ISSN 2616-7433 Vol. 8, Issue 3: 21-26, DOI: 10.25236/FSST.2026.080303

Research on Security Risk Investigation and Protection Countermeasures for Campus Office System Accounts

Jiahe Shao

School of Cyberspace Science and Technology, Beijing Jiaotong University, Beijing, China

Abstract: *Account security of campus office systems is a core component of the digital campus operation and maintenance system. The characteristic of risk transmission throughout the entire account lifecycle has imposed higher requirements on existing protection mechanisms. This paper analyzes the risk generation logic in the two core links of identity authentication and permission allocation, clarifies the risk transmission paths and triggering mechanisms in different links, and constructs a systematic risk investigation system from three dimensions: full-lifecycle investigation node setting, hierarchical classification of risk levels, and traceability verification of investigation results. Furthermore, practical protection optimization paths are proposed from three aspects: identity verification, dynamic permission adjustment, and normalized security drills. It is expected to provide a practical framework for institutions at all levels to optimize account security protection mechanisms for office systems and offer reference ideas for improving digital campus security standards.*

Keywords: *campus office system; account security; risk investigation; protection optimization*

1. Introduction

With the widespread adoption of digital campus administration models, campus office systems have become the core platforms carrying functions such as academic affairs approval, personnel management, and core data storage. Accounts serve as the only identity credentials for teachers and students to access the system and obtain corresponding services. Their security is directly related to the protection of personal information and the overall stability of campus administration operations [1]. At present, account protection in office systems of most institutions still remains at the level of single password verification. Risk identification mainly focuses on post-incident handling, and a risk prevention and control system covering the entire account lifecycle has not yet been established. Security incidents such as weak password cracking, unauthorized operations, and misuse of inactive accounts occur from time to time, posing direct threats to the security of core campus data [2]. Data from the upgrading of unified identity authentication platforms in multiple universities indicate that approximately 58.20% of student accounts and 21.70% of faculty accounts have weak password issues, while 38.46% of students fail to change their account passwords for extended periods. The delay in revoking permissions for personnel who have resigned or changed positions can reach as long as 45 days. By systematically analyzing the risk generation logic of campus office system accounts, establishing a standardized risk investigation system, and proposing practical protection optimization measures, it is possible to address the deficiencies in existing account security operation and maintenance mechanisms, reduce the occurrence probability of various account-related security incidents, and provide solid security support for the stable operation of digital campuses.

2. Risk Generation Logic of Campus Office System Account Security

2.1 Risk Transmission Path in the Identity Authentication Process

Identity authentication is the first line of defense for campus office system account security. Risks are gradually transmitted throughout the entire account lifecycle, from registration to deactivation, affecting subsequent permission usage and data security. During the registration stage, when teachers and students fill in personal information to apply for accounts, passwords with insufficient complexity become initial risk points. Such weak passwords remain in the system account database and create potential vulnerabilities for subsequent account intrusions. During the login stage, attackers may

ISSN 2616-7433 Vol. 8, Issue 3: 21-26, DOI: 10.25236/FSST.2026.080303

employ simple brute-force attacks or obtain corresponding account identity information through public information leakage incidents, impersonate legitimate users, and successfully log into the system, thereby transforming previously hidden initial risks into actual system access privileges. During the deactivation stage, if identity verification rules for account termination are insufficiently strict and accounts that are no longer eligible for use are not promptly removed by the system, such accounts may become hidden entry points for attackers. The associated risks may remain latent throughout system operation and may even trigger a series of subsequent problems, including unauthorized operations and data leakage.

2.2 Risk Triggering Mechanism in the Permission Allocation Process

Permission allocation is the core process for matching responsibilities and authorities of campus office system accounts. The degree of alignment between allocation rules and the actual work or study requirements of different roles directly affects the probability of risk generation during account usage. Administrative personnel generally possess permissions covering multiple functional modules, including academic affairs approval and institution-wide data retrieval. If the initial allocation process does not clearly define applicable scenarios and validity periods of permissions, permissions may easily exceed actual job requirements, making inactive high-privilege accounts primary targets for attackers [3]. Correspondingly, permissions assigned to teachers are generally configured according to teaching and research requirements. If original permissions are not synchronously revoked after position adjustments, permission reuse problems may arise, allowing resigned or transferred personnel to continue accessing non-public teaching and research content through the system. Permissions assigned to students are generally limited to basic functions such as grade inquiry, activity application, and submission of practical training materials. If the system fails to clearly define permission boundaries for student accounts, some accounts may gain access to content beyond their authorized scope through unconventional pathways, thereby creating opportunities for subsequent unauthorized operations. If permission allocation rules for these three categories of users lack a dynamic adjustment mechanism, fragmented permission-related issues will gradually accumulate and eventually evolve into substantial account security risks.

3. Construction of a Security Risk Investigation System for Campus Office System Accounts

3.1 Setting Investigation Nodes Throughout the Entire Account Lifecycle

Investigators may establish corresponding investigation nodes according to the circulation logic of accounts from creation to termination, covering the entire account operation process, reducing investigation gaps between different stages, and lowering the possibility of missed risk identification. The process begins with the registration stage, where the consistency between the personal information submitted by account applicants and the real-name database of teachers and students is verified, and the complexity settings of initial passwords are examined to determine whether they meet basic security requirements, thereby filtering out initial risks such as false registrations and weak passwords at the source. The investigation at the registration stage covers all newly created accounts and is completed before accounts are officially entered into the system and activated, ensuring that the basic information of every new account is verified and preventing unauthorized account applications by non-campus personnel. The investigation then proceeds to the usage stage, focusing on verifying the ownership of login devices, changes in frequently used login locations, and the compatibility between account operations and the permission scope of the corresponding role, thereby promptly identifying potential risks such as abnormal logins and unauthorized operations. Investigations during the usage stage combine periodic inspections with dynamic spot checks, covering all active accounts throughout their entire usage period and preventing subsequent risks arising from account impersonation [4]. The next step is the investigation of the modification stage, which involves verifying the correspondence between account permission adjustment applications and changes in positions or roles, as well as examining the progress of old permission revocation and the scope of newly granted permissions, thereby preventing issues such as permission reuse and excessive permission allocation. Investigations during the modification stage are initiated after permission adjustment applications are submitted and cover all accounts undergoing role changes or permission adjustments, ensuring consistency between responsibilities and authorities and preventing resigned or transferred personnel from retaining high-level permissions beyond their actual needs. Finally, the investigation of the deactivation stage is conducted by verifying the qualifications of account deactivation applicants, examining the completion

ISSN 2616-7433 Vol. 8, Issue 3: 21-26, DOI: 10.25236/FSST.2026.080303

status of pending tasks and the progress of permission revocation for accounts awaiting deactivation, and clearing inactive or dormant accounts that are no longer eligible for use. Investigations during the deactivation stage are initiated after deactivation applications are submitted and cover all accounts for which deactivation requests have been submitted, as well as accounts that have not logged in for more than six months. This helps eliminate hidden risk entry points within the account system and prevents inactive accounts from becoming gateways for attackers to infiltrate the system. The four investigation nodes—registration, usage, modification, and deactivation—are implemented sequentially to form a closed-loop investigation chain.

3.2 Hierarchical Classification Criteria for Security Risks

After completing risk identification at each investigation node, investigators require a unified classification standard to categorize all identified risks, match them with corresponding remediation resources, and improve the effectiveness of risk handling. The first criterion is the scope of risk impact, which primarily considers the number of affected accounts and the types of associated system modules. The greater the number of affected accounts and the more critical the associated system modules, the higher the corresponding risk level. Assessment from this dimension can quickly distinguish global risks from localized risks and prevent the misallocation of remediation resources. The second criterion is the degree of harm, which mainly evaluates the actual consequences that risks may cause. If a risk may result in unauthorized access to sensitive data, disruption of the normal operation of core business functions, or similar consequences, the corresponding risk level is considered higher. Assessment from this dimension enables the prioritization of risks that may cause actual losses and reduces the probability of security incidents [5]. The final criterion is the difficulty of remediation, which primarily considers the human and time costs required for risk correction as well as the extent to which remediation activities may affect normal system operations. The greater the resources required for remediation and the more significant the impact on system operations, the higher the corresponding risk level. Assessment from this dimension helps investigators reasonably plan remediation schedules and avoid situations in which remediation activities themselves interfere with the normal operation of the office system.By integrating assessment results from these three dimensions, investigators can determine the final risk level and the corresponding remediation priority. Specific classification criteria are presented in Table 1.

Table 1. Criteria for Classification of Security Risk Levels in Campus Office System Accounts

Risk Level	Scope of Risk Impact	Degree of Harm	Remediation Difficulty	
Level I	Covers all accounts or is associated with core system modules such as academic affairs, personnel, and finance	May lead to large-scale leakage of sensitive information of teachers and students and institution-wide disruption of office operations	Requires suspension of system services and coordinated remediation across multiple functional departments	Highest
Level II	Covers all accounts of a specific user role or is associated with multiple non-core business modules	May lead to leakage of non-public information of a specific user group and disruption of localized office operations	Does not require suspension of system services and can be remediated by a single functional department	High
Level III	Covers a small number of individual accounts and is associated with only a single functional module	May lead to personal information leakage of an individual user without affecting the overall operation of office services	Can be quickly remediated through routine system operations	Medium
Level IV	Involves only non-core permission anomalies of a single account and has no associated business module risks	Will not result in information leakage or business disruption	Can be remediated during routine account operation and maintenance activities	Low

ISSN 2616-7433 Vol. 8, Issue 3: 21-26, DOI: 10.25236/FSST.2026.080303

3.3 Traceability Verification Rules for Investigation Results

Traceability verification of investigation results serves as a reverse-checking process for the preliminary risk identification work. It can reduce various deviations that may arise during the investigation process and provide a reliable basis for subsequent risk remediation activities. First, investigators conduct a retrospective analysis of risk-related operation paths. Following the operational timeline of the account involved, they verify the consistency between the operator, operation content at each node, and the corresponding records in the system backend logs. If the abnormal signals identified during the investigation are completely consistent with the operational behaviors recorded in the system logs, the existence of the risk can be preliminarily confirmed. This helps prevent temporary system fluctuations or normal user operations from being mistakenly identified as account security risks. Second, investigators reproduce the triggering conditions of identified risks. In a dedicated system testing environment, the complete process through which the risk occurred is simulated by restoring the account's network environment, assigned permissions, and the specific actions that triggered the anomaly. Only when the same abnormal results can be reproduced under identical conditions can the actual degree of harm be accurately assessed. This approach reduces the likelihood of overestimating or underestimating the severity of identified risks. Third, investigators perform cross-verification of validation results [6]. After completing the first two verification steps, operation and maintenance personnel from different positions conduct a secondary review of the verification results. During this process, particular attention is paid to whether the basis for risk identification is complete and whether the risk classification conforms to established standards. Risks without objections can directly proceed to the subsequent remediation stage, whereas disputed risks may undergo another round of full-process verification. This helps prevent omissions or misjudgments resulting from the subjective assessments of individual investigators. Upon completion of the entire traceability verification process, all verified risks are documented in corresponding investigation records, including the causes of the risks, the verification procedures, and the assessment results. These records provide valuable references for future investigations of similar security risks.

4. Protection Optimization Measures for Campus Office System Account Security

4.1 Unifying Identity Verification to Reduce the Risk of Unauthorized Access

Identity verification is the fundamental mechanism safeguarding access to campus office systems. The consistency of verification rules and the strictness of verification procedures directly affect the likelihood of account impersonation and unauthorized login incidents. First, differences in existing verification rules for different user roles should be systematically reviewed. The overlapping and differing elements of the original verification procedures for administrative staff, teachers, and students should be compared one by one. Redundant and ineffective verification steps should be removed, while previously omitted verification requirements should be supplemented to establish a unified verification standard covering all account types. Regardless of user role or permission level, all accounts must satisfy the corresponding verification requirements before obtaining system access privileges. This approach eliminates security gaps caused by inconsistent verification standards across different user groups and establishes a unified access threshold for all accounts at the source. Unified password requirements should also be implemented. Passwords should contain no fewer than eight characters and include letters, numbers, and symbols. After implementing such a policy, one institution reduced the proportion of weak-password accounts from 58.20% to 12.60%, significantly lowering the success rate of brute-force attacks. Second, a multi-factor authentication model should be adopted. In addition to verifying account credentials, dynamic verification information linked to the user's personal identity should be incorporated into the authentication process. Access should only be granted when both categories of information have been successfully verified. This substantially increases the difficulty of account misuse following brute-force attacks or personal information leakage, blocks unauthorized access pathways at the login stage, and reduces subsequent risks arising from weak passwords and information disclosure. Before implementing the upgraded authentication mechanism, one institution recorded 12,476 abnormal login alerts per month. After implementation, the number decreased to 1,892, representing a reduction rate of 84.80%. Meanwhile, the success rate of phishing-link-based account theft declined significantly from 2.68% to 0.21%. Requiring successful verification of both categories of information greatly reduces the likelihood of account compromise resulting from brute-force attacks or personal information leakage. Finally, differentiated verification frequencies should be established according to account permission levels. Accounts possessing high-level privileges, such as access to

ISSN 2616-7433 Vol. 8, Issue 3: 21-26, DOI: 10.25236/FSST.2026.080303

core data or academic affairs approval functions, should be required to complete identity verification each time they access core data modules. Ordinary accounts that are limited to basic functions such as grade inquiry and material submission may be exempt from repeated verification within a predefined login validity period. This approach minimizes opportunities for unauthorized operations involving high-privilege accounts while preserving the normal user experience of teachers and students. It also reduces the security impact of compromised high-privilege accounts and achieves an effective balance between verification rigor and usability.

4.2 Dynamically Adjusting Permissions to Prevent Unauthorized Operations

Dynamic adaptation of permissions is a key approach to reducing mismatches between account authorities and responsibilities and can effectively limit opportunities for unauthorized operations during system use. First, fixed triggering scenarios for permission adjustment should be clearly defined, covering four critical stages: staff position transfers, student grade progression or advancement, semester completion, and academic year closure. At these specific stages, operation and maintenance personnel initiate comprehensive permission reviews for all accounts and match permission scopes against the latest personnel identity information one by one. This helps prevent situations in which existing permissions are not adjusted promptly following changes in user status. All active accounts are included in the review process, ensuring that no accounts are overlooked because of their permission level or user category.

Second, a comprehensive approval process for permission adjustments should be established. All permission modification requests must be accompanied by corresponding supporting documentation. Two rounds of verification should be conducted separately by the responsible personnel of the account-owning department and by system operation and maintenance staff. Permission updates may only be implemented after confirming that the requested adjustments fully correspond to the user's latest work or study requirements. Upon completion of permission adjustments, the system automatically generates and retains adjustment records. These records facilitate retrospective investigations in the event of anomalies and provide reference data for future optimization of permission allocation policies.

In addition, a regular cleanup mechanism for inactive permissions should be established. Operation and maintenance personnel should review permission usage across all accounts on a quarterly basis. Non-essential permissions that have not been used for three consecutive months should be automatically flagged by the system. After verification with the account holder, permissions that are no longer required should be uniformly revoked. For individuals who are no longer eligible to use the system, such as graduated students and resigned faculty or staff members, all associated permissions should be completely revoked within seven working days after the change in identity status. This approach fundamentally prevents individuals with invalid identities from retaining system permissions and reduces unnecessary occupation of permission resources, ensuring that the entire permission framework remains highly aligned with actual user needs. Through this mechanism, the time required to process permission adjustments associated with personnel changes can be reduced from 45 days to 6 days, significantly mitigating security risks arising from excessive account permissions.

5. Conclusion

Account security protection for campus office systems is a systematic undertaking that spans the entire account lifecycle. The generation and transmission of risks involve multiple core processes, including identity authentication and permission allocation. Therefore, relying solely on individual technical protection measures or isolated investigations is insufficient to establish a complete security protection framework. By constructing a security risk investigation system covering the entire account lifecycle and establishing standardized risk classification criteria and traceability verification mechanisms, risks can be identified at an early stage and accurately assessed, thereby providing a reliable factual basis for subsequent risk remediation. Future protection optimization efforts should balance security and usability. On the basis of unified identity verification standards, permission scopes should be dynamically adjusted according to the actual needs of different user roles. In addition, normalized security drills should be conducted to identify potential vulnerabilities in a timely manner. Through these measures, a comprehensive, practical, and full-chain account security protection mechanism can be gradually established, providing a solid security foundation for the stable advancement of digital campus administration.

ISSN 2616-7433 Vol. 8, Issue 3: 21-26, DOI: 10.25236/FSST.2026.080303

References

[1] Sun, J., Zheng, J., Yang, Y., et al. Research and Practice on Security Management of University Unified Identity Authentication Systems[J]. Network Security Technology & Application, 2025(10): 93-95.
[2] Xiao, Q. Analysis of Information Security Protection Strategies for Office Automation Systems[J]. China New Telecommunications, 2026, 28(5): 10-12.
[3] Zhao, W. Application of Artificial Intelligence in University Campus Cybersecurity Technologies in the Era of Big Data[J]. Software, 2024, 45(1): 158-160.
[4] Chen, Y. Practice of Security Authentication Methods for Campus 5G Dual-Domain Private Networks[J]. Information Technology & Informatization, 2024(7): 142-145.
[5] Dong, X., Zhao, Z. Construction and Practice of a Security Protection System for University Email Systems: A Case Study of Capital Medical University[J]. Medical Education Management, 2026, 12(1): 127-132.
[6] Hu, W., Guo, L., Wang, Y. Analysis of the Application of Artificial Intelligence in Campus Network Security[J]. Digital User, 2025(33): 40-42.