RICE UNIVERSITY
Administrative and Enterprise Systems & Services Account Application and Security Agreement

Instructions: By completing this form you are requesting access to Rice University's administrative information systems. These systems include the SCT Banner Financial, Human Resources, Payroll, Student, and Financial Aid systems and custom extensions.

Applicants must complete Part 1, Part 2 (the User Agreement) and the appropriate pages that describe the access requested; i.e. Financial, HR/Payroll, Student, Financial Aid, Rice Web Applications, Campus Card, Parking, and SEVIS.

Return the completed and signed agreement to AESS USER SECURITY MS-97. The applicant will receive an email with instructions when the account is ready for use.

Part 1: Applicant Information   (Print Clearly)

Full Name _____ Rice ID# _____

Rice email address _____ Phone _____ Department _____

Posn Type: __Faculty __Staff __Temporary __Consultant __Student Worker   Job/Title: _____

☐ New Account (NETID _____)
       *** **Please note your netid must be issued before applying for your Banner account.** **

☐ Changes to Existing Account (USER ID:_____)

PART 2: Code of Responsibility for Security and Confidentiality of Records, Files and Databases

Security and confidentiality are matters of concern to all Rice University employees and other people who have access to administrative data including financial, human resources, payroll, and/or student records either by hard copy documents or via electronic or micrographic media. The purpose of this code is to clarify responsibilities for maintaining the confidentiality of information.

1. No one shall make or permit unauthorized use of any information in files maintained, stored, or processed by any Rice University administrative systems including Finance, Human Resources, Payroll, Student, Financial Aid, Rice Web Applications systems or any other administrative system.

2. No one is permitted to seek personal benefit, allow others to benefit personally or to divulge, in any way, knowledge of any confidential information which has come to them by virtue of their work assignment.

3. No one is to exhibit or divulge the contents of any record or report to any person except in the conduct of their work assignment and in accordance with Rice University and the Human Resources policies and procedures.

4. No one shall knowingly include, or cause to be included, in any record or report, a false, inaccurate, or misleading entry.

5. No one shall knowingly change or delete or cause to be changed or deleted an entry in any record of report, unless in accordance with Rice University and the AESS information policies and procedures.

6. No official record or report, or copy thereof, shall be removed from the office where it is maintained or copied or printed via electronic means except in the performance of a person's duties, and in accordance with established procedures. Copies made in the performance of a person's duties shall not be released to third parties except as Number 3 above applies.

7. No one is to aid, abet, or act in conspiracy with another to violate any part of these terms and conditions.

8. Any knowledge of a violation of these terms and conditions must immediately be reported to the AESS Security Administrator and the employee's supervisor.

9. Passwords shall be kept confidential. All precautions shall be taken to prevent its discovery. (e.g. Do not tape password to terminal, desktop or store in another non-secure place.)

10. Terminals and workstations shall not remain logged on to the system when unattended.

11. Violation of these terms and conditions may lead to reprimand, suspension, or dismissal from the position consistent with the policies governing faculty, staff and students of Rice University. Violation can also lead to action under the policy for student conduct, contractually established disciplinary procedures, and/or State of Texas statutes pertaining to theft, alteration of public record, or other applicable sections.

12. No one may disclose or reveal the contents of a student information system record or report to anyone except in the conduct of his or her job duties and in accordance with university policies and procedures.

13. No one will acknowledge to anyone who is not a University official the existence of any student who has placed a confidentiality restriction on his/her information.

14. No one will reveal, except within their job duties, that a student has placed a confidentiality restriction on his/her records.

Procedure for Rice University Student Information System Access

University procedures are consistent with applicable state and federal laws and regulations, including the Family Educational Rights Privacy Act of 1974. *Violations of this procedure may lead to appropriate disciplinary action.*

1. Data which is identifiable to particular individuals (e.g., names, social security numbers, addresses, telephone numbers), shall be used only within the scope of an individual's official responsibilities, e.g., instructors may access data for classes they teach, departments for their majors, etc.

2. Data analysis of units or groups within the institution, or within organizations external to the University, should be coordinated with the appropriate central administrative office (e.g., Office of the Registrar, Institutional Research).

3. Actual data is made available only via the information system to users with an authorized userid and password. Data that is saved locally must be adequately protected from outside access. Saved data must be updated frequently enough that the likelihood of incorrect data being used is minimized.

4. Anyone with information system access must ensure that such data is not available to individuals who have not signed a Student Information Systems Account Application and Security Agreement, or who do not have a legitimate "need to know". An individual with information system access is responsible for the security of his/her access and auditing that security on a regular basis, but not less frequently than on an annual basis.

5. Before publishing or releasing non-personally identifiable information derived from the student information system a person must coordinate such usage with the Director of Institutional Research.

6. Requests for data or the use thereof which are outside the user's responsibilities must be authorized in writing by the appropriate administrative office (e.g., Office of the Registrar, Institutional Research, Vice President for Enrollment).

7. Any use of information extending beyond a legitimate "need to know" basis must be authorized in advance by the Office of the Registrar.

8. Subpoenas for individual or aggregate student or employee information or any request from law enforcement authorities (including Campus Police, FBI, CIA, District Attorney) should be referred to the General Counsel's office.

User Affidavit

I have read, do understand, and will comply with the Rice University's Code of Responsibility for Security and Confidentiality of Records, Files, and Databases and the procedure for Rice University AESS Access.

I am aware of my responsibilities to protect the confidentiality of the student information and agree to use information from this system for work related purposes only.

I accept the responsibility for maintaining the confidentiality and security of my password, and the data that I access.

Applicant's Signature: _____ Date: _____

PART 3: APPROVALS

This request for access to the Rice University administrative system(s) identified below is approved.

Department Head: _____ Date: _____

PRINTED NAME: _____ Date: _____

System/Data	Requested (√)	Signature Required	Signature/Date	Access detail
Financial		Controller		Parts 4 & 5
HR/Payroll		Associate VP HR		Part 6

**Please Note - PI Security Information
With this security agreement, a PI will be set up with Banner access to his/her Research funds along with the following Web Applications.
- Buy/Pay Transactions & Purchasing Card History
- Budget Information, Financial Transactions Queries and Downloads
- Memo Reservation Detail
- Fund/Org Payroll Queries and Downloads (includes Payroll by FOAPAL, Job Labor Distribution, Salary Encumbrance detail with Budget Info and Financial Transactions)

** Please list below any fund(s) other than the PI's R funds they will need access to in Banner