

**SIS SECURITY
STATEMENT OF RESPONSIBILITY**

Initial Access

I understand that I will be violating System and university regulations and state and federal law if I gain or help others gain unauthorized access to the Student Information System (SIS): I acknowledge that neither I nor anyone else possess the authority to allow anyone to use my ID or password. (See back for TAMUS Electronic Information Services Access and Security Policy)

I also understand that if I violate university regulations and state and federal laws by gaining or helping others gain unauthorized access to SIS, I will be subject to university disciplinary action and criminal prosecution to the full extent of the law. (Chapter 33, Section 1, Title 7 of the Texas Penal Code)

By logging on to this computer system, I acknowledge my responsibility for strictly adhering to university policy and state and federal law. I also am aware the penalties exist for unauthorized access, unauthorized use or unauthorized distribution of information from SIS.

I agree further not to attempt to circumvent the computer security system by using or attempting to use any transactions, software, files or resources I am not authorized to use.

<hr/> Last Name (Print Clearly)	<hr/> First Name	<hr/> MI	<hr/> Date
<hr/> Signature	<hr/> Social Security Number		
<hr/> Title	<hr/> Date of Birth	<hr/> e-mail	
<hr/> Department	<hr/> User ID	<hr/> extension	
<hr/> Supervisor (please print)	<hr/> Date	<hr/> e-mail	
<hr/> Signature	<hr/> Extension	<hr/> Model	

Model Verified by Registrar's Office _____

CTS Use Only:
Entered By: _____ Date: _____ Notified User: _____ Oper# _____ User ID: _____

TEXAS A&M UNIVERSITY SYSTEM REGULATIONS

21.01.06 Electronic Information Services Access and Security

March 7, 1997, Revised September 4, 2002

Supplements System Policy 21.01

1. The Texas A&M University System (the System) electronic information resources are vital academic and administrative assets which require appropriate safeguards. Computer systems, networks, and data are vulnerable to a variety of threats. These threats have the potential to compromise the integrity, availability and confidentiality of the information.
2. To ensure that System electronic information services are as secure as possible, various security management processes and procedures must be employed to eliminate or mitigate risks to various System information resources. The System prohibits unauthorized access to electronic information services.
3. System employees who use various electronic information services are assigned a unique login name or ID to access these resources. Users are required to protect and maintain the confidentiality of their passwords. Unauthorized access to electronic services may result in risk or liability for the user and/or the System. Measures shall be taken to protect these resources against unauthorized access, disclosure, modification or destruction whether accidental or deliberate.
4. Security officers are appointed for administrative applications for each System component. These security officers will process the appropriate security authorization forms for the applications/information resource system for which they have responsibility. These forms will include a place for the applicant to acknowledge receiving and reading the regulations contained on the form. These forms should be maintained on file and procedures should be in place to allow for the regular review of access rules granted to each login name or ID.
5. The Texas A&M University System (the System) is required to comply with the Texas Administrative Code (TAC) on "**Information Security Standards**". TAC assigns the responsibility for protection of informational resources to the component Chief Executive Officers (CEOs). The CEOs shall develop procedures to implement requirements of federal and state laws and the intent of this regulation.