I. New Account Creation ................................................................................................. 2-3
II. Usage .......................................................................................................................... 4-5
II. Account Modifications & Transfers ........................................................................... 6-7
III. Account Locking/Closing/Cleaning ........................................................................... 8-9
IV. Audits ....................................................................................................................... 10
V. General ........................................................................................................................ 11-14
  a. FERPA ....................................................................................................................... 11
  b. Training ..................................................................................................................... 11-12
  c. Passwords .................................................................................................................. 13
  d. Holds .......................................................................................................................... 13-14

SIS Access Managed by the

SIS SECURITY TEAM
JD Villanueva & Chris Villarreal

Enrollment Services
MS 2.02.04
210.458.7598
210.458.5068
SISSecurity@UTSA.edu
Student Information Systems User Policies & Procedures

I. New User Account Creation

POLICIES

Banner User Account vs Banner ID Number
A Banner User Account is not the same as a Banner ID Number.

- UTSA faculty, staff, and students are issued Banner ID numbers upon admission or appointment. The Banner ID number is currently listed on the UTSACard and is used as a personal identifier for a person’s record in Banner. This number was formerly used to login to ASAP, Banner’s web interface.

- A Banner User Account is required in order to access the Banner, the student information system used here at UTSA. Only authorized users are provided access.

Banner User Account Requests
All requests for new Banner User Accounts must be made using an updated revision of the online SIS Account Request, available online: https://sisaccessrequest.utsa.edu from the SIS Security website. As the link is revised frequently, the access request should be accessed online for each request.

A SIS User Account is considered new if the user has never been issued an account before, the account has been inactive or access removed, or the user has transferred to a new department at UTSA.

In order for an account to be created, SIS Security must receive a completed access request and the user must be a currently appointed faculty or staff member. The user should have a current @UTSA.edu email account. If the user will not be issued a @UTSA.edu email address, correspondence will be sent to the listed supervisor. Banner User Accounts will not be released until the user has officially begun employment.

Banner User Responsibility
It is the responsibility of the user to keep their Banner User Account active and open. Users should successfully login to Banner at least every 90 days and notify SIS Security immediately if there are any login issues.

PROCEDURES ON NEXT PAGE
PROCEDURES

Before requesting a Banner User Account, the requested user should:

1. Have an active appointment with UTSA & officially begun employment
2. Have an active myUTSA ID (Network ID)
3. Be issued a staff email address (exemptions accepted, when applicable)
4. Successfully complete the Banner Users & FERPA Compliance Awareness Module (C927) through MyTraining.

To request a new Banner User Account:

1. Complete a SIS Account Request in full, available at: https://sisaccessrequest.utsa.edu
   Directions to assist in completing the form are available online at:
   http://www.utsa.edu/enrollment/facultystaff/banner/
2. The completed form is submitted to SIS Security electronically via our online process.
3. The request is reviewed by SIS Security. Incorrect or incomplete forms are returned to the User or forwarded for authorization. Correct forms are processed.
4. The Banner User Account is created. Permissions are given as authorized on the form.
5. The user is notified by email (@UTSA.edu) when their account has been created. The email will include their username and access to their temporary password.
   - More information on Passwords can be found in Section c. Passwords of Part V. GENERAL of this manual.
6. If additional access has been requested (Xtender, AppWorx, BOXI), and the account created an email will be sent with all login information separately.
II. Usage

Federal Family Education Rights and Privacy Act
FERPA, The University of Texas System rules and regulations, and University rules and regulations govern the conduct of employees and School Officials with access to student records who act in the student’s educational interest within the limits of the employees or School Official’s need to know. To ensure compliance, the University requires that employees and School Officials be aware of federal law as well as System and University regulations that govern student records. SIS Security requires users acknowledge this statement by initialing on the SIS Account Request. Additionally, Banner Security requires successful completion of the Banner Users & FERPA Compliance Awareness Module (CT927) within one calendar year before Banner access will be granted.

Confidentiality
Security passwords should remain confidential. Users must lock the computer or log off any application they are using, including Banner, when they leave their computer work station.

Educational Records
Users may access student records only as required to perform assigned duties. They may not update their own record or that of any person known to them or of a relative. Within the University, anyone whose designated responsibility requires access may use information from student records for appropriate research, education, or service functions.

User Agreement
Users must understand that Banner accounts are assigned to them at the request of their supervisor to be used only in connection with assigned duties as an employee of the University of Texas at San Antonio and may be revoked without notice upon the request of the administrator or the SIS Security Team. The user must understand and accept the following terms and conditions:

• Passwords are the first line of security. The user agrees not to reveal their password nor allow anyone to use the account assigned to them. The user is responsible for any changes made to the database under their username.
• The user must maintain the confidentiality of any and all data that they retrieve in the course of their job duties, including data they use for reporting purposes or in other software products.
• Access to the records will be determined by the requirements of the user’s job, and therefore the user will only be authorized to retrieve data on a “need to know” basis.
• The user will not knowingly enter false or misleading data into any record or knowingly expunge a record or data entry.
Student Information Systems User Policies & Procedures

• The user agrees to comply with all institutional policies on security, computer access, confidentiality of data, data standards, and data integrity.
• Any violation of these policies may lead to the immediate suspension of computer privileges. Unauthorized release of sensitive or restricted information is a breach of data security and may be cause for disciplinary action, which could include dismissal.

Resources

• UTSA Acceptable Use Policy
  http://www.utsa.edu/hop/chapter8/8-15.html

• UTSA Information Resources Use and Security Policy (HOP 8.12)
  http://www.utsa.edu/hop/chapter8/8-12.html

• Office of Information Security
  https://www.utsa.edu/oit/FacultyAndStaffServices/Policies/index.html
III. User Account Modifications & Transfers

POLICIES

Account Modifications to Access
Any access change to an existing Banner User Account is considered an Account Modification. Unless otherwise stated, Account Modifications require the completion of a SIS Account Request, with all appropriate authorization for the new access being requested. Users submitting a request for modification to an existing account will be required to complete any training required of new users if they have not completed it within a year.

Non-Access Account Modifications
Modifications to existing Banner User Accounts that do not require a change in access are allowed under certain circumstances.
If a user requests for their Banner Username to reflect their new name, the request must be made in writing by email to SiSSecurity@UTSA.edu. The new name must already be reflected in their @UTSA.edu staff email address.
Changing the Banner Username will not change the name anywhere else.

Transfers
Users transferring to a new department are not considered modifications but new accounts. When a user is leaving a department, regardless of reason, SIS Security should be notified. The user’s account will be locked after their last day in the department. The user’s new department will need to submit a new, complete SIS Account Request.
SIS Security may lock the account of a transferred Banner User until a new SIS Account Request is received and processed.

PROCEDURES ON NEXT PAGE
Account Modifications are processed similar to Banner User Accounts

1. Complete a SIS Account Request in full, available at:
   http://www.utsa.edu/enrollment/facultystaff/banner/
   Directions to assist in completing the form are available online at:
   http://www.utsa.edu/enrollment/facultystaff/banner/
2. If the user has not already done so within a year, they must successfully complete the Banner Users & FERPA Compliance Awareness Module (CT927) through MyTraining.
3. The completed SIS Account Request is submitted to SIS Security.
4. Incorrect or incomplete forms are withdrawn and a new Request needs to be created. Correct requests are processed.
5. The user’s account is modified as indicated on the request. Unless otherwise stated, permissions are added to existing access if the user retains the same title/department.
6. The user is notified by email (@UTSA.edu) when their account has been modified.
7. If additional non-Banner access modifications have been requested (Xtender, AppWorx, BOXI), the user will be notified separately if non-Banner accounts have been modified.

Transfers within the UTSA Community are processed:

1. Leaving department notifies SIS Security of user’s departure. This can be done by the department emailing SISSecurity@UTSA.edu or the completion of a Separation Notice through HR.
2. SIS Security will lock the user’s account after the user’s last working day in the leaving department.
3. The user’s new department completes SIS Account Request in full.
4. If the user has not already done so within a year, they must successfully complete the Banner Users & FERPA Compliance Awareness Module (CT927) through MyTraining.
5. The completed request is submitted to SIS Security.
6. Incorrect or incomplete requests are returned to the User or forwarded for authorization. Correct requests are processed.
7. The user’s existing access is replaced by the new access requested.
8. The user’s account is unlocked. If it has been over 30 days since the user last accessed their account, the password will be reset and expired.
9. The user is notified by email (@UTSA.edu) when their account is unlocked and modified to fit their new department.
10. If additional non-Banner access has been requested (Xtender, AppWorx, BOXI), the user will be notified separately if non-Banner accounts have been modified.
IV. Account Expiring/Locking/Cleaning

POLICIES

Expiring, Locking, and Cleaning accounts is necessary to ensure proper access is granted. Users who only infrequently access Banner should take care to keep their account active by logging in on a regular basis (at least once every 90 days) and notifying the SIS Security Team promptly should there be any problems.

Inactive Accounts
Accounts are considered Inactive if there has not been a successful user login for 90 or more days. Inactive accounts are Locked. Users must contact SIS Security if they find their account has been locked for any reason, including inactivity. To prevent an account from being inactive, the user should successfully login to Banner on a regular basis. Logins to ASAP or a third party application, such as Application Xtender or Crystal Reports, do not constitute a Banner Account login. Only successful logins to Banner INB PROD are used to measure account activity.

Locked Accounts
An account may be locked after too many incorrect password attempts, at the end of a temp hire period, when considered inactive, or upon receipt of a Separation & Transfer notice. The reason for the lock will determine how the account can be unlocked. Accounts locked due to inactivity or too many incorrect password attempts require an email request to SISSecurity@UTSA.edu from the user’s staff email account. Accounts locked due to separation, transfer, or end of temp hire period require submission of a new, complete SIS Account Request to regain access.

Cleaning Locked Accounts
Accounts locked and/or expired for any reason for 90 or more days will be cleaned of access. Once cleaned, the user will need to submit a new, complete SIS Account Request to regain access. As no record is kept of past access, a new request is required and no exceptions are allowed.

Expired Accounts/Cleaning Expired Accounts
Accounts will be expired upon creation or in the event of a password reset. Accounts expired for 90 or more days will be cleaned of access. Once cleaned, the user will need to submit a new, complete SIS Account Request to regain access.
Banner User Responsibility

It is the responsibility of the user to keep their Banner User Account active and open. Users should successfully login to Banner at least every 90 days and notify SIS Security immediately if there are any login issues.

PROCEDURES

Expired Accounts

1. Upon creation or during password reset, Banner User Account is expired.
2. Upon login, user will be notified that password is expired and prompted to create a new password.
3. Once new password is entered, Account is considered Open.
4. Accounts left Expired for any reason for 90 or more days are cleaned of all access, including new accounts.
5. Once an account is cleaned, the user must submit a new, complete SIS Account Request if he or she wishes to regain access.

Locked Accounts

1. Accounts can become Locked after too many incorrect password attempts (5), when the account is considered inactive, at the end of a temp hire period, or after the last day of employment within the department as defined by a Separation & Transfer notice.
2. Once Locked, the user will need to notify SIS Security to regain access. This could require a password reset, an email from the department, or a new SIS Account Request, depending on the reason for the lock.
3. Accounts locked for any reason for 90 or more days are cleaned of all access.
4. Once an account is cleaned, the user must submit a new, complete SIS Account Request if he or she wishes to regain access.
V. Audits

POLICIES

Regular audits are necessary to maintain appropriate access. SIS Security conducts many different types of audits including:

- Object audits to review users of a particular Banner object (also called screens and forms)
- Class audits to review both the users of a particular group of objects or the objects that have been assigned to the class
- Access audits to review the status of all Banner User Accounts
- Other audits, as needed

If a user whose access has been removed or modified as a result of an audit requests to be returned to their previous level of access, they will be directed to have their supervisor send an email to SISSecurity@UTSA.edu including the user’s name and Banner ID #, the request the user needs access to, modify or query, and a quick statement explaining why this access is needed. This email will then be forwarded to the Custodian who requested the user’s access be removed. It will be up to the Custodian and SIS Security to determine if access will be returned.

If a user’s account has been locked as result of an audit due to inactivity, the user will need to email SISSecurity@UTSA.edu to request their account be unlocked. If the account has already been cleaned of access, a new SIS Account Request will be necessary.

If the user’s account has been locked as a result of an audit finding an expired employment appointment, the user’s supervisor will need to send an email to SISSecurity@UTSA.edu verifying the user continues to work in the same position, in the same department. Banner Security may verify this information through HR before unlocking the account.

Banner User Responsibility

It is the responsibility of the user to keep their Banner User Account active and open. Users should successfully login to Banner at least every 90 days and notify SIS Security immediately if there are any login issues.
VI. General

a. FERPA

Federal Family Education Rights and Privacy Act (FERPA)

FERPA, The University of Texas System rules and regulations, and University rules and regulations govern the conduct of employees and School Officials with access to student records who act in the student’s educational interest within the limits of the employee’s or School Official’s need to know. To ensure compliance, the University requires that employees and School Officials be aware of federal law as well as System and University regulations that govern student records.

Banner User Accounts will not be released without the completion of the FERPA training and completion of the acknowledgment page affirming that they are aware of federal law as well as System and University regulations that govern student records.

Banner User Accounts will not be released nor will non-Banner requests be processed without the user’s successful completion of the Banner Users & FERPA Compliance Awareness Module (CT927) through MyTraining. The user must review the module, successfully complete the quiz within 2 attempts, and access their course certificate.

Violations in regulations regarding student records can result in loss of Banner User Account.

b. Training

Training, both classroom-based and online, is available to assist Banner Users and University staff with understanding and using Banner. Questions concerning course content can be directed to the posted contact(s) for the course(s). Questions concerning difficulties using or logging in to the MyTraining website can be directed to HR Training & Development.

UTSA Human Resources
Training & Development
210.458.4658
trainingsupport@utsa.edu

Banner Users & FERPA Compliance Awareness Module (CT927)
The Banner Users & FERPA Compliance Awareness Module (CT927) is an online training module available to all UTSA staff through MyTraining and required before a Banner User Account can
be released. The module can be accessed at any time, from any computer with internet access, and is estimated at 30-45 minutes for completion. Users must have an active myUTSA ID (network account) in order to login to MyTraining.

The FERPA module consists of several referrals to existing information regarding FERPA from different sources, a 5 question quiz, a certificate, and a course evaluation. The certificate and evaluation are only accessible if the quiz is passed within two attempts with a grade of at least 80. Users who do not pass the quiz must contact Banner Security to begin any new attempts.

**NOTE:** SIS Security is notified once the certificate is accessed, not once the quiz is passed; therefore completion of the module for the purpose of releasing an account is based upon accessing the certificate.

**Banner General Navigation Training (CT923)**
The Banner General Navigation Training (CT923) is an online training course available to all UTSA staff through MyTraining. It can be accessed at any time, from any computer with internet access, and is estimated at 30 minutes to an hour for completion. Users must have an active myUTSA ID (network account) in order to login to MyTraining.

The Navigation Training consists of explanations, interactive demonstrations, and activities to increase the user’s familiarity with Banner. Some common Banner uses, such as searching for a person and querying are covered. There is no quiz; the course certificate can be accessed once the training has been reviewed in full. A course evaluation is available.

**Banner Registration Training (CT926)**
The Banner Registration Training (CT926) is a classroom-based training course available to all UTSA staff. Staff must register for the course through MyTraining. Users must have an active myUTSA ID (network account) in order to login to MyTraining.

The Registration Training reviews the steps to registering students in Banner and how to overcome common registration problems. It is recommended that participants complete Banner General Navigation Training (CT923) before taking this class.

**Other Training**
The following training is offered independently from SIS Security:

**Academic Class Schedule Preparation (CT724)**

**Banner Advisor Training** (through USSTS)

**Banner Faculty Workload Training** (through VPAFS)
c. Passwords

**Password Requirements**
Banner User Account passwords require:
- at least one letter (A, B, C, etc)
- at least one number (1, 2, 3, etc)
- one special character from *this list only*
  - ! (exclamation mark)
  - % (percent sign)
  - * (asterisk)
  - + (plus sign)
  - - (dash)
  - / (forward slash)
  - : (colon)
  - ? (question mark)
  - _ (underscore)

**Password Guidelines**
Current password policy requires:
- The Banner User Account will be locked after 5 unsuccessful password attempts. The user will need to contact SIS Security for assistance.
- Password Reset requests must be made in writing from the user’s official email address (@UTSA.edu).

d. Holds

**Hold Information**
Holds are issued to students for a number of reasons – they need to pay tuition, need to turn something in, need to verify some information, need to speak to an advisor, etc. Holds are only active during the date range provided. Holds that are future dated or have already passed the To are NOT active and no longer effect the student. “Expired” holds are often left on record as a history of the transaction.
Issuing/Modifying Holds

Holds are issued to students using SOAHOLD in Banner based on a Hold Type and an originator (Orig). The Banner User placing the hold must have both modify access to the SOAHOLD screen AND permission to grant the specific hold type/originator.

Staff can only modify holds with a hold type and originator they have been granted access to. Users requesting access to a hold should have their supervisor submit the request by email to SISSecurity@UTSA.edu. The request will then be forwarded to the hold owner for authorization.
The information in this manual is updated and maintained by

SIS SECURITY TEAM
JD Villanueva & Chris Villarreal

Enrollment Services
MS 2.02.04
210.458.7598
210.458.5068
SISSecurity@UTSA.edu