



Document Imaging (IBPM) Access Request Form

User Information: (Please Print)

NOTE: Form will not be processed without proper signatures on page 2!

*Name: _____ *EWU ID _____
(Last, First, Middle Initial)

*Email _____ *Job Title: _____
NOTE: IF YOU DO NOT HAVE AN EWU EMAIL ADDRESS
PLEASE LIST SUPERVISOR'S EMAIL

*Department: _____ *Rm/Bldg.: _____ Phone: _____

*Indicate Type: Advisor _____ Student Services _____ Administrative _____

*Indicate Status: Fulltime _____ Part time _____ Student _____

*Supervisor: _____ Phone: _____

* You generally use a: PC _____ Mac _____

*Is this account replacing an existing account? _____ If yes, whose account? _____

Can that account be deactivated or does it need to be updated? _____

Briefly describe access needed or position duties:

I.E. LOOKING UP EVALUATIONS, REVIEWING FINANCIAL AID EXCEPTIONS, ETC.

Security Policy for Users with Document Imaging Access

All employees of Eastern Washington University (administrative, academic, staff and students) are required to abide by the policies governing review and release of student education records. The Family Educational Rights and Privacy Act (FERPA) of 1974 mandates that information contained in a student's education record must be kept confidential and outlines the procedures for review, release and access of such information.

Approval for access to the document imaging system (IBPM) will be granted to those individuals who have been determined to have a legitimate educational interest in the data by the Director of the functional area which oversees the student data being requested.

Individuals who have been granted access to any part of the document imaging data base must understand and accept the responsibility of working with confidential student records.

The following rules apply to all university employees with a Document Imaging account:

1. Each employee given access to the system will be assigned a Login ID and password. **Passwords are to be kept confidential and are not to be shared or given to anyone, including supervisors, co-workers, student employees, or friends. It is the responsibility of each employee to keep his/her password confidential and to change passwords whenever he/she feels someone else may have obtained access to it.**

2. **Employees shall use their own Login ID for all transactions.** If access to additional documents is needed, requests should be made through your departmental supervisor to the Director of the functional area. **Each employee given a Login ID is held responsible for any data input or retrieved using that Login ID. All transactions on the system can be traced back to the Login ID, which was utilized to access the data.**

A complete policy statement on the Eastern implementation of FERPA guidelines can be found in the Registrar's Office. In part, the policy states that officials of the University may be given access to student education records on a "need-to-know" basis and that such access must be **limited to job-related, legitimate educational interests.**

The information contained in a student's education record shall not be released to a third party without the written consent of the student.

Inappropriate use or misuse of student records is a violation of Eastern's statutes and could result in civil and/or criminal prosecution.

Examples of *inappropriate* use of student records are:

1. Accessing and/or updating a student's record without legitimate educational interest or for personal business.
2. Releasing confidential (non-directory) information to another student, university employee, parent, or anyone not having legitimate educational interest, without the student's written consent.
3. Leaving reports or computer screens containing confidential student information logged on or in view of others, who do not have legitimate educational interest in the data.
4. Giving your personal password to anyone for any reason.
5. Discussing the information contained in the student record outside of the University or while on the job with individuals who do not have a legitimate educational interest in the information (need-to-know).

Under no circumstances should an employee give confidential student information to any other student, employee, or persons who have not been authorized to receive such information by their departmental supervisor. Although directory information may be released without prior consent, any requests coming from anyone off campus should be referred to the Office of Records and Registration or the Associate Vice President for Enrollment Management.

** Students may request that directory information concerning them be restricted. Check Banner for student confidentiality requests prior to releasing any directory information.

I have read and clearly understand it is my responsibility to respect and maintain the confidentiality of all records and information to which I have been given access on the computer. I acknowledge the receipt of the security guidelines and further understand that the violation of these rules could result in disciplinary action, including suspension, termination and/or prosecution.

Required Signatures:

User: _____ Date: _____

Department Chair/Supervisor: _____ Date: _____

Send completed/signed forms to the Office of Records and Records, 201 Sutton, Cheney, WA 99004-2448 or fax to 359-6153. Phone 359-6586, 359-6544 or 359-6576 with questions.

For internal use only:

RR Security Mgr.: _____ Date: _____

Tech Security Mgr.: _____ Date: _____

Security type/notes: _____