OFFICE OF THE REGISTRAR
COLORADO STATE UNIVERSITY

Departmental Banner Administrative Pages Access Request

Please complete the form,
Sign at the bottom of page 1 (Supervisor, Department Head) and page 2 (User)
Email to banner_security@mail.colostate.edu
OR Campus Delivery 1063, Office of the Registrar, Centennial Hall

Name: (Printed)
Phone:
NetID:
Department:
CSU ID:
Dept. #:
E-mail:

BANNER:

☐ Departmental Access
(Access to update departmental advising holds and overrides - Make sure department and dept. # above is correct)

SCAIT:

☐ SCAIT Data Entry FOR: ☐ Main Campus (M) ☐ Online (MC) ☐ Both

☐ Entire College
☐ Entire Department
☐ Subject Codes

Institutional Research Authorizing Signature

For SCAIT, YOU MUST list a college, a department/department #, or subject codes and departments:

(For **TWARBUS** access please go to http://busfin.colostate.edu/Depts/ALR.aspx, click on the 'TWARBUS Access Request Form' link and fill out the form online.)

OTHER REQUESTS:

Approval Signatures (Both MUST be filled out)

Supervisor Signature:
Date
Print Supervisor Name:
Dept. Head Signature:
Date
Print Dept. Head Name:

Banner Security Administrator
Date Implemented

ver 20250417

This agreement outlines the responsibilities and expectations for individuals granted access to Colorado State University's Student Information System (SIS) and related systems (e.g., faculty/staff portal, document imaging, degree audit). By accessing these systems, you acknowledge and agree to the following terms:

1. Confidentiality of Student Information
    - Student information is confidential and protected under the **Family Educational Rights and Privacy Act (FERPA).**
    - Access to student records is granted strictly for university business and to fulfill job responsibilities.
    - Any use of student data outside of official university purposes is strictly prohibited.
      Proper Use of Login Credentials
2. Proper Use of Login Credentials
    - Your NetID/username and password must never be shared with others.
    - You are personally responsible for all activity recorded under your login credentials.
    - Do not store or write down login details in visible or unsecured places (e.g., sticky notes, memos, or shared documentation).
3. Security Standards and System Use
    - You must follow all CSU and CSU System Information Technology security policies and acceptable use standards. **Acceptable Use Policy**, **Information Collection and Personal Records Privacy**, and Section I of **Information Technology Security**
    - Do not access or alter your own records, or those of family, friends, or student employees you supervise.
    - Do not store personally identifiable student data on removable media (e.g., laptops, USB drives, CDs) taken outside the office.
    - Always log out of, or lock, your computer when not in use to prevent unauthorized access.
4. Employment Status and Access
    - System access is granted based on your current role at the university. If your employment within the CSU System or within a department ends, your access will be revoked.
    - If you change departments and need continued access, you must reapply through the standard access request process.
5. Unauthorized Use
    - If you are unsure about the appropriate release or use of information, consult your supervisor or the Office of the Registrar.
    - If you become aware of unauthorized access or use, you must immediately notify your supervisor and the **SIS Security Team**.

By signing this agreement, you acknowledge your understanding of these responsibilities and agree to comply with all related policies. Violation of this agreement may result in revocation of access and/or disciplinary action in accordance with CSU personnel policies.

User's Signature:		
Print User's Name:		Date