ALAMO COLLEGES

Information Technology Services

Banner (INB) User Access Process and Procedures

Type	Standards, Procedures and Guidelines
Approved/Revised Date	October 30, 2014
Target Audience	See Scope:
Effective Date	October 30, 2014
Current Version	1.6

Note:

- Information in this document is subject to change without notice; therefore, this document should be accessed online for currency.
- This document should not be transmitted or stored externally without consent from the District ITS Risk and Security Office.

Published by: The District ITS Risk and Security Office

Table of Contents

1.0 Overview

This document list standards and procedures, workflows and controls for gaining access to Internet Native Banner (INB) also known as Banner.

Alamo Colleges recognizes that inappropriate access increases the threat of inappropriate disclosure of data or unauthorized modification to data. In addition, the reliability and integrity of the Internet Native Banner (INB) System data may also be at risk.

Banner user's need access to screens (known as objects/forms) to be able to view and modify data based on their assigned duties. Depending on their job function, they may need "view only" and/or "update" access to these forms or objects. In Banner, "view only" equals "query" while "update" is known as "maintenance". Banner contains hundreds of forms/objects that can be granted directly to individual users however, the task of granting access using this method is inefficient and high risk. Therefore, Ellucian (formally Datatel and SunGard Higher Education services) added the Banner functionality for combining objects and forms into a unit called a "security class" or "role". This allows for a group of objects/forms to be placed into a unique security class or role. Security classes cannot include other security classes. By using this method, each user can be enrolled into an appropriate class or multiple classes based on "least privilege" in order to perform their job function.

1.1 Purpose

The purpose of this document is to identify the Account Management process for Banner provisioning and de-provisioning user access practices and to comply with the Texas Administration Code (TAC) security standards for higher education. TAC security standards require Institutions of Higher Education to preserve the confidentiality, integrity and availability of information resources.

1.2 Scope

This document applies to all Alamo Colleges users who intend to access and use the Banner System to perform their assigned job responsibilities.

1.3 Definitions

- **Banner User Account** – The Banner created user identification account to allow Banner system access.

- **Banner ID Number** – A Banner generated nine digit number beginning with the number 9nnnnnnnn assigned as a personal identifier to Alamo Colleges Faculty and Staff in Banner.

- **Banner System** – consists of data from Banner system modules such as Finance, Financial Aid, Human Resources, Student, and other interfaces to these systems. Includes but not limited to; associated databases, tables/views, files, directories, and forms.

- **Designated functional Point of Contact (POC)** – coordinates Banner System access with the data owners for their functional area(s).

- **Data Owners** – determine the level of data classification associated with the data within their functional area(s), as well as changes required by the organization. Data owners may include but not limited to Vice Chancellors, Vice Presidents, Directors and Managers, Supervisors or other designees).

- **Data Users** – Users who work with Banner data to perform their daily jobs supporting the mission of District and Colleges.

- **District ITS Risk and Security Office** – Performs but not limited to provisioning and de-provisioning of Banner user accounts and security classes. Provides a reasonable level of protection for Information Technology resources. Ensures that the Alamo Colleges internal controls, procedures and mechanisms are functional, adequate and in compliance with Alamo Colleges policies, Texas Administrative Codes, Federal, State and Local regulations, or best practices for higher Education.

- **Least Privilege** – Is the minimum level of capabilities to access data and functions necessary to perform a user's duties.

- **Senior Management** - May include but not limited to the Board, Chancellor, Vice Chancellors, Vice Presidents, Directors and Managers, Supervisors or other designees).

- **Third Parties** – Include Vendors, Consultants, Contractors, and Non-Employees.

1.4 Responsibilities

The Alamo Colleges District Information Technology Services (ITS) Risk and Security Office is responsible for coordination, development, approval, publication and dissemination of these Standards, Procedures and Guidelines.

The District ITS Risk and Security Office will:

- Grant or modify access to the Banner System based on documented approval and confirmation that any prerequisite training such as Banner Navigation Training or Self-Service Training has been completed. The designated functional Point of Contact (POC) should provide more detail training information if needed verify non-employee security agreement has been completed

- Remove user data access to the Banner System based on documented notification.

- Provide the designated functional POC's and data owner's routine Banner account reports for review and confirmation that access privileges assigned to data users reflect their assigned job function.

- Maintain appropriate documentation (access requests forms, separation reports, emails etc.) regarding new and existing user account changes such as (additions, modifications, and separations/transfers) to support internal and external Audits.

- Keep appropriate documentation based on regulatory, Alamo College's or best practice retention policies/standards.

Data Owners and Senior Management are required to:

- Ensure all employees comply with security policies, standards and procedures.
- Verify a non-employee security agreement is completed prior to requesting Banner access.
- Approve and sign appropriate Banner access request forms
- Perform periodic review of user account authorizations to Banner System data to ensure that their access is still appropriate.
- Notify the designated functional POC and District ITS Risk and Security Office of changes in the employee job responsibilities which require access changes, including separation and department transfers.

Designated functional Point of Contact's (POC) are required to:

- Evaluate all aspects from all access requests that fall within their capacity.
- Evaluate all aspects from all access requests that fall within their capacity.
- Work closely with data owners or designees to:
  - Design user access privileges
  - Ask relevant questions in order to minimize unnecessary access
  - Approve all user access within their scope.
- Perform periodic review of user authorizations to Banner system data and submit any changes to the District ITS Risk and Security Office.
- Notify the District ITS Risk and Security Office immediately when Banner system accounts are no longer required, or when access roles change.
- Retain appropriate documentation (access and deletion reports, Banner access request forms, emails etc.) regarding new and existing user account changes such as (additions, modifications, and separations/transfers).

Designated Functional POC's

See section 7.0 Contact Information.

Data Users are required to:

1. Keep any account authentication information in a secure place.
2. Not permit any other person to use the account for any purpose whatsoever.
3. Use all necessary precautions to safeguard confidentiality of the password.
4. Change the password when directed to comply with scheduled security reviews.
5. Notify their supervisor, local Helpdesk, District ITS Risk and Security Office if the password may have been compromised.
6. Direct individuals with a formal request for information, Subpoena or Court Order to the Alamo Colleges' Legal Services Office using appropriate disclosure channels.
7. Be accountable for use of their account.
8. Not use an access account and password belonging to someone else.
9. Not leave the Student Information System running on any computer while not in attendance. As such, users must lock their computers by ctrl-alt-delete
10. Keep their accounts active and open by successfully logging to Banner at least every 30 days.
11. Acknowledge that infrequent use or inactivity of an INB Banner Account for 30 days or more may be subject to account being disabled and locked based on conditional criteria.

12. Acknowledge that accounts will be disabled if employee no longer performs their authorized functional role (i.e. separates, transferred, acquires a new job function)

Third Parties are required to:

- Protect all Banner system data from unauthorized use, disclosure, modification, or destruction.
- Be responsible for the privacy and control of data within their capability or view.
- Create passwords according to established rules.
- Prohibit the sharing of Banner account ids and passwords to protect themselves from inadvertent disclosure to others.

1.5 Policies, Standards and Procedures

Additionally, users with access to Banner System data must adhere to provisions set forth in the following policies and procedures:

1. *C.1.9 (Board Policy) Appropriate Use of Information Technology Resources.*
2. *C.1.9.1 (Board Procedure) Appropriate Use of Information Technology Resources*

1.6 Banner System Modules

The current Banner System Modules at Alamo Colleges is as follows:

	Modules	Data Owners
1	Finance	Pamela Ansboury/Gertrud Moreno
2	Human Resources	Linda-Boyer Owens
3	Payroll	Pamela Ansboury/Gertrud Moreno
4	Student	Cynthia Mendiola-Perez
5	Student Accts Receivable	Pamela Ansboury/Susan Swan
6	Student Financial Aid	Harold Whitis

Each of the modules above has a designated functional (POC) who is responsible for coordinating access (**see 1.4 Responsibilities**)

1.7 Banner Security Classes

Banner Security Classes are units of objects/forms (screens) and are used to control access. They are grouped based on module and function. All security classes should be built at the lowest level and assigned to users based on their job functions.

Protocol for naming security classes start with “**ACCD**” for all Banner System Modules. The second node should contain the Banner Module name, for example “**ACCD_STUDENT_**”. It should be followed by a descriptive name.

“ACCD_ Gen_All” is a generic security class defined in Banner that contains the necessary forms and processes for a user to log in. The class will automatically be assigned to all new Banner User Accounts.

Ellucian delivers default security classes for each Banner module, however these classes are not allowed to be assigned to users. These security classes, if assigned to a user would give them maintenance to all screens in the module. This would defeat the purpose of having security controls. These classes are identified and begin with “**BAN**”.

1.8 Query vs. Maintenance

An object/form in a security class can be given maintenance (update) access or query (view) access. If a user, who is enrolled in multiple security classes, has both query (Q) and maintenance (M) access to the same form, the maintenance privilege will always take precedence over the query privilege.

1.9 Requesting Access to Enterprise (INB) Banner

NOTE:

➢ Banner INB accounts are not necessary for Banner Self Service (BSS) only

A. Summary

1. Initiated by or for an employee.
2. Sent to employee Supervisor for Approval
3. Validated for a completed CSA form.
4. Sent to District IT Risk/Security Office (Security@Alamo.Edu)
5. Routed by District IT Risk/Security Office to obtain Data Owner approvals
6. Returned to District IT Risk/Security Office (Security@Alamo.Edu)
7. Repeat (steps 4 & 5) until
   – Approval process is complete; or
   – Request is declined
8. Notification sent to security coordinators, supervisors and requestor by Security@Alamo.edu when a request is:
   – Processed based on approval or may be
   – Declined.
9. Retention of all documentation for auditing purposes.

B. Detail

❖ Users must complete a ““**Banner Access Request Form**” in full.

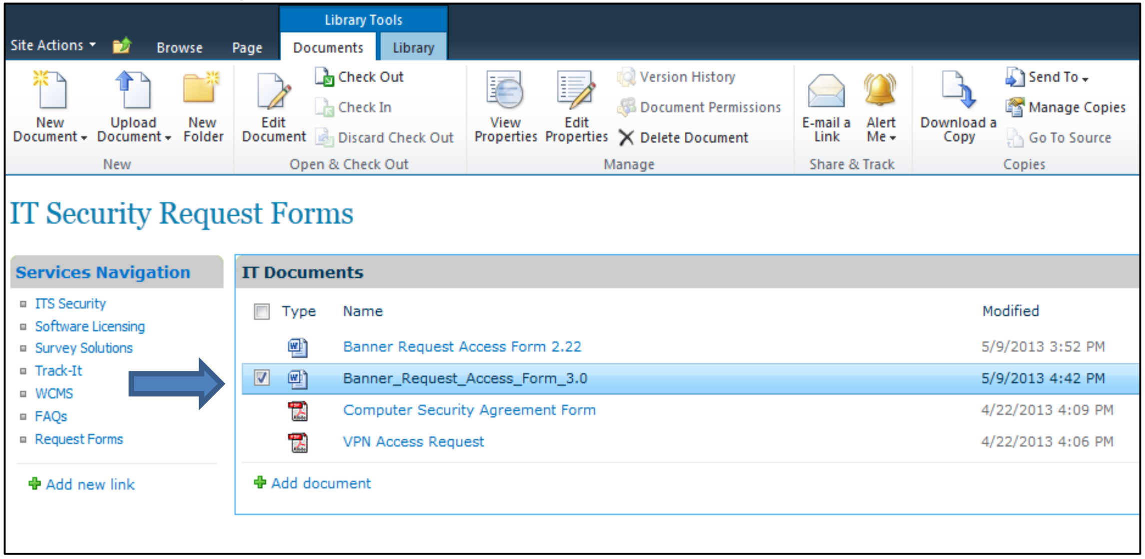
- Click on the link in **Step 1** below; follow the steps to download and save a copy of the current version of the "**Banner Access Request Form**" located in **Alamo Share.**

> **Note:**
> ***Please do not re-use the downloaded copy for future requests as this form may change without notice.***

Step 1: Banner Access Request Form - Click Here

Step 2: Hover over and place a check mark in the box next to the **"Banner Request Access Form**".

Screen shot example

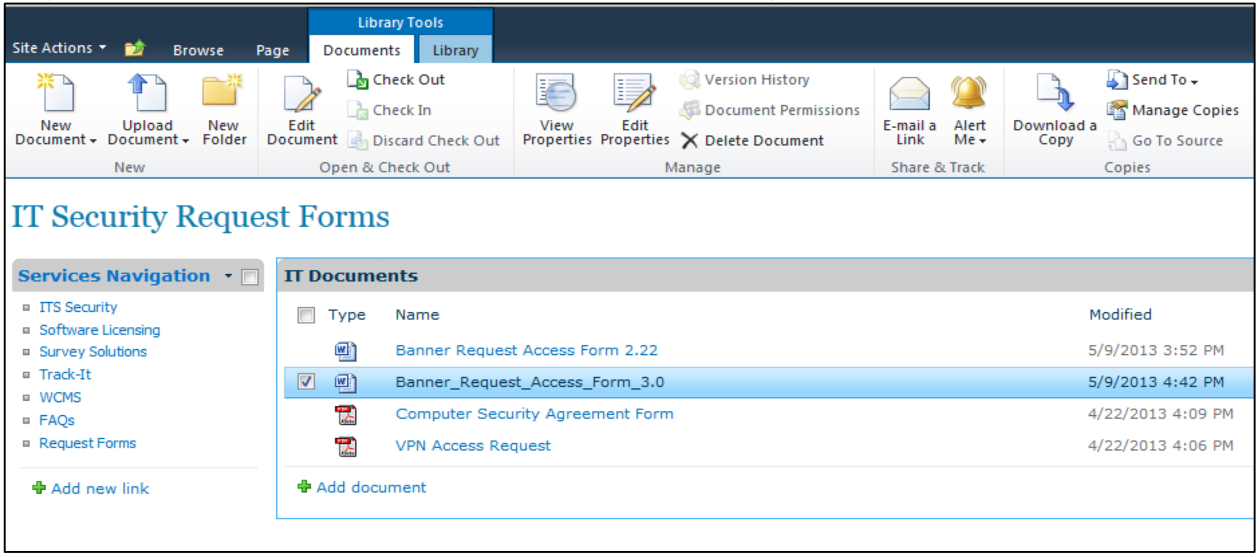


IT Security Request Forms

IT Documents

□ Type	Name	Modified
	Banner Request Access Form 2.22	5/9/2013 3:52 PM
☑	Banner_Request_Access_Form_3.0	5/9/2013 4:42 PM
	Computer Security Agreement Form	4/22/2013 4:09 PM
	VPN Access Request	4/22/2013 4:06 PM

Step 3: Click on the “Download a Copy” icon and save a copy



IT Security Request Forms

Services Navigation

- ITS Security
- Software Licensing
- Survey Solutions
- Track-It
- WCMS
- FAQs
- Request Forms

Add new link

IT Documents

□	Type	Name	Modified
	W	Banner Request Access Form 2.22	5/9/2013 3:52 PM
☑	W	Banner_Request_Access_Form_3.0	5/9/2013 4:42 PM
	PDF	Computer Security Agreement Form	4/22/2013 4:09 PM
	PDF	VPN Access Request	4/22/2013 4:06 PM

Add document

Step 4: Open your downloaded copy of the “**Banner Access Request Form**”.

Form Layout:

This form is composed of four sections:

- Section I - User Identification
- Section II - Banner Access Rights / Role Assignments (Authorizations)
- Section III - Supervisor and Functional Level Approval(s)
- Section IV - Comments or Concerns – Used for Data Owner reference only

B1. User Identification - Section I

1. Click on the “**Required Field**” next to “**Select Action**” to select the appropriate response:
   a. “**Add New Account**”,
   b. “**Change Existing Account**”
   c. “**Remove All Authorizations**”.

Note:
***A Banner User Account is considered new if the user has never been issued an account before or access has been removed, or the user has transferred to a new department**.*

2. Click on the date next to the “**Date required”** to invoke the calendar and select current date.
3. **Last Name:** [Enter Last Your Name]
4. **First Name:** [Enter First Name]

5. **Middle Initial**: [Optional]
6. **ACES/Email ID**: [Enter your ACES id if known; enter full email if unknown or "No ACES Id**"**].
7. **Banner Person ID**: [This is the 9 digit number assigned to you from the Banner System that begins with the number 9]
8. **Location:** [Click on the "**Required Field**" next to "**Location**" and select your location from the drop down values].
9. **Enter Department Name**: [Department Name]
10. **Position**: [Enter your position]
11. **Phone Number**: [Enter your phone number including area code]
12. **Employee Status**: [Click on the "**Required Field**" next to "**Employee Statu**s" and select from drop down box]
13. **Effective Date**: [Enter a start date]
14. **Access Termination Date**: [Click the field next to the "**Access Termination Date**" to invoke the calendar and enter the account expiration date]. **Mandatory for all temporary and Non-Alamo Colleges employees**.
15. **User Change Event Type**: [Select appropriate selection from drop down list]
16. **User Experience in Banner**: [Select the appropriate selection from the drop down list]
17. **Activate GOAEACC only:** [Check box to activate GOAEACC]. This field is for HR use only.
18. **Comments**: [Use this text box to enter additional facts that should be considered for example, covering during a vacation period, coverage of FMLA, additional responsibilities within the department, a security class not listed on form etc.]
19. Go to the appropriate functional area in **Section II.**

B2. Banner Access Rights / Role Assignments - Section II

Section two of the "**Banner Access Request Form**" is organized by the following functional areas:

- Student System Roles,
- CSI – Student System Roles
- CE – Student System Roles
- Financial Aid System Roles
- Student Accounts Receivable System Roles
- Human Resources System Roles
- Payroll System Roles
- Finance System Roles
- IT Roles

1. Complete the appropriate functional area with guidance and critical review from supervisory staff and data ownership.
2. Ensure that all business segregation of duties is observed.
3. Click on the "**click here**" link to view descriptions of the roles for each functional area:
4. Select the appropriate box: "**G**" for Grant Access or "**R**" for Remove Access to a security class/role.
5. Save and email the completed FORM as a WORD attachment to your supervisor for approval.
6. Retain a copy for your records to verify what selections had been made. This will be necessary until the development and implementation of workflow process for Alamo Colleges.

B3. Supervisor and Functional Level Approvals - Section III

The supervisor approval section precedes each of the Functional Level Approvals (Data Owners) and is required.

> **Note:**
> ***Request to "Remove All Authorizations" require ONLY supervisor approval. This request should be forwarded to Secuity@Alamo.Edu for immediate processing.***

Supervisor Approval:
Provides a contact point for all questions and will prevent unnecessary delays in processing the request. Details on completing the supervisor section are as follows:

- ❖ Upon receipt of "**Banner Access Request Form"** request via email; open the attachment and complete the following fields:
  1) **Supervisor Last Name**: [Enter supervisor Last Name]
  2) **Supervisor First Name**: [Enter supervisor First Name]
  3) **Supervisor Person ID**: [Enter supervisor's 9 digit Banner person number.]
  4) **Department:** [Enter the Department Name]
  5) **Title / Position**: [Enter supervisor's Title /Position information]
  6) **Email**: [Enter the first part of the Alamo email]
     a. (For example, **aperson**@alamo.edu enter "**aperson**" only)
  7) **Telephone**: [Enter Telephone Number]
  8) **Signature**: [Type Your Name]
  9) Forward the completed Form to the appropriate Data Owner(s) for approval based on the selections made in **Section – II** for each functional area.

Data Owner Approvals:
Provides a contact point for all questions and will prevent unnecessary delays in processing the request. Details on completing the Data Owner section are as follows:

- Upon receipt of "**Banner Access Request Form"** request via email; open the attachment and complete the following fields:
  1) Verify that the **User Identification - Section 1** has properly been completed.
  2) Review any comments entered in Comments Text Box.
  3) Move to the appropriate functional section for your area (i.e., Student, Finance, Payroll, etc.)
  4) Review the access requested for this user and validate appropriateness based on the **User Identification - Section I** completed information**.**
  5) Verify that Supervisor Approval is present, if not return to requester
  6) Move to the appropriate Signature line of the approvals section and enter your name.
  7) Move to the Email line and enter your email address
  8) Enter and comments or concerns - this will be for your reference only
  9) Save the FORM as a WORD document and attach to a new email and forward to Secuity@Alamo.Edu for appropriate routing.

Data Owner Approvals (continued):

- Steps to Reject the Request
  1) Enter the reason for rejection in the **Comments or Concerns – Section IV**
  2) Save the FORM as a Word Document
  3) Forward to Security@alamo.edu for appropriate routing.

Note:

An email from the appropriate data owner approver(s) may be accepted in conjunction with a request.

2.0 Banner Account De-Provisioning – Remove Account Access

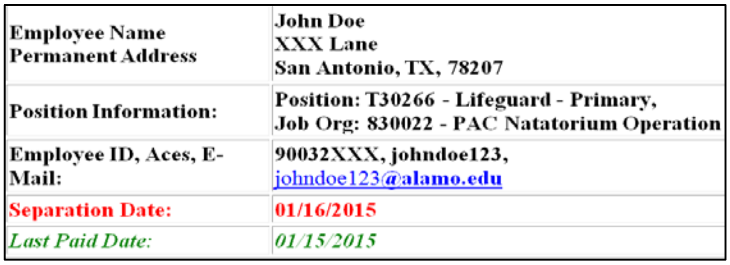
In 2009, an email process was institutionalized to alert all systems and physical security administrators of employee and non-employee separations. This process was revised in 2014, to include a Human Resources (HR) Employee Personnel Action Form (EPAF) Banner Work-Flow process. It is the responsibility of HR to notify the District ITS Risk and Security Office of separated employees on a timely basis including new hires and transfers. Upon notification, the District ITS Risk and Security Office will notify all District and College ITS administrators via a separated user email.

Functional departments who hire personnel like temporaries, consultants, and/or other non-employees not processed through HR must still notify the District ITS Risk and Security Office when a separation or transfer occurs. The designated communication method for non-employee separations not processed through HR is by email to Security@Alamo.Edu. Non-compliance to timely notify the District ITS Risk and Security Office increases the risk of unauthorized access to Alamo Colleges' resources.

2.0.1 Account Access Removal Process

1. HR's EPAF Banner Work-Flow initiates an employee change of status email to Secuity@Alamo.Edu.

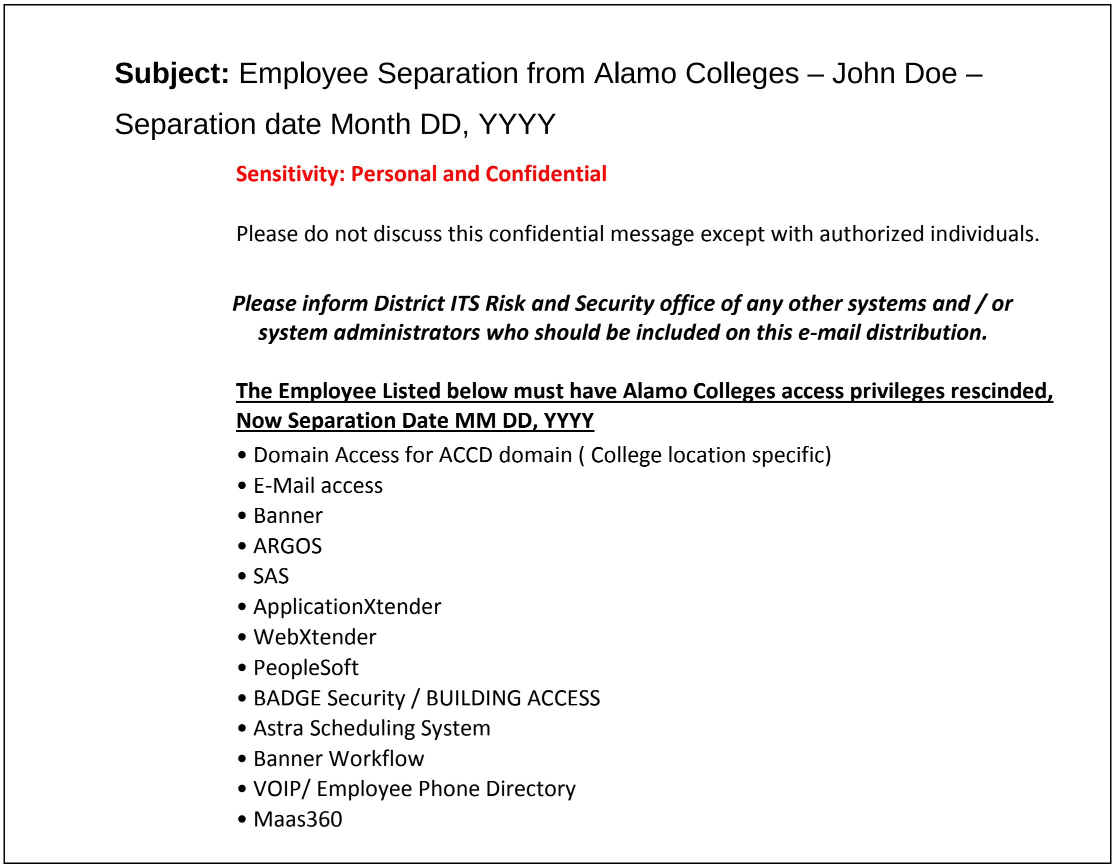
Sample EPAF Notification



Employee Name **Permanent Address**	**John Doe** **XXX Lane** **San Antonio, TX, 78207**
Position Information:	**Position: T30266 - Lifeguard - Primary,** **Job Org: 830022 - PAC Natatorium Operation**
Employee ID, Aces, E-Mail:	**90032XXX, johndoe123,** **johndoe123@alamo.edu**
Separation Date:	**01/16/2015**
Last Paid Date:	***01/15/2015***

2. District ITS Risk and Security Office will distribute to appropriate administrators via email a change of status notification.

Sample of email content



Subject: Employee Separation from Alamo Colleges – John Doe – Separation date Month DD, YYYY

Sensitivity: Personal and Confidential

Please do not discuss this confidential message except with authorized individuals.

Please inform District ITS Risk and Security office of any other systems and / or system administrators who should be included on this e-mail distribution.

The Employee Listed below must have Alamo Colleges access privileges rescinded, Now Separation Date MM DD, YYYY

- Domain Access for ACCD domain (College location specific)
- E-Mail access
- Banner
- ARGOS
- SAS
- ApplicationXtender
- WebXtender
- PeopleSoft
- BADGE Security / BUILDING ACCESS
- Astra Scheduling System
- Banner Workflow
- VOIP/ Employee Phone Directory
- Maas360

EMPLOYEE SEPARATION:
Employee Name: John Doe
Banner ID**: 900999999**
Email ID: jdoe
Effective Date: MM/DD/YYYY

3. ITS Risk and Security Lock in Banner.
4.
5. ITS Administrators will remove or disable all logical and physical access to Alamo College's resources.
   a) If an employee has transferred, that user's access privileges must be removed and a new set of access privileges must be assigned or enabled based upon the new job role of that user to prevent unauthorized access rights accumulation.
   b) Accounts that are locked due to separation will be cleaned of access and assigned the "**ACCD_DISABLED _USER_ACCOUNT**" security class which has no login or access privileges.

3.0 Audits

The District ITS Risk and Security Office will review on a monthly basis all Banner user and system accounts that have not been accessed for 30 days or more. If a user or systems account has not been active for 30 days or more the District ITS Risk and Security Office may Lock the Banner User or System account for inactivity and/or lack of legitimate business need unless irregular business use has been communicated and approved by the Data Owner and District ITS Risk and Security Office.

Banner Self-Service users who also have a Banner User Account and are active employees and do not log in to Banner INB will **NOT** be locked. This condition normally applies to Faculty and other irregular accounts such as Vice Chancellors and Presidents who may never login to Banner via INB. These accounts must remain unlock to prevent channel errors in Banner Self-Service.

4.0 Banner INB Account Statuses

To prevent a Banner User Account from being locked, users should successfully login at least every 30 days.

Locked Accounts

- An account will become locked after too many incorrect password attempts.
- An account will automatically become locked at the end of the expiration date of a temp, contractor, consultant or other non-employee when the "**Active To**" date is entered on the user's account. Although this will prevent a user from logging in, the status of the Banner Account will display as "**Open**" until manually locked.
- An account locked due to inactivity will be based on the current employee status in the Banner System

Inactive Accounts

- An account is considered inactive if there has not been a successful user login for 30 days, however the account may or may not be locked based on specific conditions (**see 3.0 Audits**).

Clean Accounts

- An account is considered cleaned when the account is “**Locked**” and assigned the “**ACCD_DISABLED _USER_ACCOUNT”** security class.

5.0 Banner INB Password Protection

Each individual is responsible for safeguarding his or her user id and password. A user should never “share” or “loan” their user id and password with anyone else. Each user should immediately reset their password after initial login, by using form **GUAPSWD.** Passwords must be alpha-numeric and a minimum length of eight (8) characters. Passwords will expire every 180 days and will be automatically locked 7 days after expiration.

Frequent Questions

- ***What characters can I use?***
  Alpha, Numeric and Special Characters minus the @ symbol.

  Acceptable Special Characters:

!	Exclamation Mark	**“**	Double Quote	**#**	Hash/Pound	**$**	Dollar Sign	**&**	And Symbol
(	Left Parenthesis	**+**	Plus sign	*****	Asterisk	**,**	Comma	**-**	Minus
)	Right Parenthesis	**/**	Slash	**=**	Equals sign	**:**	Colon	**;**	Semi Colon
>	Greater Than	**<**	Less Than	_	Underscore	**‘**	Single Quote	**?**	Question Mark

Note:
Use of @ symbol will result in a locked password the next time you try to logon and must not be used.

- ***How many unsuccessful password attempts before my Banner User Account gets locked?***
  *Unsuccessful Login Attempts is **5***

- ***What will happen if I exceed the number of password attempts?***
  You will be temporarily “lock/timed” for 5 minutes, after 5 minutes you may try to log in again.

  If after 5 minutes you are still locked, email Security@Alamo.Edu or contact your local helpdesk for assistance.

- ***What if I can’t wait 5 minutes and need to log in now?***
  Email Security@alamo.edu or contact your local helpdesk for assistance.

- ***Can I reuse my previous last 3 passwords?***
  No, only after 180 days have elapsed for each password

- ***I receive an ERROR* User not authorized to access GUAINIT..?***
  *Your account does not have the security class “**ACCD_GEN_ALL**”. Email Security@Alamo.edu*

- ***How do I Change My Password?***
  *By entering the form **GUAPSWD** on the **Go To….** field **Or** clicking on **Change Banner Password** on the General Menu form **(**GUAGMNU**)***

6.0 Non-Employee Banner Access Requests

Non-employees who need access to Banner INB are required to obtain a guest account.
To obtain a guest account, please follow the instructions from the link:
http://luminusdev.alamo.edu/eforms/ggerequest.aspx

7.0 Contact Information

Designated Functional POC's

Area	**Primary**	**Secondary**
Human Resources	Alicia Reyes	Allen Hime
Finance	Grace Villarreal	Mark E Martinez
Financial Aid	Dr. Harold Whitis	Michele Hill
Student Accounts	Jennifer Zamarrippa	Cynthia Mendolia-Perez
Student Accounts A/R	Susan Swan	

District ITS Risk and Security Office:

Email the District ITS Risk and Security Office to submit your questions and concerns or

Contact: Enterprise IT Risk/Security Manager (osalazar25@Alamo.Edu) at ext. 50403

8.0 Revision History

Version	Date	Description	Change History
1.4	02/01/2013	Initial release	
1.5	7/17/2014	Revised	Revised with new EPAF Banner-Workflow
1.6	10/30/2014	Revised	Revised format, reviewed and updated obsolete information