UNIVERSITY OF ALASKA FAIRBANKS

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

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

Employee UA ID: _____ Email Address: _____

Banner Userid (if known): _____ 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 (please check all areas of access required to perform the duties of your position):

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 sent an email to uaf-ofa@alaska.edu requesting enrollment in the Blackboard Banner Navigation course.

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 emailed uaf-ofa@alaska.edu requesting enrollment in the Blackboard Banner Procurement training course.

☐ **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 to perform the duties of your position)**:**

☐ ***eDir Department & Employee Update (enter unit id(s) as shown in eDir):*** _____

☐ **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)

☐ **Toad:** I need to query information in RPTP

I have reviewed and approve all marked areas of responsibility which are needed to perform the job duties of this employee's position with our department.

_____ _____ _____
Department Approval Signature Printed Name Date
(you may ***not*** sign for your own access)

SUBMIT COMPLETED FORM AND DIRECT ANY QUESTIONS TO: uaf-ofa@alaska.edu

UNIVERSITY OF ALASKA FAIRBANKS

Administrative Access STATEMENT/RULES
(Unix, Oracle, Banner, & EDIR)

To Be Completed By User (Please PRINT):

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

Employee UA ID: _____ Email Address: _____

Banner Userid (if known): _____ Dept.: _____

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 as specified herein.

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

1. System users shall not personally benefit nor 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 access any confidential record or report, or disclose 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 nor cause to be included in any record or report a false, inaccurate, or misleading entry.
4. System users shall not knowingly expunge or cause to be expunged a data entry from any record or report, except as 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 nor cause to be published any University records, reports, or other information which contains confidential data 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 anyone nor transcribe them in any manner, such as, but not limited to: written, stored, transmitted on computer systems, or embedded within automatic login 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 Ellucian applications must comply with the conditions of the license agreement the University has established with Ellucian. The agreement requires you and your organization to not sell, give away, or circulate any part or all of the Ellucian system to anyone. Ellucian applications are the property of Ellucian and they 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 you to loss of information access privileges, reprimand, suspension, or dismissal in such manner as is consistent with Regents' 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.

User Signature: _____ Date: _____

Approval Coordinator: _____ Date: _____
UAF Security Administrator or Designee

SUBMIT COMPLETED FORM AND DIRECT ANY QUESTIONS TO: uaf-ofa@alaska.edu