EASTERN KENTUCKY UNIVERSITY
Banner Access Request Form

USER INFORMATION
Name: ___________________________________________ Title: ___________________________________________
Department: ___________________________________________________________________ Phone: ____________
EKU ID: _____________________________________________________________________________________________
Access Effective Date: _______________________ Access Expiration Date (to revoke access): ___________________
Are you a current user of the system? ___ Yes _____________________________ (List current login name)
___ No

Please mail this completed form to: Banner Security, Perkins 306, or FAX to 2-1738.
If you have questions, please contact the helpdesk at 2-3000 or email itdssecurity@eku.edu.

Describe the information / processes you need to access thru Banner.
_________________________________________________________________________________________________
_________________________________________________________________________________________________
_________________________________________________________________________________________________
_________________________________________________________________________________________________
_________________________________________________________________________________________________

______ Grant same Banner access as: ______________________________________________ (List user login name)

List existing Banner form(s) / processes that you wish to change: (Q) Query, (M) Modify, (R) Revoke access.
_________________________________________________________________________________________________
_________________________________________________________________________________________________
_________________________________________________________________________________________________
_________________________________________________________________________________________________

ORGANIZATION (Budget) Code(s):
__________________________________________ ________________________ ________________________
__________________________________________ ________________________ ________________________
__________________________________________ ________________________ ________________________

EMPLOYEE SIGNATURE _________________________________ DATE: __________________
SUPERVISOR SIGNATURE _______________________________ DATE: __________________
OTHER REQUIRED SIGNATURE ___________________________ DATE: __________________

* The employee requesting Banner access must read the back of this form and sign in the appropriate place

05/15/2003
Security, confidentiality, and respect for critical University services are matters of concern to the Eastern Kentucky University (EKU) community. Those who have access to university records either by hard copy documents or via electronic media should be particularly sensitive to safeguarding university electronic assets. Authorized users of EKU networks and computer systems include: (1) faculty, staff, and students of the University; (2) anyone connected from a public information service for the University; (3) others whose access furthers the mission of the University and whose usage does not interfere with other user's access to resources.

By virtue of your employment/association with Eastern Kentucky University, and your authorization for access to the Banner Database, your signature below certifies your full understanding, support, and agreement of the following:

As outlined in the current Eastern Kentucky University Undergraduate Catalog entitled “Provisions of the Family Educational Rights and Privacy Act of 1974 (as amended), Public Law 93-380”, intentional disclosure of records which contain individually identifiable information to any unauthorized person is prohibited.

Accessing, or attempting to access or view, any account for which there is no specific authorization is prohibited.

Attempts to circumvent data protection schemes or exploiting security loopholes which disrupt, delay, endanger or expose University operations are prohibited.

Responsibility for the security of an assigned password rests solely with the assignee. This includes changing passwords on a regular basis and making sure no one else knows them.

The use of EKU’s computing resources are not completely private. While individual usage is not routinely monitored, normal operation and maintenance require logging of activity, monitoring of general usage patterns, and other such activities for maintaining availability and performance. Authorized monitoring of activity and individual user accounts, including individual login sessions and communications, may occur without notice. Monitoring may occur in the following instances:
- The user has voluntarily made them accessible.
- It reasonably appears necessary to do so to protect the integrity, security, or functionality of the University or to protect the University from liability.
- There is reasonable cause to believe that the user has violated, or is violating, this policy.
- An account appears to be engaged in unusual or unusually excessive activity, as indicated by the monitoring of general activity and usage patterns.
- Upon receipt of a legally served directive of appropriate law enforcement agencies.

When an authorized user changes status (i.e. termination, graduation, retirement, or position / responsibility changes), the Budget Unit head responsible for initiating the status change must coordinate with the user to ensure that access authorization to all University resources is appropriate. An individual may not use facilities, accounts, access codes, privileges, or information for which he/she is not authorized.

I have read, do understand, and will comply with the above EKU Code of Responsibility for Security and Confidentiality of Records, Files, and Databases, EKU Code of Ethics for Computing & Communications located at [http://www.itds.eku.edu/codeofethics/](http://www.itds.eku.edu/codeofethics/), and EKU University Policy – Fiscal Misconduct located at [http://www.administrativeaffairs.eku.edu/docs/EKUFraudPolicy_Approved11-8-2002_.pdf](http://www.administrativeaffairs.eku.edu/docs/EKUFraudPolicy_Approved11-8-2002_.pdf). I am also aware that intentional misuse or fraud, or disclosure of EKU computing resources or data could constitute just cause for disciplinary action, up to and including termination of employment regardless of whether criminal and/or civil penalties are imposed. Additionally, criminal and civil penalties could be imposed as implied in federal U.S. Codes and Chapter 434 of Kentucky Revised Statutes.

Signature: ___________________________ Date: ________________

05/15/2003