

BANNER User Access Request Instructions

Below are the instructions for requesting Banner access. Failure to follow these instructions may lead to an incomplete request which will delay the processing. Incomplete requests will be sent back to the requesting supervisor. Completed requests are processed within 3-4 working days. If needed, Banner Navigation Training will be scheduled 2-3 days after request processing.

Initial Banner INB access requests require the following documents:

1.02.000_Banner Request Checklist
1.03.002_Banner Security User Maintenance Form
1.05.000_Information Security Agreement
1.06.000_Acknowledgement of the Request of Appropriate Banner Access
TrainTraq Transcript – FERPA and Information Security Awareness

1. The user's supervisor will request access through the use of the most current "Banner Security User Maintenance Form". The user's information must be complete and correct. This is the supervisor's responsibility.
2. Supervisor will then work with the appropriate Information Owners (see Banner Information Owners) to assess what classes the user will need access to fulfill their job duties. The appropriate Information Owners will sign off granting access on the "Banner Security User Maintenance Form".
3. A signed "Information Security Agreement" for the user and proof that the user has had "FERPA" and "Information Security Awareness" training must be provided. (Available through TrainTraq in HR Connect.) The agreement must be signed and training must be completed no more than 6 months prior to the date that the request is submitted.
4. Supervisor must complete the "Acknowledgement of the Request of Appropriate Banner Access" form.
5. To assist in ensuring that the request is complete, a "Banner Request Checklist" must be turned in.
6. Completed forms and all supporting required documentation must be routed to the Business Affairs Information Resources office (Gilchrist Rm. 122).
7. The user will be contacted for Banner Navigation Training 5 to 7 days after completed request is received and approved. User will be required to present a valid university ID at training to receive their login information.
8. If disapproved, the requesting supervisor and Information Owner will both be notified via email and phone.

Additional Banner INB access requests require the following documents:

1.02.000_Banner Request Checklist
1.03.002_Banner Security User Maintenance Form
1.06.000_Acknowledgement of the Request of Appropriate Banner Access

1. The user's supervisor will request access through the use of the most current "Banner Security User Maintenance Form". The user's information must be complete and correct. This is the supervisor's responsibility.
2. The supervisor will then work with the appropriate Information Owners (see Banner Information Owners) to assess what additional classes the user will need access to fulfill their job duties. The appropriate Information Owners will sign off granting access on the "Banner Security User Maintenance Form".
3. Supervisor must complete the "Acknowledgement of the Request of Appropriate Banner Access" form.
4. To assist in ensuring that the request is complete, a "Banner Request Checklist" must be turned in.
5. Supervisor must route the form and all supporting required documentation to the Business Affairs Information Resources office (Gilchrist Rm. 122).
6. Request will be processed within 4 working days of receipt.
7. If approved, after processing the request the requesting supervisor and Information Owner will both be notified via email and phone.
8. If disapproved, the requesting supervisor and Information Owner will both be notified via email and phone.

Initial Panthertracks "Advisor" access requests require the following documents:

- 1.02.000_Banner Request Checklist
- 1.03.002_Banner Security User Maintenance Form
- 1.04.000_Banner Panthertracks Initial Access User Information Form (For non-faculty ONLY)
- 1.05.000_Information Security Agreement
- 1.06.000_Acknowledgement of the Request of Appropriate Banner Access
- TrainTraQ Transcript – FERPA and Information Security Awareness

1. The user's supervisor will request "Advisor" access through the use of the most current "Banner Security User Maintenance Form". (Advisor access is not initially given to faculty members upon their employment at the university.) The user's information must be complete and correct. This is the supervisor's responsibility.
2. The supervisor will then work with the appropriate Information Owner, the Registrar, to assess if "Advisor" access is needed. The Registrar, will sign off granting access on the "Banner Security User Maintenance Form".
3. A signed "Information Security Agreement" for the user and proof that the user has had "FERPA" and "Information Security Awareness" training must be provided. (Available through TrainTraQ in HR Connect.) The agreement must be signed and training must be completed no more than 6 months prior to the date that the request is submitted.
4. Supervisor must complete the "Acknowledgement of the Request of Appropriate Banner Access" form.
5. To assist in ensuring that the request is complete, a "Banner Request Checklist" must be turned in.
6. Supervisor must route the form and all supporting required documentation to the Business Affairs Information Resources office (Gilchrist Rm. 122).

7. The form will be processed within 3-7 working days of receipt.
8. If approved and the user is a current faculty member, access will be granted immediately and the supervisor will be notified. (Note: A faculty member person record is created in Banner by Institutional Research when the individual's contract and "Faculty Database Form" is received. Therefore, the "Banner Panthertracks Initial Access User Information Form" is not required.)
9. If approved and the user is a non-teaching staff, the supervisor will be asked to turn in a "Banner Panthertracks Initial Access User Information Form". Upon receipt of the completed form the user will be contacted for Panthertracks Navigation Training 3-7 working days after approval. User will be required to present a valid university ID at training to receive their login information.
10. If disapproved, the requesting supervisor and Information Owner will both be notified via email and phone.