



## Area and System Coordinators

AREA/SYSTEM	COORDINATOR	PHONE	E-MAIL
Student	Rebecca Hunter	Ext. 7561	<a href="mailto:rhunter@clarku.edu">rhunter@clarku.edu</a>
Human Resources	Lynn Olson	Ext. 7294	<a href="mailto:lolson@clarku.edu">lolson@clarku.edu</a>
Payroll	Kathy Cannon	Ext. 7499	<a href="mailto:kcannon@clarku.edu">kcannon@clarku.edu</a>
Finance/Budgets/Accounts Receivable	Kathy Cannon	Ext. 7499	<a href="mailto:kcannon@clarku.edu">kcannon@clarku.edu</a>
Financial Aid	Mary Ellen Severance	Ext. 7478	<a href="mailto:meseverance@clarku.edu">meseverance@clarku.edu</a>
Alumni/Advancement <i>(query only)</i>	Karen Doherty	Ext. 7718	<a href="mailto:kdoherly@clarku.edu">kdoherly@clarku.edu</a>

## Banner Finance/Budget Access

Banner ID: \_\_\_\_\_

Last Name (print) \_\_\_\_\_ First Name \_\_\_\_\_ Middle \_\_\_\_\_

Department Name: \_\_\_\_\_ Phone: \_\_\_\_\_

Job title \_\_\_\_\_ Email \_\_\_\_\_

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

**Budget Authority Approval:**

Banner Finance/Budget security is based on FUND and ORGN. In order to facilitate the request please complete the information below: I am authorizing the person noted above to view transactions for:

\_\_\_\_\_ all FUNDs for the department of \_\_\_\_\_

\_\_\_\_\_ all ORGNs for the department of \_\_\_\_\_

**OR** \_\_\_\_\_ is limited to the following:

Fund _____	Org _____	Fund _____	Org _____
Fund _____	Org _____	Fund _____	Org _____
Fund _____	Org _____	Fund _____	Org _____
Fund _____	Org _____	Fund _____	Org _____

Other comments regarding access limits for this applicant:

---



---



---

\_\_\_\_\_  
**Primary Budget Authority Signature** **Date**

\_\_\_\_\_  
**Printed Name Primary Budget Authority** **Title**

*If there are any questions regarding the completion of this side, please call Business and Financial Services. Be sure to complete items 1-8 on page 1 of this form. This page should be forwarded directly to Kathy Cannon in Business and Financial Services.*

*Office use only:*  
 Controller/Associate Controller approval: \_\_\_\_\_ Date: \_\_\_\_\_  
 User established in Banner by \_\_\_\_\_ Date: \_\_\_\_\_

## 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](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.**