業務之需求訂定系統可以存取之帳號、群組、及其存取權限。

5.3.3.重要應用系統應考量記錄使用者登入、登出與操作敏感性之相關資訊，並依業務需求賦予使用者最適當權限。

5.3.4.視需要建立工作群組，統一對工作群組賦予權限。

5.4. 具特殊存取權限之管理

5.4.1.由權責主管依據員工的工作職責或作業性質指派權限。

5.4.2.作業、應用系統或帳號管理者，依據申請資訊，設定使用者存取

權限。

5.4.3.使用者職務異動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。

5.4.4.具備系統或帳號管理者權限之使用者，權責主管應審查其合適性。

5.4.5.當委外廠商有使用應用系統管理員帳號(或高作業權限帳號)之需求時，應由各系統負責人代為填寫「電算中心軟硬體需求服務申請表」，並開設臨時性帳號，系統負責人於委外廠商當次作業完成後應立即停用或移除。

5.4.6.本校校務行政系統的作業及維護須填寫「電算中心軟硬體需求服務申請表」辦理。

5.4.7.應用系統管理員帳號或高權限帳號密碼至少每六個月變更一次。

5.4.8.資料庫作業申請，應由申請人填寫「電算中心軟硬體需求服務申請表」，並於奉核後進行資料庫作業。

5.4.9.權責主管應審核申請者提出之申請與資料庫管理者之處理說明，確保資料庫存取之適切性。

5.5. 使用者之秘密鑑別資訊的管理

5.5.1.應針對使用者的秘密鑑別資訊制定配置的原則

5.5.2.秘密鑑別資訊須妥善保管，避免他人知悉。

5.5.3.使用者初次登入電腦系統，應有立即變更秘密鑑別資訊之措施。

5.5.4.建立秘密鑑別資訊變更前確認使用者身分的相關程序

5.5.5.暫時性秘密鑑別資訊宜以安全方式傳遞，避免使用外部或未保全的郵件傳遞

5.5.6.各系統應有設定連續秘密鑑別資訊登入錯誤次數限制，要有錯誤紀錄，必要時得停止該帳號之登入或鎖定該帳號。

5.5.7.秘密鑑別資訊如採密碼設定可採用靜態密碼、一次性密碼。

5.5.8.一般之靜態密碼的安全性及使用須符合至少 8 碼且英數字混合之規定。

5.5.9.每隔六個月得變更密碼。

5.5.10.上述規範若屬功能限制或老舊系統無法提供此功能，待版本升級或更新系統時改善。

5.6. 使用者存取權限的定期審查

5.6.1.應每六個月執行使用者存取權限查核，查閱人員異動資料(到職、調職或離職)，抽檢到職、調職及離職人員之權限申請、註銷或關閉作業紀錄並核對系統中之設定。

5.6.2.應定期將資訊機房主機、關鍵業務系統、網路安全設備之管理者帳號權限設定資料印出，或填寫於「帳號清查紀錄表」，進行帳號權限清查，並將查核結果紀錄於「帳號清查結果報告」呈各權責主管審查。

5.7. 存取權限之移除或調整

5.7.1.員工執行內部轉調，應由人事單位通知生效日起，將轉調人員前使用之帳號或權限移除，新職務之帳號及權限，依相關申請程序辦理。員工離職時，依據德明財經科技大學人事相關法規辦理各項離職相關事宜。員工離職應將其配附之相關資訊資源、帳號及權限刪除。

5.8. 秘密鑑別資訊之使用責任

5.8.1.使用者應於權限申請核准後首次登錄系統時，依密碼設定原則立即修改預設密碼。

5.8.2.秘密鑑別資訊之使用須妥善保管，避免他人知悉。

5.8.3.秘密鑑別資訊之使用不能以容易破解的明碼格式寫在紙上，並放在未經授權之人士可能看到的地方。

5.8.4.當使用者懷疑其秘密鑑別資訊之使用被他人知悉時，必須立即提出變更申請。

5.8.5.所有使用者不得對任何人透露或提供自己的秘密鑑別資訊。

5.8.6.公務與非公務使用目的勿使用相同秘密鑑別資訊。

5.9. 資訊存取限制

5.9.1.重要應用系統應考量記錄使用者登入、登出與操作敏感性之相關資訊，並依業務需求賦予使用者最適當權限。

5.9.2.各應用系統管理員帳號(或高作業權限帳號)，若由系統承辦人持有，委外廠商有使用該應用系統管理員帳號(或高作業權限帳號)的需求，得向該系統承辦人索取帳號密碼，並由系統承辦人協同使用該組密碼，且承辦人於委外廠商當次作業完竣後應即變更密碼。

5.9.3.若因應作業需求，須由委外廠商持有應用系統管理員帳號，應用系統承辦人應考量操作系統之安全需求，對委外廠商執行之作業採取適當審核與確認。

5.9.4.資料庫存取限制

5.9.4.1.使用資料庫必須經由資料庫管理系統進行身份認證與權限控制。

5.9.4.2.應用程式存取資料庫之帳號不應有異動與資料庫相關檔案的作業系統權限，並禁止應用程式使用資料庫管理者之帳號連線資料庫。

5.9.4.3.一般使用者禁止直接連接資料庫，只能透過應用程式存取資料庫之資料。

5.9.4.4.應用軟體開發者如需直接連接資料庫，須先提出申請。

5.9.4.5.存有敏感性資料（教職員生身分證相關資料、成績或個人隱私資料）之資料庫，應以獨立運作為原則。

5.9.4.6.除有特殊需求，禁止將帳號與密碼寫於不需組譯之應用程式

或 Script 檔中。

5.10. 系統保全登入程序

5.10.1.對於限制存取的應用系統，應採取身分認證(如帳號、秘密鑑別資訊)或其他身分鑑別的機制。

5.10.2.程式設計應具備檢驗登入身分識別與秘密鑑別資訊功能，秘密鑑別資訊如採密碼，其保護機制應考慮包含密碼長度限制、密碼組合限制、密碼錯誤次數限制。

5.10.3.開放一般教職員生使用之應用系統，則以不影響教職員生權益原則下規劃適當系統身分驗證機制，並於申請時建議帳號使用安全注意事項及變更預設密碼。

5.10.4.程式設計需使用帳號驗證機制時，應優先考慮與其他安全驗證機制整合，並以較嚴謹之機制為優先，參考順序為授權認證(CA)機制、輕量級目錄存取協定(LDAP)、作業系統帳號整合。

5.10.5.無法使用作業系統提供的驗證機制，則需在應用程式中使用自訂驗證機制，並加密處理後寫入資料庫。

5.10.6.各應用系統均應規劃適當之閒置時間，使用者登入較具機密性之應用系統後，若超過 30 分鐘無任何動作時，系統須設定將其帳號鎖定或登出 (特殊系統不在此規範) 。

5.11. 通行碼管理系統

5.11.1.應以互動式使用者通行碼管理系統，以安全有效的鑑別使用者身分。

5.11.2.應宣導使用者於權限申請核准後首次登錄系統時，依密碼設定原則立即修改預設密碼。

5.11.3.使用者若離職，由系統管理者立即註銷或停用其帳號。

5.11.4.不要將密碼以自動登入的方式登入系統。

5.11.5.停用帳號之刪除及回復應有正式程序並留下紀錄。

5.11.6.儲存於系統之密碼檔須加密儲存。

5.12. 具特殊權限公用程式之使用

5.12.1.應嚴格限制具有作業系統或應用系統特殊權限之公用程式的使用，如系統管理或權限控管功能。

5.13. 程式原始的存取控制

5.13.1.系統於開發或測試階段時，委外廠商應備份所有應用系統之程式碼及設定檔，並於開發完成後提供完整的程式安裝檔，供系統負責人保存。

5.14. 密碼式控制措施(加密控制措施)

5.14.1.資訊系統應保護敏感等級(含)以上之資料，防止洩漏或被竄改，必要時應使用資料加密等技術保護。

5.14.2.儘可能使用伺服器端程式，避免將程式置於客戶端(Client)執行，

以免遭受破解，並且不要在伺服器端(Server)上留有暫存檔，若必須使用設定檔，應避免使用容易猜測之檔名或採取適當檔案保護措施(如：加密或存取限制)。

5.14.3.對外提供敏感性資料的傳輸(如線上交易、線上金流等)應採取加密傳輸，以確保資料在網路傳輸過程中的安全性。

5.15. 遠距工作

5.15.1.如有資訊設備連線之需求，須由廠商填寫「網路連線服務服務申請表」，經相關權責主管核准後，執行權限開放。

5.15.2.於連線有效期間後，確實關閉或刪除外部人員連線功能。

5.15.3.連線存取機密性資料時須隔離 IP 網路區段，並限定其連線使用範圍。

5.15.4.臨時性廠商不開放連線申請，除有特殊需求，依相關規定辦理。

5.15.5.僅提供必要之網路服務項目、通訊協定、與連線時間，所有行為不得與原有之網路安全相關限制、規定相抵觸。

5.16. 存取事件紀錄的管理

5.16.1.系統有提供紀錄功能應予啟動，若無則視系統之重要性，以書面方式記錄之。

5.16.2.各系統的系統紀錄存取，應限定僅由系統管理者或具讀取權限者存取。

5.16.3.除預設之系統紀錄功能外，應考量記錄以下事件：

5.16.3.1.系統管理者及具備特殊權限帳號之登入成功及失敗事件紀錄。

5.16.3.2.使用者帳號異動及對密碼檔案之讀取與變更。

5.16.3.3.變更正式應用系統的程式原始碼及程式執行碼。

5.16.3.4.對於作業系統設定檔之存取及變更。

5.16.4.檢視各項系統紀錄及其異常狀況，要求各系統負責人進行改善，並依據「矯正管理規定」辦理。

5.17. 可攜式資訊設備管理

5.17.1.使用可攜式資訊設備時應謹防資訊外洩。

5.17.2.可攜式資訊設備應確實按規定安裝防毒軟體，若需要使用內、外部網路，應先評估網路環境之安全性，並確認檢查作業系統修正程式與更新病毒碼最新版本。

5.17.3.於公共空間使用時，應注意畫面是否有遭旁人窺視之疑慮。

5.17.4.不可將可攜式設備至於視線以外之處，並隨身攜帶不可拖運。

5.18. 非本校可攜式設備管理

5.18.1.訪客攜入可攜式裝置至本校機房需經機房管理人員許可。

5.18.2.處理機密等級為機密以上資料之工作區域(如資訊機房)，未經許可禁止使用相關設備進行拍攝或是螢幕畫面捕捉之行為，使用時需有本校人員在場陪同。

5.18.3.未經授權許可，禁止以設備及媒體執行網路偵測、弱點掃描、封包蒐集分析等高危險軟體。

6. 參考文件

6.1. 網路安全管理規定。
6.2. 資訊應用系統安全管理規定。
6.3. 矯正管理規定。
6.4. 電算中心軟硬體需求服務申請表。
6.5. 校園網路帳號申請表。
6.6. 帳號清查紀錄表。
6.7. 帳號清查結果報告。
6.8. 網路連線服務申請表。