UNIVERSITY OF ALASKA ADMINISTRATIVE ACCESS STATEMENT/RULES

(Administrative level access to UA information resources including Banner, OnBase, Unix, Oracle, EDIR)

To Be Completed By User: Please PRINT

Name: **First** _____ **MI** _____ **Last** _____

UA ID #: **(***e.g.,* 30123456**)** _____ **Contact Phone:** _____

UA Username: **(***e.g.,* fmlast1) _____ **UA Legacy ID:** **(***e.g.,* anxyz**)** _____

Statement of User Responsibility and Rules of Conduct

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.* Unauthorized use of, or access to, confidential data will subject you to disciplinary action. Please refer to University Policy and Regulations on information resources at https://www.alaska.edu/bor/policy/02-07.pdf.

Rules of conduct for administrative access to information resources and data include, but are not limited to these:

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 exhibit nor 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 nor cause to be included in any record or report a false, inaccurate, or misleading entry.
4. System users shall not knowingly expunge nor 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 imbedded within automatic login procedures.
8. No person shall aid, abet, or act in concert with another to violate any part of these rules.

Users must comply with the license terms and conditions of software licensed to the University of Alaska. You may not to sell, give away, or circulate any part of licensed software. If you have any questions regarding the licensing terms and conditions for use of software, please contact your campus information Security Coordinator.

Violation of these rules of conduct may lead to loss of access to information resources, disciplinary action as described in University Policy and Regulations (https://www.alaska.edu/bor/policy/02-07.pdf) and/or 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:** _____

PROCESSED BY: Security Administrator or Designee

Name: _____ **Date:** _____

UNIVERSITY OF ALASKA ADMINISTRATIVE ACCESS REQUEST

(Administrative level access to UA information resources including Banner, OnBase, Unix, Oracle, EDIR)

To Be Completed By User: Please PRINT

Name: **First** _____ **MI** _____ **First** _____

UA ID #: **(***e.g.,* 30123456**)** _____ **Contact Phone:** _____

UA Username: **(***e.g.,* fmlast1) _____ **UA Legacy ID:** **(***e.g.,* anxyz**)** _____

Request Type: **New User___** **Transfer___** **Termination___** **Access Change___**

Other_____

User Category: **Faculty___** **Staff___** **Student Employee___** **Contractor___**

Other_____

Department: _____ **Location:** _____

Details of Request

NOTE: I acknowledge my responsibility to conduct periodic reviews of employee access privileges and update those privileges in light of any job transfers, terminations or other changes.

Department Manager Signature below indicates agreement and approval

Signature/Title: _____ **Date:** _____

Printed Name: _____ **Tel #:** _____ **UA email:** _____

PROCESSED BY: Security Administrator or Designee

Name: _____ **Date:** _____