Student Data Systems Guidelines for Access

Table of Contents

PURPOSE

To establish procedures and guidelines for accessing and using the University of California, Riverside Banner Student Information System and associated systems.

Ensure security, confidentiality, and appropriate use of all Banner data which is processes, stored, maintained, or transmitted on UCR or personal computer systems and networks. Includes protection from unauthorized modification, destruction, or disclosure, whether intentional or accidental.

SCOPE

These policies apply to all users (faculty, staff, student employees, and authorized affiliates) with access to any student data. This policy also applies to any system or database server that stores, uses, or accesses student data, computers that run programs using student data (including workstations and mobile devices to which data has been downloaded), and printed documents that display student data.

DEFINITIONS

Authorized Personnel: any person who has been determined to have a business or educational need to know and access student information in order to effectively perform job duties or assess academic and co-curricular programs.

Protected data[1]: The data comprising personal information governed by these guidelines is defined as protected data. This protected data includes an individual's first and last name in combination with any of the following:

- social security number AND/OR
- driver's license number AND/OR
- financial account or credit card number in combination with any password that would permit access to the individual's financial account

GOVERNANCE

Steering Committee

Provides oversight of the implementation initiative from the campus perspective.
Speaks for the university in areas of priorities, policy, and direction.
Ensures that decision affecting the implementation will be made in a rapid and efficient manner.

Banner Administrative Committee

Provides oversight of the overall project implementation, to include budgetary and fiscal concerns. Escalates issues to the Banner Steering Committee for review.

Project Management

Manages the implementation of all project-related activities, coordinates and communicates with the vendor and project committee chairs, while monitoring the successful completion of each phase to reach project milestones.

Implementation Working Group

Members are the Project Committee Chairs.
Responsible for establishing appropriate collaboration process and communication between Project Committees' work

efforts. Responsible for determining Project Committee project task responsibilities and assignments, resolving issues, and managing implementation plan and work progress.

Project Committees

Responsibility to ensure proper implementation of solutions within the designated timeframes and budgets. Ensure that the system being implemented supports UCR's processing requirements, while evaluating new processes in support of more efficient practices. Work with Ellucian consultants on timely completion of activities and tasks related to implementation.

Deployment Facilitation Work Groups

Communications - Responsible for overseeing communications effectiveness both within the project team, as well as, external to the team.

Training - Responsible to manage and coordinate Ellucian led training sessions and artifacts, as well as, to develop training material and coordinate training for campus users.

Change Management and Policy - Identify and execute those activities required for departments outside of the project team. Monitor Compliance with existing policies and recommend changes when required.

SECTION 1: GUIDELINES FOR STUDENT DATA SYSTEMS ACCESS

Determining who Needs Access to Student Data Systems

Security classifications ("Roles") have been established based on job function. The list of available roles can be found on the Banner Support site. Access will be granted to authorized personnel only. Security administrators (Application and Departmental SAA's) are responsible for ensuring users are only granted access to forms and data that are required to complete job responsibilities.

Student Employee Access

Student employees are only granted update access based on exceptional approval by the Director of Student Affairs Information Systems. Core Administrative offices (Registrar, Financial Aid, Undergraduate Admissions, Graduate Admissions, Student Business Services, and Summer Session) may have student employees with limited update access.

Third Party, Vendors, Affiliate Access

Access for a third-party, vendor, or other affiliate will be reviewed on a case-by-case basis.

Audit and Advisory Access

A role has been established for auditors and institutional researchers.

Systems and Technology Access

Access for non-core administrative department system and technology staff will be reviewed on a case-by-case basis. Typically, most non-core administrative department system and technology staff are more interested in receiving a data feed/API in order to facilitate the use of a custom developed application or third-party system. Information on how to obtain access to the Common File can be found by contacting the appropriate Technology Advisory Group (TAG) representative for your department or organization.

Denial of Access

Typically requests are denied for the following reasons:

1) Job functions do not align with the requested role
2) Information is available on another form / role
3) Information is available in a report format and access to a form would grant more access than is needed by the staff/faculty member
4) Information is available in Faculty/Advisor Self-Service

Denial notification will include an explanation of why access was denied.

Appeal Process

For student-related forms access, appeals should be sent to the Director of Student Affairs Information Systems. For accounts receivable-related forms access, appeals should be sent to the Director of Student Business Services. If you are not satisfied with your appeal or the appeal process, contact the UCR Banner Project Manager, who will refer the matter to the Banner Administrative Committee (BAC) for review. If you are not satisfied with the appeal decision made by BAC, the last (and final) decision will be made by the Banner Steering Committee based on a review of your job description, information from you and/or your manager, the type of access you are requesting, and the impact/risk to the University.

Removal of Access

Access to Banner (and associated systems) that use student data will be removed if an end user is found to be non-compliant with applicable federal, state, UC, and campus security policies.

SECTION 2: GUIDELINES FOR BANNER COGNOS REPORT ACCESS

Determining who needs access to Banner

Security classifications ("Roles") have been established based on department, function, and sensitivity of data. The list of available Banner Cognos roles can be found on the Banner Support site. Access will be granted to authorized personnel only. Security administrators (Application and Departmental SAA's) are responsible for ensuring users are only granted access to roles that are required to complete job responsibilities.

Denial and Appeal Process

The same process will be followed as described above for Student Data Systems access.

SECTION 3: ESTABLISHING AND MAINTAINING ACCESS TO STUDENT DATA SYSTEMS

BANNER, COGNOS, DEGREE WORKS, RECRUITER, WORKFLOW, BANNER DOCUMENT MANAGEMENT, CASHNET

ESTABLISHING FIRST TIME ACCESS – APPLICATION SAA AUTHORIZATIONS ONLY

Requests for new, first-time access begin by reviewing the Banner Support site for available roles and associated, required trainings. Requests are then submitted in ***Workfront – Banner Systems Access***.

MODIFICATION TO ACCESS

Requests to add a role follow same process as Establishing First-Time Access.

Removing a role: submit a request in ***Workfront - Banner Support Ticket***

If requesting to modify an existing role (a change that would impact ALL users assigned to that role) please submit an email to: sasytems@ucr.edu

REVIEW OF ACCESS

Access should be reviewed/cancelled when:

1. Faculty/staff are no longer employed by the University of California, Riverside
2. Faculty/staff have had significant changes in job responsibilities
3. Faculty/staff transfer departments

ANNUAL REMINDER/ACKNOWLEDGEMENT OF RESPONSIBLIITIES

Faculty and staff will be required to annually certify that they have taken and understand the FERPA training.

SECTION 5: BEST PRACTICES FOR SECURING STUDENT DATA

Password protect files that contain student data or share the information over a secure network (iShare).

Delete files that you do not need to maintain.

Ensure that your databases and systems have appropriate security measures in place.

Use discretion when sending data via e-mail.

Never include the SID/SSN in the subject line of an email.

Do not send student information to non-UCR e-mail addresses.

SECURITY GUIDELINES

UCR will utilize "masking" (hiding from view) any piece of data that must be protected from *most* users.

Establish roles (classes) that can be assigned to ANY Banner user by a departmental SAA. Only roles that have "view only" to ALL forms within the role should be in this group.

Application SAA would grant access to all other users utilizing EACS or native Banner security forms (depending on the situation).

Accounts Receivable forms: Student Business Services

Student or Financial Aid forms: Student Affairs Information Systems

SECTION 7: RESOURCES

Security Breaches Involving Personal Information: http://cnc.ucr.edu/securitybreaches/

UCR FERPA POLICY

Business and Finance Bulletins (available for reference in the Labor Relations Office):

RMP-7: Privacy of and Access to Information Responsibilities

RMP-9: Guidelines for Access to University Personnel Records by Government Agencies

Campus Policies and Procedures Manual: Policies

800-70: Privacy and Access to Information

400-35: Information Systems (Access, Use, & Security)

California and United States

- California Civil Code - Sections 1798.29 and 1798.82
- California Information Practices Act of 1977 (IPA)
- California Public Records Act (CPRA)
- Federal Family Educational Rights and Privacy Act of 1974 (FERPA)

University of California

- Electronic Communications Policy, August 2005
- Policies Applying to Campus Activities, Organizations, and Students, October 2009

UC Business and Finance Bulletins

- IS-3, Electronic Information Security
- IS-10, Systems Development and Maintenance Standards
- RMP-8, Legal Requirements on Privacy of and Access to Information

UCR Technical Security Notes

- Server Side Security and Firewalls
- Securing Protected Data