California University of Pennsylvania
Pennsylvania State System of Higher Education

Technology Procedure Number 2012-01
Banner Data Management Standard

Approved by:	**Banner Team Leads**
History:	**Issued – 8/2/2012**
	Revised
	Additional History – Version 13
Related Policies:	Acceptable Use Policy (AUP), UTech Security Incident Reporting and Response Policy, Data Classification Policy, University Records Retention Policy, Information Security Policy
Additional References:	

I. Introduction

This document affects all Administrators and anyone requesting access to the Banner System.

II. Purpose

The purpose of this document is to list rules and procedures for setting up and managing security within the Banner System at California University of Pennsylvania. It also outlines the responsibilities of all who access and manage the Banner-based data.

III. Standards

Those Affected by this Document

This document affects all Administrators and anyone requesting access to the Banner System.

Proper Use and Banner System Information Privacy

Access to Banner is granted only to those individuals who must access this information in

the normal course of their work responsibilities. A student worker, graduate assistant or affiliate may access this information only with permission from the Data Owner. No shared accounts are to be used. Access to administrative information will be granted to approved University employees only.

Users who are granted access to Banner are responsible for protecting their access privileges. Access and use must comply with University Acceptable Use Policies and Procedures.

Information in the Banner system is considered confidential and must be handled accordingly. Information obtained from the Banner system should never be shared outside the workplace or used for any purpose that is not related to the users assigned job responsibilities.

Job Function Roles

Banner security roles are established based on job function. When users need access to a form to do their job in Banner, the user will be assigned to a role class that has that form in it. Cal U will avoid assigning direct form access to a user. Users will be assigned a role or several roles depending on their particular needs as established by their Data Owner.

Job Changes

Banner access roles do not carry with a person from one position to another. When a person leaves a position for another, he/she will be granted only the access required for the new position. When a person enters a new position, the process for requesting access would be used to request a role change. The prior role assignment will be removed unless specified and justified within the access request.

Changes to employment, with accompanying role addition/removal requests should be reported by the employees Supervisor within two business days to the Helpdesk.

Data Owners

Data Owners, by virtue of their position at California University of Pennsylvania, have ultimate responsibility for the security, accuracy and confidentiality of data within their areas of accountability. An individual in each area of a specific application shall be designated as the Data Owner.

The responsibilities of this person are to:

- Ensure proper operating controls over the application to maintain a secure processing environment.
- Ensure accuracy and quality of data residing in the application.
- Approve all requests for access capability and update capability to the specific system and data.

- Ensure that system issues impacting the quality of data within the system are properly reported and adequately resolved.

The following table includes a list of applications, the data types within those applications, and the data owners assigned:

Application	Data Types	Data Owners
Admissions – Graduate	Prospects, Applicants, Admitted, Confirmed	Dean of Graduate Studies
Admissions – Undergraduate	Prospects, Applicants, Admitted, Confirmed	Dean of Admissions
Degree Audit	Student	Registrar
Financial Aid	Student Financial Aid Info	Director of Financial Aid
Student Accounts Receivable	Tuition, Student Fees	Bursar
Student Information	Demographic, Registration, Academic History, Catalog	Registrar
Student Housing	Housing Room Assignments	Housing Office Manager
Human Resources	Employee Information	Director of Human Resources

Employee

An employee is defined as any person that is employed by the University as their primary status within the University. This document also applies to temporary workers that may be hired while a permanent employee is on leave or for any other temporary purpose. A student worker or graduate assistant who is hired for work during the school year is not considered an employee, but is bound as an employee to comply with the University Acceptable Use Policy. Student workers and graduate assistants must not access the system without proper supervision and access must only occur during work hours. Companies may have contracts with the university and as a result have workers that need access to parts of the Banner system. The employees of these companies are also responsible for maintaining confidentiality and security as outlined in this document.

Data Protection

All Employees shall take reasonable steps to ensure a secure office environment in respect to data and any automated systems used to access data. Data Owners and Supervisors shall validate the level of access required for their respective staff, according to job functions, before access is provided.

Distributing Administrative Information

All Employees are responsible for determining what data from Banner is appropriate for distribution. It is their responsibility to ensure that information that is distributed adheres to any state or federal security requirements as well as relevant University Policies. Communications with external parties who are requesting California University data must be coordinated through Institutional Research.

Legal Accountability

By law, certain institutional data (e.g., personnel data) are confidential and may not be released without proper authorization. Employees or any person having access to automated administrative data must comply with any applicable federal and state laws concerning storage, retention, use release, and destruction of data.
Applicable Laws, Policies, and Regulations (including but not limited to):

AUP	(Acceptable Use Policy)
FERPA	(Family Educational Rights and Privacy Act)
Red Flags	(Identity Theft Protection)
HIPAA	(Health Insurance Portability and Accountability Act)

Maintaining Confidentiality of Restricted Data

It is the responsibility of the Data Owner to ensure that all individuals that have been granted access to their specific systems are aware of the confidential nature of the information they may access and the limitations for its disclosure.

When an individual is granted a user account, the individual is required to maintain the confidentiality of data within the specific systems without exception. Release of information outside the range of its distribution without the appropriate approvals and the approval of the Data Owner will not be tolerated. Unauthorized release of information will result in appropriate disciplinary action, including possible dismissal.

Reporting Data Security Breaches

It is every individual's responsibility to report possible data breaches. You are required to report such occurrences to the Compliance, Auditing, Risk, and Security (CARS) Team through the Helpdesk. Such reports will be held in strict confidence and promptly investigated. Data Owners are also responsible for reporting security breaches. Suspected security breaches are to be reported to the Help Desk.

A copy of the UTech Security Incident Reporting and Response Policy can be found here.

Requesting Access to Banner

Before requesting access to Banner, an individual should discuss with his or her Supervisor whether the need to access Banner is valid. If both the individual and supervisor agree Banner access is needed, then the following procedure must be followed.

Process for Request or Revocation of Access

1. All requests for changes in access must be made by supervisors, department heads, or directors. Requests should be submitted to the Data Owner through the Helpdesk for review two weeks prior to the date needed.
2. The Data Owner must review the request for access and grant or deny the request.
3. The Data Owner must submit approved requests to UTech Services through the Helpdesk System.
4. Approved requests then go to the Applications Team to assign the role. The Applications Team updates and closes the Footprints Ticket which sends a request to the individual notifying them that access has been granted or revoked.

   Note: No requests will be fulfilled without a Helpdesk Ticket.

IV. Definitions

- Employee - any person that is employed by the University as their primary status within the University.

- FERPA – The Family Educational Rights and Privacy Act (FERPA) is a federal law that protects the privacy of student educational records.

- HIPAA– The Health Insurance Portability and Accountability Act of 1996 protects health information - known as Protected Health Information (PHI) - that can be associated with a specific person.

- PCI (Payment Card Industry) - Security procedures from the PCI Security Standards Council for merchants that accept credit cards online.