Oregon TECH

System Access Request

Complete this form with the help of your supervisor. Read and Sign last page before submission.

Name (print)_____ ☐ Faculty/Staff ☐ Student ☐ Other _____

OIT ID (918 xx xxxx)_____ Department _____

Job Title_____ Location/Mailstop _____

Campus Email_____ Campus Telephone _____

Indicate access requested and route to appropriate office(s) for signatures. Send completed form to ITS service desk. If completing this form through DocuSign, the routing will happen automatically.

FERPA Training is required before system access is granted. FERPA Completed?_____(Registrar Office initials)

Student System Access   **Route To** ⇨   _____ _____
- ☐ Banner Student (INB forms)   Registrars Approval   Date
- ☐ Web for Faculty (Banner SSB)
- ☐ FAST Student
- ☐ Etrieve Student
- ☐ Civitas - Inspire
- ☐ _____

Finance System Access   **Route To** ⇨   _____ _____
- ☐ Financial Edge (FENXT)   Business Affairs Approval   Date
  - ☐ Budget Authority
  - ☐ Web Purchasing
- ☐ FAST Finance
- ☐ Etrieve Finance
- ☐ _____

Human Resources System Access   **Route To** ⇨   _____ _____
(This access is rarely given outside of HR staff.)   Human Resources Approval   Date
- ☐ HR (Banner INB Forms)
- ☐ FAST Human Resources
- ☐ Etrieve HR
- ☐ _____

Admissions Systems Access   **Route To** ⇨   _____ _____
- ☐ Slate CRM   Admissions Approval   Date

Reason for needing access

- ☐ Current employee (not changing depts) needing additional access. Replicate: _____

  Reason for additional access: _____

- ☐ Employee is replacing previous employee - replicate their access_____

- ☐ Employee is in a newly created position within Oregon Tech.
  Employee's access should be set up similar to this employee: _____

- ☐ Employee moving to a different department on _____Revoke existing department access on _____

  Replicate this employee's access: _____

Financial Edge role(s) - check appropriate boxes below if you selected Financial Edge boxes on first page

Common roles:	**For BAO employees**:	**Unique roles**:
☐ * Office Manager	☐ Purchasing	☐ FENXT Administrator
☐ Credit Card Custodian	☐ Accounts Payable	☐ ITS Administrator
☐ Executive Assistant	☐ Accounts Receivable	☐ USSE Payroll
☐ Budget Authority	☐ Budget Office ☐ Journal Entry	☐ USSE Financial Reporting
☐ Budget Authority – Grant Only	☐ General Accounting	☐ USSE Treasury
☐ Other_____	☐ Grants Management	

 * Account strings for Office Managers: _____

Etrieve access – list details if any Etrieve boxes were checked on first page

   Content areas, workflows or other: _____

   [Common Areas: Athletics, BAO Accts Payable, BAO Procurement card, BAO Vendors, Students]

Edify Workspace(s)- if Edify box was checked on first page _____

Slate details - list role(s) if Slate box was checked on first page *(Admissions office may edit this information)*
   Role(s) or permission needed: _____

Additional access instructions:

_____

_____

Department Head – Supervisor - Sponsor Access Approval
Approved Signature:_____**Date:** _____
Print Name:_____**Title**: _____

Statement of User Responsibility:

Security and Confidentiality of Computer Records, Reports and Files

Security and confidentiality are matters of importance to all Oregon Tech employees. The purpose of this statement is to clarify your responsibilities in these areas pursuant to ORS 164.377. OIT's Banner Information System, which includes Student (SIS), Financial (FE), Human Resources (HRIS), associated data warehouses, and any extracted data containing confidential information. All users are expected to adhere to the security principles stated below.

As a person who has access to such information, **you will not**:
1. Share your password with anyone, or permit anyone to work in any program with your login.
2. Permit the unauthorized use of any information in data files maintained, stored, or processed in Banner or any data warehouse or any data extract or any other client application used to access OIT's administrative information systems.
3. Seek personal benefit, or allow others to benefit personally, from the knowledge of any information that you or they have acquired through work assignments.
4. Knowingly include or cause inclusion of false, inaccurate or misleading entry in any record or report.
5. Knowingly expunge or cause deletion of data entry from any record, report or file.
6. Remove or copy any official record, report or file from the office where it is maintained, except in the performance of your duties.
7. Aid, abet or act in conspiracy with another to violate any part of this code.

As a person who has access to such information, you will adhere to the following data use policies:
1. Data created for publication or for use in any public meeting must be authorized in writing by the appropriate office.
2. Data which is identifiable to particular individuals (e.g. inclusion of names, social security numbers, addresses, and telephone numbers) shall be used only within the scope of the individual's responsibilities, e.g., instructors may access data for classes which they teach.
3. Any release of any individual or aggregate student information to anyone outside of OIT employees who have legitimate educational "need to know" must be authorized by the Office of the Registrar with a written request stating the use of the data.
4. Anyone with warehouse access must ensure that such data is not available to individuals who do not have access to the same data via a normal Banner account, who have not signed a Request for Banner Access form, or who do not have a legitimate educational "need to know" for this data.
5. Data which is saved locally must be adequately protected from outside access. Saved data must be updated frequently enough such that the likelihood of incorrect data being used is minimized.
6. Requests for data or the use thereof which are outside the user's scope must be authorized in writing in advance by the Banner module owner.
7. Requests (or subpoenas) for individual or aggregate student information from law enforcement authorities (including campus security, OSP, FBI, CIA, District Attorney) or legislative officials should be referred to the University Registrar.

Employees or persons acting on behalf of Oregon Tech must immediately report any knowledge or violation of these principles to the violator's supervisor. Violations may lead to reprimand, suspension, or dismissal from the job, consistent with applicable personnel policies. Violations can also lead to action under the State of Oregon statutes pertaining to theft, alteration of public records, or other applicable sections.

Your signature below indicates that you have read, understand and will comply with the above policies.

_____   _____   _____

Printed Name   **Signature**   **Date**