UNIVERSITY OF ALASKA FAIRBANKS

FINANCE Administrative Access Request (Banner/DSD/Vista Plus/eDir)

User Name (print): _____ (First Name) _____ (MI) _____ (Last Name)

Employee ID: _____ Email Address: _____

Banner Userid: _____ Dept.: _____

Phone: _____ Fax: _____ Supervisor's Name: _____

Request Type: ☐ New User ☐ Position Change ☐ Termination ☐ Other: _____

User Category: ☐ Faculty ☐ Staff – Regular ☐ Staff – Temporary ☐ Student Employee

BANNER ACCESS:

REQUIRED TRAINING – all Banner Finance users must complete a Banner navigation course (please check one):

☐ I completed Banner navigation with Statewide on _____ (date) with _____ (instructor)

☐ I completed the Blackboard Banner navigation course

☐ I have emailed slokelley@alaska.edu to schedule Banner navigation training

Please check the type(s) of Banner Finance access you require:

Banner TRNX (the Banner training module) is automatically granted to users requesting Banner Finance access.

☐ **Banner Finance Query:** I only need to lookup finance information for my department (i.e., lookup the status of finance transactions such as purchases, payments and budgets).

☐ **Banner Finance Entry for Purchasing (includes Banner Finance Query):** I need to enter purchases and receiving for my department using purchase requisitions, call numbers, limited purchase orders, etc.

REQUIRED TRAINING – in **addition** to the required navigation training, users requiring Banner Finance entry access for purchasing must complete Procurement training (please check one):

- ☐ I completed Procurement training on _____ (date)
- ☐ I have scheduled Banner Procurement training either through the Procurement office (474-6461) or through their website http://www.uaf.edu/procurement/links-for-staff-and-facul/procurement-training-in-b/

☐ **Banner Finance Entry for Travel (includes Banner Finance Query):** I need to enter travel documents (TA's and TER's) for my department.

☐ **Additional Banner Finance Access(es):** My job requires me to have specialized entry access as noted below. (Please be as specific as possible stating the specific forms required and/or the specific tasks to be performed.)

_____

_____

_____

WEB BASED ACCESS (please check all areas of access that you require)**:**

☐ ***eDir Employee & Department Update for the following Unit ID(s):*** _____

☐ **Vista Plus:** I need to view finance information, incomplete/open documents lists, budget status, and grant inception to date via the Vista Plus web queries.

☐ **DSD:** I need to monitor restricted funds/grants (project administration), view and/or create reports of budget information, encumbrance lists and property lists via the DSD web queries (QMenu/QAdhoc).

I have reviewed and approve all the marked areas of responsibility that the above user has indicated, which he or she needs in order to perform his or her job with our department.

_____ (Department Approval Signature) _____ (Printed Name) _____ (Date)

(you may *not* sign for your own access)

SUBMIT COMPLETED FORM TO: slokelley@alaska.edu or fax to 474-6468. QUESTIONS? Call 474-6424

UNIVERSITY OF ALASKA FAIRBANKS

FINANCE Administrative Access Request

To Be Completed By User:

Email Address: _____ Employee ID: _____

Banner Userid: _____ Dept.: _____

User Name (print): _____ _____ _____

First Name MI Last Name

Statement of User Responsibility and Rules of Conduct

All university employees and authorized systems users are responsible for the security and confidentiality of university data, records, and reports. Individuals who have access to confidential data are responsible for maintaining the security and confidentiality of such data as a 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 prosecution to the fullest extent permitted by law.

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

1. 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.
2. System users shall not exhibit or divulge the contents of any confidential record or report to any person, except in the execution of assigned duties and responsibilities.
3. System users shall not knowingly include or cause to be included in any record or report a false, inaccurate, or misleading entry.
4. Systems users shall not knowingly expunge or cause to be expunged a data entry from any record or report, except as is a normal part of their duties. Due caution will be exercised in the disposal of documents and reports containing sensitive information.
5. System users shall not publish or cause to be published any university reports, records or other information which contains confidential information for unauthorized distribution.
6. System users shall comply with information security procedures and rules of conduct as promulgated by the University.
7. System users shall not share passwords with office workers or with anyone else, have their passwords written down, stored, transmitted on computer systems, or imbedded within automatic log in procedures.
8. No person shall aid, abet, or act in concert with another to violate any part of these rules.

In addition to the above items, the users of SCT applications must comply with the conditions of the license agreement the university has with SCT. The agreement requires you and your organization to not sell, give away, or circulate part or all of the SCT system to anyone else. The SCT applications are the property of SCT and that must be treated as Confidential Information. Should you have any questions regarding the conditions for use of the system, please contact your campus information Security Coordinator.

Violation of these rules of conduct may subject an individual to a loss of information access privileges, to reprimand, suspension, or dismissal in such manner as is consistent with Regent's policies and university regulations, and to prosecution under federal and state computer and information security laws.

I have **READ** and fully **UNDERSTAND** the Statement of User Responsibility and Rules of Conduct printed on this form and shall comply with such statement and rules. **This includes access to personal ID and/or operator number.** 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: _____

Approval Coordinator: _____ Date: _____

Shannon O'Kelley

SUBMIT COMPLETED FORM TO: slokelley@alaska.edu or fax to 474-6468. QUESTIONS? Call 474-6424