Banner Access Form

1. _____
   Last Name (print) First Name Middle

2. Department Name: _____ Phone: _____

3. Job title _____ Clark Email _____

4. My status: (circle one) Staff Faculty Administrator Student Other

5. This is a request to: _____ Create a new Banner account
   _____ Modify my Banner account (Banner username _____)

6. I am requesting access to the following areas:

_____Finance/Budget _____Financial Aid _____Student _____Admissions _____Human Resources _____General _____Advancement

7. I have read, signed and attached the Confidentiality Statement. I agree to abide by the policies outlined.

Applicant Signature: _____ Date:_____

8. Supervisor Authorization - Please attach the official job description to help us assign the correct roles.

Does the person need access to Xtender/BDMS? Yes No

Does this person need access to Argos? Yes No

Does this person need access to BI Query? Yes No

Does this person need a jobsub account? Yes No

Who was in this position prior to this person? _____

As departmental representative, I approve the access requested by the above employee on both sides of this form. If the user of the above computing account leaves this department, I will notify ITS so that the account may be removed.

_____ _____ _____
Signature of Supervisor **Date** **Phone**

Supervisors should route this and the Confidentiality Statement to the first Banner Data Manager.

9. Banner Data Managers' Authorizations

Banner Classes and/or Oracle Role(s)	Banner Data Manager Signature	Date
Finance/Budget		
Financial Aid		
Student		
UG Admissions		
Grad Admissions		
Human Resources		
General		
Advancement		
Discoverer		
Xtender		

It is assumed we will mask SSN, unless authorized otherwise. Please circle if data should not be masked: Not Mask

Initials of person approving unmasking SSN. _____

Confidentiality and Privacy Policy

Many offices within the University maintain highly confidential and restricted data about current and former students, faculty, staff, alumni or University business matters. In order to properly safeguard these records, and to ensure professional and confidential management of this information, it is required that all University faculty, staff and student employees acknowledge that:

- All data that originates at Clark or is stored at the University, including storage on a University-owned computer system, is considered University property for the purpose of this policy.
- All Clark faculty, staff, student employees and consultants are expected to comply with state and federal regulations as well as University and departmental policies that govern access to, and use of, this information (visit **http://www.clarku.edu/offices/its/policies/data_security_all.cfm** or see Human Resources for hard copy).
- Clark University data will only be accessed by and/or disclosed to an individual, group, organization, and/or office on a "need-to-know" basis in order to accomplish legitimate University business. The access/disclosure will be limited to the minimum amount of confidential information necessary to accomplish the intended purpose, disclosure or request. Before sharing information with others, electronically or otherwise, reasonable care is expected to ensure that the recipient is authorized to receive that information and understands his/her data responsibilities.
- All confidential information must be handled with discretion, safeguarding it when in use, as well as when not in use, disposing of it properly (i.e. shredding) when no longer needed, and not disclosing or discussing it with any unauthorized person. To safeguard computer data, faculty, staff, student employees and consultants should never share computer login or password information; leave their computer unsecured when away from their desk for extended periods; or ever leave mobile devices that access University systems unattended.
- There may be legitimate requests for data from law enforcement officers. When contacted by a law enforcement officer requesting student information you should direct the inquiry to the University Registrar or Dean of Students. When contacted by a law enforcement official for information about faculty or staff you should direct that inquiry to the Director of Human Resources.
- An obvious or deliberate breach of Clark's Data Security Policies will be considered a serious infraction of University rules and the breaching employee or consultant may be subject to disciplinary action, up to and including termination.
- Unauthorized use of confidential information may also subject an individual to personal, civil and/or criminal liability and legal penalties.

I certify that I have reviewed and understand the above Confidentiality and Privacy Policy as well as the University's Data Security Policies and that I will take appropriate measures to preserve the confidentiality and privacy of this information.

_____

Employee/Consultant Name (Please print)

_____ _____

Employee/Consultant Signature Date Signed

Note: the completion of additional confidentiality statements may be required to access University data and/or computer systems and/or computer systems.

Data Managers

AREA/SYSTEM	COORDINATOR	PHONE	E-MAIL
Finance/Budget	Kathy Cannon	Ext. 7499	kcannon@clarku.edu
Financial Aid	Mary Ellen Severance	Ext. 7478	meseverance@clarku.edu
Student	John Ohotnicky	Ext. 7561	jrohotnicky@clarku.edu
Undergraduate Admissions	Terry Malone	Ext. 7432	tmalone@clarku.edu
Graduate Admissions	Jerry Czub	Ext. 7559	jczub@clarku.edu
Human Resources	David Everitt	Ext. 7397	deveritt@clarku.edu
General	Becky Frieden	Ext. 3812	bfrieden@clarku.edu
Advancement *(query only)*	Paul Milionis	Ext. 3834	pmilionis@clarku.edu