SNOW COLLEGE DATA ACCESS FORM - FINANCE

Department: _____ Box # ☐☐☐☐ Date _____

Name: _____ Phone # ☐☐☐☐

Novell User Name: _____ Banner ID ☐☐☐☐☐☐☐☐☐
(Your Novell Username will also be your Banner username) (For Web access, may provide Banner Generated ID instead)

Type of Access Requested (Check all that apply)

☐ Requisitions Approved by: _____

☐ View Budget query forms (balance available, transaction details, etc.)

☐ Web Self Service (access to submit Requisitions, Approve Requisitions and Query Budgets)

FUND/ORG Security Access

☐ Copy same INDEX access as _____ [Go to Default ORG]
(Banner / Novell Username)

☐ List INDEXES that will provide access to all current finance data under your control:

INDEX	INDEX Description

INDEX	INDEX Description

Default ORG

ORG code to use as default for requisitions (Optional - INDEX that you use most often) ☐☐☐☐☐

Approval (must be signed by all responsible parties of ORGS/FUNDS listed or by someone higher in the organizational structure)

Printed Name	Signature	Date
_____	_____	_____
_____	_____	_____

Statement of Responsibility on back of form must be READ carefully and signed by employee.
Supervisors should review this statement with the employee, stress its importance, and then sign as witness.

Statement of Responsibility and Rules of Conduct

All SNOW employees and authorized system users are responsible for the security and confidentiality of institutional data, records, and reports. Individuals who have access to confidential data (see GRAMA officer for definition of confidential data) are responsible for maintaining the security and confidentiality of such data as condition of their employment. The unauthorized use of, or access to, confidential data is strictly prohibited and will subject the individual to disciplinary action up to and including termination and up to and including prosecution to the fullest extent permitted by law.

The system access rules of conduct and user responsibilities include, but are not limited to:

- System users shall not personally benefit or allow others to benefit by knowledge of any special information gained by virtue of their work assignments or system access privileges.
- System users shall not exhibit or divulge the contents of any record or report containing confidential data to any person, except in the execution of assigned duties and responsibilities.
- System users shall not knowingly include or cause to be included in any record or report a false, inaccurate, or misleading entry.
- System users shall not knowingly expunge or cause to be expunged any data entry from any record or report, except as is a normal part of their duties. Due caution will be exercised in the storage and disposal of documents and reports containing confidential data, including those stored electronically.
- System users shall not publish, or cause to be published, any reports, records, or other information without proper authorization.
- System users shall comply with information security procedures and rules of conduct as promulgated by the College.
- System users shall not share passwords with office workers or anyone else. Passwords that are written down, stored electronically or imbedded within automatic log in procedures must be physically secured, e.g., encrypted, password protected, or physically locked.
- System users are responsible for the proper use of their account, including not allowing others to use their account and insuring that while logged into the account only he/she has access to the account by using means such as password protected screen savers. The system footprints user activity and you will be held responsible for anything done under your login name.
- System users shall review finance data (budget, revenue, and expenditure transactions) under their control at least monthly.
- No person shall aid, abet, or act in concert with another to violate any part of these rules.

  Violation of these rules of conduct may subject an individual to loss of information access privileges, to reprimand, suspension, or dismissal in such manner as is consistent with College policies, and to prosecution under Federal and State computer and information security laws.

I have **READ** and fully **UNDERSTAND** the State of User Responsibility and Rules of Conduct printed on this form and shall comply with such statement and rules. I understand that violation of such may result in disciplinary action up to and including the termination of my employment and may also include prosecution under Federal and State law.

User signature _____Date_____

Witness signature _____Date_____