UNIVERSITY OF ALASKA FAIRBANKS

# **HUMAN RESOURCES** Administrative Access Request (Banner/DSD/Vista Plus/PJP)

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

Employee ID: _____ Email Address: _____

Banner User ID (if available): _____ Dept.: _____

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

**Request Type:** ◯ New User ◯ Position Change ◯ Update

**User Category:** ◯ Faculty ◯ Staff – Regular ◯ Staff – Temporary ◯ Student Employee

**BANNER ACCESS:**

TRAINING FOR NEW USERS

New users may receive Banner navigation training through one-on-one training with an experienced user, in a classroom setting or online. For Banner HR navigation or Termination Workflow training call 474-7700 or email jjyoungberg@alaska.edu to make arrangements. For general Banner navigation and reports training, email lawrightsman@alaska.edu, or sign up at http://www.alaska.edu/oit/training/.

Please check the type(s) of Banner/DSD/Vista Plus HR access you require:

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

☐ **Banner HR Query:** I need to query miscellaneous employee information including employee time keeping locations (TKL), job class, job begin and end dates and pay rates. (HR_QUERY_GEN_CLS; USER_DSD_HRUSER_CLS; HRV_QUERY_GEN_UAF_CLS)

☐ **Banner HR Reports Print:** I need to print Banner job forms and/or timesheets. (HR_REPORTS_CLS)

☐ **Banner HR PPA Query:** I need to query employee job and payroll information including pay rates, labor distribution, gross and net pay and pay document type. (HR_PPA_CLS; HRV_PPA_UAF_CLS)

☐ **Banner Terminations Workflow for PPA (Training Required) :** I need to enter employee terminations (see below). (HR_TERMWF_CLS)

☐ I completed Terminations Workflow training on_____ (date) with _____(instructor)

☐ **Electronic Jobs Submissions for PPA:** I need to update existing jobs electronically. (HR_EPAF_CLS, HRV_EPAF_CLS)

☐ **Electronic Jobs Submissions for Approver/FYI:** I need to approve or review electronic jobs submissions.

My role is (check one):

◯ Fiscal Officer (HR_FISCAL_CLS*) ◯ Grants & Contracts (HR_GRANTS_CLS*)

◯ Fin Aid (HR_FINAID_CLS*) ◯ Budget Tech (HR_BUDGET_TECH_CLS*)

◯ Budget Approver (HR_BUDGET_APPR_CLS*)

*Includes VISTA – HRV_EPAF_CLS

**Additional Banner HR 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.)

**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 (you may *not* sign for your own access) | Printed Name | Date

**SUBMIT COMPLETED FORM by fax to 474-5859. QUESTIONS? Call 474-6407**

UNIVERSITY OF ALASKA FAIRBANKS

# **HUMAN RESOURCES** Administrative Access Request

**To Be Completed By User:**

User Name: _____ _____ _____
First Name MI Last Name

Employee ID: _____ Email Address: _____

Banner User ID: _____ 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 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: _____
HR Security Coordinator