MAXIENT SECURITY REQUEST FORM

USER INFORMATION (PLEASE PRINT) ☐ **Initial Request** ☐ **Renewal**

Last Name	First Name	MI	Date
Title		Email	Extension
Network ID		Department	Bldg & Room #

Individual found in violation of the terms below are subject to loss of access to the Maxient System. Your signature below acknowledges agreement to these terms.

Applicant Signature	Date	UIN

ACCESS APPROVALS

Supervisor Name	Email	Date
Supervisor Signature	Title	Extension
Registrar Signature		Date
SCCE Admin Signature		Date

Texas A & M University System Regulations

21.01.06 Electronic Information Services Access and Security
   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 officer are appointed for administrative applications 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.

FOR OFFICE OF STUDENT CONDUCT & OIT PERSONNEL USE ONLY

Level Access: 1   2   3   4   Approved by: _____   Date: _____

Comments: _____

Original-Security Officer/OIT   Canary-Office of SCCE   Blue-Registrars   Pink-Applicant