The Texas A&M University System
Texas A&M Engineering Extension Service

Standard Administrative Procedure

61.01.02.01.2 - Student Management Systems (SMS) Access and Privilege

Approved: September 1, 2005
Revised: March 10, 2011
Revised: September 9, 2021
Next Scheduled Review: September 9, 2026

Summary

This document provides guidance and procedures for acquiring access privileges to the TEEX student management systems.

Definitions

Student Management Systems (SMS) – TEEX systems that is used for the entry and storage of participant and class information (Course Class Maintenance [CCM], TEEXApps)

User - TEEX employee (full-time, wage or student worker) that requires access to student management systems as part of their job duties.

Requirements

1. General

1.1. The SMS is the universal repository used for entering, recording, and securely storing documentation related to TEEX sponsored events.

1.2. All TEEX sponsored events provided by the agency must be entered into the SMS. All training and technical assistance scheduled (delivered or canceled) by the agency must be accurately entered in the SMS. TEEX emergency response efforts as delivered by Texas Task Force are not recorded in SMS; this State directed technical assistance is recorded in the Task Force's independent data management system

2. System Owner

2.1. As required by *Title 1, Part 10, Chapter 202, Rule §202.22, Texas Administrative Code* the Assistant Agency Director for the Strategic and Education Services (SES) Department is the appointed system owner of TEEX SMS and is primarily responsible for the accuracy and integrity of the SMS information.

2.2. The SMS Administrator is the agency main point-of-contact for SMS and TEEXApps systems in order to promote the quality and integrity of the data entered and reported into the systems.

2.3. The SMS Custodian is the Chief Information Officer (CIO), Associate Agency Director of Network Information Systems (NIS) and is entrusted by the information owner to provide proper protection and care of the information resource and to ensure availability of the SMS information.

2.4. The system owner and custodian are responsible for:

2.4.1. Approving access privileges and assign custody of the information resources asset;

2.4.2. Determining the asset's value;

2.4.3. Specifying data control requirements and convey them to users and custodians (NIS, Items 1.A-E, G, and H; SES, Item F);

2.4.4. Specifying appropriate controls, based on a risk assessment, to protect the state's information resources from unauthorized modification, deletion, or disclosure. Controls shall extend to information resources outsourced by the agency;

2.4.5. Confirming that controls are in effect that reasonably ensure the accuracy, authenticity, and integrity of data;

2.4.6. Ensuring compliance with applicable controls;

2.4.7. Assigning custody of information resources assets and provide appropriate authority to implement security controls and procedures; and

2.4.8. Reviewing access privilege lists based on documented agency security risk management decisions

3. Security

3.1. The SMS environment is a proprietary information resource, owned and operated by TEEX. The SMS environment is an on-premise solution that operates in TAMU datacenters. The TAMU data centers comply with Texas A&M University, Texas A&M University System and Texas Administrative Code requirements for physical protection of information resources. TEEX information resources in the TAMU data centers are digitally protected by a TAMU and TEEX network boundary.

3.2. All TEEX information resources, including the SMS environment, is protected according to the TEEX Information Security Controls Standards Catalog, established by the TEEX SAP 29.01.03.N0.01, *Information Security Program*. The TEEX Information Security Controls Catalog (a modified NIST 800.53) complies with Texas A&M University System and Texas Administrative Code 202 security requirements.

3.3. Any exception to the security controls or related SAPs used to protect the SMS environment will be reviewed by appropriate personnel including, but not limited to, the agency Chief Information Officer, Information Security Officer and SMS Information Owner for approval or denial.

4. Access

4.1. The SMS information owner, or SMS administrator is responsible for approving and documenting access privileges for SMS users and coordinates with NIS to ensure that appropriate controls are implemented and enforced to protect the confidentiality and integrity of the data entered into and stored in the SMS.

4.2. All new SMS users are required to complete the CCM/TEEXapps User Training which shall be coordinated with and delivered by the SMS Administrator.

4.3. Division Directors, Associate Directors, Business Services Directors or Division SMS Leads must request access privileges for their SMS users.

4.4. The CCM/TEEXApps Access form (Form SES-44) shall be submitted by email to the SMS Administrator in SES.

4.5. The TEEX Network Information Services (NIS) HelpDesk shall notify the SMS Administrator of any employee termination or inactivation (wage employee) and the SMS Administrator shall immediately remove all SMS user access privileges for the terminated or inactivated employee.

4.6. Based upon any changes in duties for approved SMS users, TEEX business units shall submit a request to the SMS Administrator to remove, downgrade, or upgrade an employee's SMS user access privileges.

Quality Assurance Measures

The SMS Administrator maintains a user access privilege list and reviews the list at least semi-annually for accuracy with Division SMS Leads.

Related Statutes, Policies, or Requirements

Tex. Educ. Code Chapter 202, *Information Security Standards*
ACCET Standard II.D.1
TEEX SAP 29.01.03.N0.01, *Information Security Program*
TEEX Form SES 44, CCM/TEEXApps Access form

Responsible Office

Strategic and Educational Services
(979) 458-6807