UTSA Student Information Systems Security
USER POLICIES & PROCEDURES

UTSA Student Information Systems Security

USER POLICIES & PROCEDURES

Banner User Accounts

Banner User Accounts vs. Banner ID

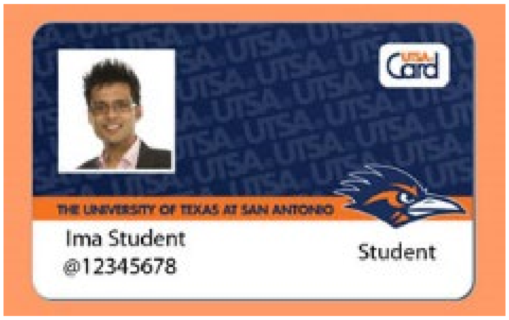
A Banner User Account is different from a Banner ID (Example: @01234567).

Banner IDs

UTSA Faculty and Staff are assigned Banner IDs upon employee appointment.
Prospective and Admitted Students are assigned a Banner ID upon receipt of an admission application, or admission-related requirements (test scores, high school/college transcript(s), etc.) and Financial Aid Applications.

Each UTSA constituent is assigned a unique Banner ID.
Banner IDs are used to link Banner User Accounts to a single-individual.

Banner IDs are commonly found on an individual's UTSA Card [as shown below]:



Banner User Accounts

Banner User Accounts are required to access Banner, UTSA's student information system, and requested through the Student Information Systems (SIS) Security Access Request Portal.
Only employees with an active employee appointment and active University credentials may initiate an access request.

Before initiating an Access Request, the employee must have the following University credentials:

- An active employee appointment with UTSA, and officially started employment.
- An active myUTSA ID (*Network ID*).
- A staff email address.

Requesting Access

Note: The Access Request Portal, and Banner, are only accessible from a UTSA-networked workstation, or via VPN if working remotely.

Requests for Access follow a six-stage process as articulated in-depth on our webpage, *Understanding the SIS Account Request Process*:
https://www.utsa.edu/enrollment/sissecurity/access/request-process.html

In short, the Access Request Process is as follows:

- **STAGE 1: Employee initiates the request by acknowledging our user agreement.**
- **STAGE 2: Supervisor requests access on the employee's behalf.**
- **STAGE 3: SIS Security routes the access request.**
- **STAGE 4: Data Custodian(s) review.**
- **STAGE 5: SIS Security processes the account(s) accordingly.**
- **STAGE 6: SIS Security notifies the employee.**

UTSA Student Information Systems Security
USER POLICIES & PROCEDURES

Types of Access Requests fulfilled via the SIS Access Request Portal:
https://sisaccessrequest.utsa.edu/

New Access Requests

New Access Requests are applicable when establishing new access.
This is most common for the following:

- New Employees.
- Department Transfers.
- Returning Employees.
- Student Employees.
- Temporary Employees.

Modify Access Requests

Modify Access Requests are applicable when the employee already has a Banner user account but requires access to additional Banner forms.
This is most common for the following:

- Employees with existing access that require one –or a few additional Banner Forms.
- Employees that require a limited scope of access.
- Supervisors establishing access for new employee positions.

Types of Access Requests not fulfilled via the SIS Access Request Portal

Memorandum of Understanding (MOUs)

To account for departments that require non-traditional, temporary-access for special projects to enhance established access for one –or more employees, SIS Security requires an MOU to identify the following:

- Who requires additional access?
- What additional access is requested?
- Why the additional access being requested?
- How long will the indicated employee(s) require such access, if approved?

MOUs are submitted to SIS Security by the supervisor or department head, and routed to the corresponding Data Custodian(s) for review. If approved, access is applied accordingly with an end-date of access on each respective Banner user account to prevent run-over of access.

Changes to pre-existing Banner Security Classes

Requested changes to pre-existing Banner Security Classes can be:

- Banner Forms to be added or removed.
- Users to be added or removed.

These requests are submitted to SIS Security by the supervisor or department head, and then will be routed to the corresponding Data Custodian(s) for review by SIS Security.

If approved by the Data Custodian, SIS Security will notify the requestor and Data Custodian once changes have been successfully applied.

New Banner Security Classes

- In an effort to create business-driven, customer-support access profiles a supervisor or department head may request that New Banner Security Classes be created.

An access summary and rationale for access must be presented to SIS Security for Data Custodian review.

If approved, SIS Security will create a new Banner Security Class(es), in the Pre-Production Database for testing by the requestor, followed by deployment into Production Database, which includes exchanging pre-existing access in affected user profiles for the new Banner Security Class(es) in affected user profiles.

Audits

SIS Security conducts audits including, but not limited to:

- Data Custodian requested audits:
    - Banner Form audits to review users with access privileges to a specific Form.
    - Banner Security Class audits to review both:
        - the users assigned to a Security Class
        - the Banner Forms assigned to the Security Class.

- Non-Data Custodian requested audits must be:
    - Submitted via the Banner Audit Request form: https://forms.office.com/r/6KTYFX3iRT
    - Approved by the designated Data Custodian.

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 employees' or school officials' 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.

Violations of regulations regarding student records may result in loss of Banner User Account privileges without notice.

FERPA Training

From January 1st, 2011 through March 1, 2020, Access Requests required completion of CT927: Banner Users and FERPA Compliance Module through https://mytraining.utsa.edu/online/

Effective March 2, 2020, employees are no longer required to complete the "CT 0927: SIS Security Account Request FERPA Compliance Module; in place of the Module", instead users will receive additional information in the User Agreement portion of the Access Request Portal.

Users must now complete the Institutional Compliance Module, as mandated by Institutional Compliance.

Banner Users & FERPA Compliance Awareness Module (CT927)
Although the *Banner Users & FERPA Compliance Awareness Module* (CT927) is no longer a requirement of the access request process, an online training module is available to all UTSA staff via https://mytraining.utsa.edu/online/ under "IT Software".

UTSA Student Information Systems Security

USER POLICIES & PROCEDURES

Banner Account Policies

Inactive Accounts

Accounts are inactive if there is no user activity for an extended duration.
Once a Banner user account is deemed inactive, the Banner user account is locked.

Users that encounter their account inaccessible or locked, must contact SIS Security to verify the locked status and seek remedy.
In some cases, locked users may be required to initiate a new access request via the SIS Access Request Portal: https://sisaccessrequest.utsa.edu/
NOTE: The SIS Access Request Portal is only accessible from a UTSA-networked workstation or via VPN if working remotely.

To prevent an account from being inactive, users should login to Banner on a regular basis.
Only successful logins to the Production Database are used to measure account activity.

Effective August 2021:
Users are notified via email when their accounts are at risk of being locked due to inactivity.
Users are provided a timely opportunity to show login activity to the Production Database; thereafter, if no action is taken by the user, the account is locked.

Locked Accounts

A Banner user account may be locked for the following:

- Incorrect Oracle password attempts.
- The end of a Temporary Employment period.
- Receipt of a separation or transfer notice.
- When inactive.

Purging Locked Accounts

Accounts that remain locked after an extended duration of time with no petition to unlock will be purged of all previously granted permissions.

Users that have had their Banner user accounts purged must initiate a new SIS Account Request to re-establish Banner access.

UTSA Student Information Systems Security
USER POLICIES & PROCEDURES

Oracle Password Guidelines

Front-end Banner 9 users will login using their myUTSA ID and Passphrase.

Banner users that access the Database by alternate means, such as TOAD or Crystal Reports must adhere to the Current Oracle password policy:

- The Oracle password will expire after 180 days
- The Banner User Account will lock after five unsuccessful Oracle password attempts.
  - Locked users must contact SIS Security for assistance.
  - Requests for Oracle password resets must be made from the user's UTSA employee email address (@UTSA.edu).

Oracle passwords must be at least 8 characters long and include the following characteristics:

- at least one letter (a, b, c, etc), not case-sensitive.
- at least one number (1, 2, 3, etc).
- at least one special character from the list below:

Acceptable Special Characters		
! (exclamation mark)	% (percent sign)	* (asterisk)
+ (plus sign)	- (dash)	/ (forward slash)
: (colon)	? (question mark)	_ (underscore)

Passphrase Standards

https://passphrase.utsa.edu/ResetHelp/

- There are NO RESTRICTIONS on the types of characters you can or cannot use.
- Your passphrase must contain a minimum of 15 characters.

Passphrase Requirements

https://passphrase.utsa.edu/ResetHelp/

- A minimum of 15 characters
- No common phrases
- No patterns of numbers and letters
- Not similar to your previous passphrase
- Not guessable by knowing you or reviewing information about you (such as on Facebook, Twitter, etc. or your birth date, name)