Student Information System Special Access Procedure

Introduction
Access to the Banner Student Information System is generally granted through Internet Native Banner (INB) or Self Service Banner (Blue and Gold) at Texas A&M University-Kingsville (TAMUK). There are special situations where report writers and developers need access to the Banner database outside of these methods.

Purpose
The purpose of this procedure is to define the procedures for special access to the Banner database.

Audience
This procedure applies to individuals requesting special access to the Student Information System database for report writing or development.

Definitions
1. Argos: The institutionally supported platform for report development.
2. Banner: TAMUK’s Student Information System.
3. Banner Internet Native Banner (INB): This is the administrative interface into Banner.
4. iTech Banner Security Officer (BSO): Person responsible for monitoring and implementing security controls and procedures for Banner.
5. iTech support site: The iTech help desk ticketing system site accessible at http://support.tamuk.edu.

Student Information System Special Access Procedure
1. Report writers should use Argos for report development which provides the appropriate security and encryption necessary to meet University standards for access to sensitive or confidential information.
2. Argos access must be requested through the iTech support site. All requests for development level access will be approved through the Banner Users Group.
3. For users requiring direct access to the Banner database, all connections must be over an encrypted medium. iTech currently supports the use of SSH tunneling in order to provide this access. All requests for this level of access must be requested through the iTech support site and approved by the Banner Users group.
4. 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 Banner Security Officer immediately.
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