AUGUSTA UNIVERSITY SYSTEM ACCESS REQUEST FORM

Part 1, 2, and 3 must be completed by the Requestor. Part 4 will be completed by the Data Stewards. Insufficient information listed in Part 3 will result in the return of your request. Please be as specific as possible. Upon completion return to banneraccess@augusta.edu for processing.

PART 1: SYSTEM ACCESS REQUEST

The Augusta University Information Systems Security and Computer Usage Policy ensures that information systems resources are allocated in an appropriate and responsible manner consistent with the mission of the Augusta University institution, and that the use of these resources is in accordance with Augusta University policies, procedures, federal and state law. This policy applies to the Banner System and all information systems resources that are controlled, administered or accessed by Augusta University students, faculty, employees, visitors or any other person accessing from on-campus as well as off-campus. The appropriate use and protection of all information systems and associated resources is expected from all users including faculty, students, employees, and visitors throughout the institution. "Appropriate use" of information systems resources is defined as use which is for the purpose of furthering the mission of Augusta University.

Data Sharing & Confidentiality Agreement

Augusta University holds data privacy, confidentiality, and security practices in the highest regard. Institutional data is protected as defined by the Family Educational Rights and Privacy Act (FERPA) and The Health Insurance Portability and Accountability Act (HIPAA). The Family Educational Rights and Privacy Act (FERPA) of 1974 is a federal law that requires colleges and universities to protect the confidentiality of student education records. The law states that, except in specified circumstances, no one outside the institution shall have access to a student's education records, nor will the institution disclose any information from those records without the written consent of the student. Banner users have a legal responsibility to protect the confidentiality of student education records provisioned by the Data Stewards. Banner users are only provisioned access to student information for legitimate use in the completion of assigned responsibilities as a university employee.

This document outlines the manner in which to utilize institutional data and protect personally identifiable information. A signed agreement form is required from all Augusta University staff to verify agreement to adhere to/abide by these practices. The failure to adhere to guidelines may result in personnel action, up to and including termination. Please review each guideline below and sign Part 1 to acknowledge that you will adhere to each.

As an employee of Augusta University, I hereby affirm that:

- I have read the Data Sharing and Confidentiality Agreement.
- I have completed/will complete Human Resources Annual Compliance Training.
- I will use a password-protected computer when accessing data and reporting systems, viewing institutional records, and downloading reports.
- I will not share or exchange individual passwords, for either personal computer(s) or system user accounts.
- I will log out of and close the browser after each use of Augusta University data and reporting systems.
- I will only access data in which I have received explicit written permissions from the data owner.
- I will keep sensitive data on password-protected state-authorized computers.
- I will keep any printed files containing personally identifiable information in a locked location while unattended.
- I will not share student/workforce/patient-identifying data during public presentations, webinars, etc. I understand that dummy records should be used for such presentations.
- I will delete files containing sensitive data after working with them from my desktop, or move them to a secured server.
- I will publish only aggregate data in groups no smaller than five in reports and only for valid purposes.
- I will take steps to avoid disclosure of personally identifiable information in reports, such as aggregating, data suppression, rounding, recoding, etc.
- I will not use email to send screenshots, text, or attachments that contain personally identifiable or other sensitive information. If I receive an email containing such information, I will delete the screenshots/text when forwarding or replying to these messages.
- I will not transmit student/workforce/patient-level data externally unless explicitly authorized in writing by the Data owner and Institutional
- I understand that when sharing student/workforce/patient -identifying data with authorized individuals, the only approved methods are Secure File Transfer Protocol (SFTP). Also, sharing within secured server folders is appropriate for Augusta University internal file transfer.
- I will immediately report any data breaches, suspected data breaches, or any other suspicious activity related to data access to my supervisor and the AU Information Security Officer. Moreover, I acknowledge my role as a public servant and steward of student/workforce/patient information, and affirm that I will handle personal information with care to prevent disclosure.
- I understand that failure to report violation of confidentiality by others is just as serious as my own violation and may subject me to personnel action.
- I agree that upon the cessation of my employment from Augusta University, I will not disclose or otherwise disseminate any confidential or personally identifiable information to anyone.

By signing this document, I acknowledge that I have read the information outlined in Part 1: System Access Request and agree to abide by the procedures set forth in this document. I acknowledge I am only requesting the access needed for my current job duties. As the supervisor, I acknowledge that I have reviewed and approve the requested access.

Requestor:	_____ Print Name	_____ Signature	_____ Date
Supervisor:	_____ Print Name	_____ Signature	_____ Date

AUGUSTA UNIVERSITY

SYSTEM ACCESS REQUEST FORM

PART 2: PERSONAL INFORMATION

Name:	**User ID:**
Title:	**Department:**
Phone:	**Email:**
Supervisor:	**Supervisor Email:**

Status: ☐ New User ☐ User Modification

PART 3: ACCESS INFORMATION

Please initial next to each statement below to verify completion of each audit requirement.

☐ Banner ☐ Crystal Reports ☐ JagTrax ☐ Document Manager (Xtender) ☐ CIR
☐ Scheduling Coordinator ☐ Navigate

Banner: List the specific objects you require to complete current job duties and a corresponding justification. If you do not know which objects are required, provide a detailed list of job duties that require Banner.

Banner Object	Justification/Job Duty

Crystal Reports: List the specific reports you require to complete current job duties and a corresponding justification. If you do not know which reports are required, provide a detailed list of job duties that require Crystal.

Report Number	Justification/Job Duty

JagTrax: Complete the chart below to specify the student population you will need access to view in JagTrax.

College	Degree	Major	Minor	Concentration	Alphabet	Earned Hours

Document Manager (Xtender): ☐ Admissions Records

CIR: List the department(s) you need access to for CIR processing.

UCRN Process: List the prefixes you will be responsible for updating.

PART 4: DATA STEWARD USE ONLY

Description:	**User ID:**
	Date Received:
	Ticket Number:
	Ticket Submission Date:
	Ticket Closed Date:
	Access Reviewed Date:
	Access Reviewed By:

Admissions Office	_____ Signature	**Financial Aid**	_____ Signature
Business Office	_____ Signature	**Registrar's Office**	_____ Signature