Student Information System Access Procedure

Purpose
The purpose of this procedure is to establish the procedures for accessing the student Information system or Banner.

Audience
This procedure applies to employees seeking access to the TAMUK’s student information system.

Applicability
Employees seeking access to the Banner student information system must complete a Banner Security Request form.

Definitions
1. **Banner**: TAMUK’s Student Information System.
2. **Banner Internet Native Banner (INB)**: This is the administrative interface into Banner. Access discussed in this procedure refers to this mode of access.
3. **iTech Banner Security Officer (BSO)**: Person responsible for monitoring and implementing security controls and procedures for Banner.

Student Information System Access Procedure

1. Account Creation
   a. The Banner Access Request form must be completed and signed by the applicant and his or her supervisor. The form will then be submitted to the Office of the Registrar for assignment of the Banner security class best suited to the applicant’s duties.
      1) Since TAMUK follows the principle of least privilege, employees are given the minimum access to student information necessary to perform their duties.
      2) If access to the Banner Financial Aid module is required, approval from the Director of Student Financial Aid Services or designee is required.
      3) If access to the Banner Accounts Receivable module is required, approval from the Director of Business Services or designee is required.
   b. The Office of the Registrar then returns one copy of the form to the applicant. The original is sent to the BSO.
   c. The BSO creates an account in test and production and assigns the security classes identified by the Office of the Registrar.
      1) The applicant and the Office of the Registrar are notified via email when the Banner Access Credentials have been created.
      2) The applicant must receive Banner training from an approved source before getting his or her production Banner Access Credentials. If there is no member of the applicant’s department to provide training, the Office of the Registrar will conduct the training.
      3) The production account remains locked until notification of training is received by the BSO.

2. Account Monitoring
   As part of the account maintenance process all supervisors are required to review their employees’ access quarterly. The BSO will send user access reports quarterly to every supervisor for their review. It is the responsibility of the supervisor to determine if the access granted to their direct reports is current and accurate. Discrepancies should be reported to the BSO immediately.
3. Account Password Expiration/Inactivity
   a. INB account passwords expire after 90 days and must meet complexity requirements defined in the TAMUK Password Procedure.
   b. Accounts that have passwords expired for over 30 days are locked
      a. Users must submit a ticket via the iTech Support Site in order to have their accounts unlocked.
   c. Accounts that have their passwords expired for 90 days must submit a new Banner Access Request form.
   d. Accounts not accessed for 90 days will be deleted and must submit a new Banner Access Request form.

4. Account Termination
   Termination of accounts will be conducted through the employee checkout process for employees who terminate through the normal university checkout process. The BSO will also perform weekly cleanup of accounts of employees who do not terminate through the normal university checkout process.

Disciplinary Actions
Violation of this procedure may result in disciplinary action up to and including termination for employees and temporaries; a termination of employment relations in the case of contractors or consultants; dismissal for interns and volunteers; or suspension or expulsion in the case of a student. Additionally, individuals are subject to loss of TAMUK Information Resources access privileges, civil, and criminal prosecution.

References
1. Copyright Act of 1976
2. Computer Fraud and Abuse Act of 1986
4. DIR Practices for Protecting Information Resources Assets
5. DIR Standards Review and Recommendations Publications
7. The Health Insurance Portability and Accountability Act of 1996 (HIPAA)
8. IRM Act, 2054.075(b)
9. The State of Texas Information Act
10. The State of Texas Penal Code, Chapters 33 and 33A
11. Texas Administrative Code, Chapter 202
12. Texas A&M University-Kingsville Procedure 29.01.03.K1.010
13. Texas A&M University-Kingsville Procedure 29.01.04.K1.010
14. Texas Government Code, Section 441