System Access Request: Banner .. NOLIJ .. FAST

Complete this form with the help of your supervisor. Read and Sign page 2 before submission.

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

OIT ID (918 xxx xxx) _____ Department _____

Job Title _____ Location/Mailstop _____

Campus Email _____ Campus Telephone _____

Indicate access requested and route to appropriate Office

Banner: Internal Student, Finance, HR systems, includes Web for Faculty access. NOLIJ: Document Imaging/Electronic File system. FAST: System Reporting.

Student System Access

☐ Student (Banner INB Forms)
☐ Web for Faculty (Banner SSB)
☐ _____
☐ FAST Student
☐ NOLIJ

Route To ⇨ **Registrars Approval** **Date**

Finance System Access

☐ Finance (Banner INB Forms)
☐ Web for Finance (Banner SSB)
☐ Budget Authority Access
☐ _____
☐ NOLIJ
☐ FAST Finance
☐ Buyer Code

Route To ⇨ **Business Affairs Approval** **Date**

Human Resources System Access

☐ HR (Banner INB Forms)
☐ FAST Human Resources
☐ _____
☐ NOLIJ

Route To ⇨ **Human Resources Approval** **Date**

Admissions System Access

☐ Recruit CRM

Route To ⇨ **Admissions (SEM) Approval** **Date**

To be completed by Department Head/Supervisor

Reason for access:

_____

☐ Employee is in a new position within Oregon Tech.
☐ Employee is replacing/replicating an employee's access: (Employee's Name) _____

☐ Revoke existing access (applies when changing departments). Date of change: _____

Contract Code: ☐ AO ☐ NO ☐ AB Department: _____

Additional access/access instructions: _____

_____

Approved (Supervisor signature): _____ **Date:** _____

Print Name: _____ Title: _____

ITS Use Only: Request Completed On _____ By _____ Login UserID Created _____

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 (FIS), Human Resources (HRIS), associated data warehouses, and any extracted data containing confidential information. All Banner and warehouse 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 another person, or permit anyone to work in Banner or any data warehouse under 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 Development 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, departments for their majors, etc.
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**