Table of Contents

1. **Introduction to Access Security** ........................................................................................................ 3
2. **Resources for Security Administrators** .................................................................................................. 3
3. **The Data Confidentiality Agreement** ...................................................................................................... 4
4. **View Security Documents** .................................................................................................................. 5
5. **Security Access Reports** ...................................................................................................................... 6
6. **Access to Systems not administered by Access Management** .............................................................. 7
7. **Access Request Tips** ................................................................................................................................ 8
8. **Security Forms – Paper and Workflow** ............................................................................................... 9
9. **Request Access to Cognos and Imaging** .......................................................................................... 10
10. **Request Access to FAMIS, BRM, GPS, and more** ............................................................................. 10
11. **Request Access to Banner** ................................................................................................................ 11
12. **The Banner Security Workflow** ....................................................................................................... 12
13. **Job Change or Separation Procedure** ............................................................................................. 13

**Appendix A. Document Imaging Reference Guide** ............................................................................... 14

1. LOGGING INTO APPXTENDER WEB ACCESS .................................................................................. 14
2. APPXTENDER WEB ACCESS NAVIGATION ** ................................................................................... 14
3. LOGGING OUT OF APPXTENDER WEB ACCESS ................................................................................ 14

**Appendix B. Security Reports Search Guide** ....................................................................................... 15

**Appendix C. Paper Security Access Forms Guide** ............................................................................... 17
1. Introduction to Access Security

A Departmental Security Administrator is the designated individual who is responsible for helping staff obtain access to University data systems, and for removing access when it is no longer needed. A department should have a Security Administrator and a backup SA.

Security Administrators complete forms to request authorization for an employee to access a system. He or she may confer with the Data Steward to determine the appropriate access to request. The Data Steward for the system reviews the request. If it is approved, the office of Security and Access Management fulfills the request. Notification is sent to the Security Administrator, who notifies the employee.

2. Resources for Security Administrators

Office of Security and Access Management
AccessManagementGroup_DCO@kent.edu

330-672-1366

Fax 330-672-3253

Access Management Web site  [https://www.kent.edu/it/systems-access](https://www.kent.edu/it/systems-access) offers links to:

- Data Stewards List
- Security Administrators List
- Data Confidentiality Agreement
- Security Access Request forms
- Security Access Reports

FlashLine offers links to

- Security Document Imaging
- Banner Security Workflow
3. The Data Confidentiality Agreement

Prior to gaining access to any University administrative systems, the employee must read and sign a form called the *Data Confidentiality Agreement*.

A Security Administrator or Data Steward must submit their own signed Data Confidentiality Agreement, in order to be given the authority to submit security requests for other employees.

The form can be downloaded at:

[https://www.kent.edu/it/confidentiality-form](https://www.kent.edu/it/confidentiality-form)

Check the Security Documents imaging database to see if the Employee has a Data Confidentiality Agreement Form on file. If the employee does not have a Confidentiality Agreement on file, please have the employee fill out the Data Confidentiality Agreement form and sign it. Send the Data Confidentiality Agreement to Access Management, AMGroup_DCO@kent.edu.

If you are requesting Banner production access, you may scan and upload the document image in the Banner Security workflow form. If you are submitting an access request using a **paper form**, attach the Confidentiality Agreement to the request form and send to:

Access Management, 246 Stewart Hall

Fax 330-672-3253
4. View Security Documents

You have the ability to sign into document imaging to view Confidentiality Agreements and Completed Banner Access Request Forms.


<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Open a web browser</td>
</tr>
<tr>
<td>2.</td>
<td>Log in to FlashLine at <a href="http://www.kent.edu">www.kent.edu</a></td>
</tr>
<tr>
<td>3.</td>
<td>Navigate in the Employee category, the Resources page, and the Additional Employee Resources section</td>
</tr>
<tr>
<td>4.</td>
<td>Click the link for <em>Banner Integrated Document Imaging Application</em></td>
</tr>
<tr>
<td>5.</td>
<td>You may be asked to sign in a second time. Click the Security Documents link</td>
</tr>
<tr>
<td>6.</td>
<td>Click the New Query button to initiate a search</td>
</tr>
<tr>
<td>7.</td>
<td>In the records search screen, type the Employee criteria in the search fields</td>
</tr>
<tr>
<td>8.</td>
<td>Click “Run” to retrieve results</td>
</tr>
<tr>
<td>9.</td>
<td>Hover the mouse over the Page Icon to preview, or click the dropdown arrow to select an action option such as open, or print</td>
</tr>
<tr>
<td>10.</td>
<td>There are icons to enlarge and rotate the view</td>
</tr>
<tr>
<td>11.</td>
<td>The Print Document icon prints all pages</td>
</tr>
<tr>
<td>12.</td>
<td>Click the New Search breadcrumb link to search another record</td>
</tr>
</tbody>
</table>
5. Security Access Reports

You have the ability to view reports which tell you the access that an individual currently possesses. Quickly look up individual users and groups of users with these reports. Report data may be exported and saved as a spreadsheet.

To access the reports, open a browser and go to this address:

https://webservice.kent.edu/BannerSecurity/

Log in using your full @kent.edu email address as the Username, and your FlashLine password. The INB Banner Security Reports screen will appear.

There are two ways to run reports:

1) Click the link “View Cognos Security Reports” to select a security class and see a table of users who have access to that security class.

2) Select a Report Name from the drop menu.

See Appendix B., Security Reports Search Guide for search examples and more information about these reports.
6. Access to Systems not administered by Access Management

There are many systems in use at the University to which access is not administered by the Office of Security and Access Management. Rather, access to a system is controlled by the institutional owner or licensee, or by Client Services. Consult with your business manager to learn about tools and resources that may be available to you, and contact the system administrator directly to request access.

For systems administered by Client Services, you may fill out a service request at http://support.kent.edu

<table>
<thead>
<tr>
<th>System or Tool</th>
<th>Administered by</th>
</tr>
</thead>
<tbody>
<tr>
<td>ABC Signup - event registration</td>
<td>HR Training and Development</td>
</tr>
<tr>
<td>Hobson’s - contact and event management</td>
<td>University Admissions</td>
</tr>
<tr>
<td>Drupal - web content management</td>
<td>University Communications &amp; Marketing</td>
</tr>
<tr>
<td>Blackboard Learn - course management</td>
<td>Educational Technology</td>
</tr>
<tr>
<td>Wimba, Citrix - web conferencing</td>
<td>Departmental license holders</td>
</tr>
<tr>
<td>Cisco WebEx - web conferencing</td>
<td>IT Client Services (support.kent.edu)</td>
</tr>
<tr>
<td>SharePoint - web collaboration</td>
<td>IT Client Services (support.kent.edu)</td>
</tr>
<tr>
<td>Cisco VPN - off campus access to systems</td>
<td>IT Client Services (support.kent.edu)</td>
</tr>
<tr>
<td><strong>Shared Network Drives</strong> for departments</td>
<td>IT Client Services (support.kent.edu)</td>
</tr>
</tbody>
</table>
7. Access Request Tips

- Access Management cannot honor a request to 'give employee B the same access as employee A'.
- You must specify exactly what access is needed on the access request form.
- It may be necessary to submit a paper form, and/or multiple workflow requests; to cover access to multiple systems.
- Access is granted using the employee's FlashLine username.
- The username is also needed for Security to look up and troubleshoot an individual's access. When you contact the office of Security and Access Management about an employee, always provide the FlashLine username. Whether you contact Security by email (Access Management Group_DCO@kent.edu) or phone (330-672-1366) the employee FlashLine username is required.
- Security Administrators or Data Stewards may not authorize an access request for themselves. If a Security Administrator or Data Steward needs access, a backup Security Administrator or Department Head may sign the paper form. A backup Security Administrator must submit the workflow forms.
- The Banner Security workflow provides easy viewing of past requests with no printing needed.
- When you request access for an employee using a paper form, Access Management will reply with an email which lists the access that was granted. You can save these messages in a mail folder or copy the access information from the email into an Excel spreadsheet, giving yourself a record for later reference. You should notify the employee when access is granted.
- The only forms that the employee should sign are the Data Confidentiality Agreement form, and the Remote Access to Administrative Systems form, required if the employee must access certain systems from off-campus via the Cisco VPN.
- All other forms are signed only by the Security Administrator and Data Stewards.
8. Security Forms – Paper and Workflow

- Banner production access requests using the workflow form.
- All other system access requests, and Banner test access requests, are made using paper forms.

Please do not save blank copies of paper security forms for later use. Forms are constantly updated with new information, and you must use the current version, which is available from the Security and Access Management web site:

https://www.kent.edu/it/systems-access

A request which is submitted on an obsolete form will be returned to the Security Administrator with a request to resubmit the request using the current version of the form. Using the current form will ensure that Access Management can commence processing the request on the day that it is received.

If you do not know exactly which permission classes to check off on a form, please contact the relevant Data Steward, who is your resource for identifying the appropriate access to request for an employee.

See Appendix C., Paper Security Access Forms Guide, for details of how to complete paper access request forms.
9. Request Access to Cognos and Imaging

<table>
<thead>
<tr>
<th>To obtain this access level</th>
<th>Use this form</th>
</tr>
</thead>
<tbody>
<tr>
<td>Consumer access to Official Folders and Reports</td>
<td>Official Folder access form</td>
</tr>
<tr>
<td>Report authoring capability, and access to restricted internal administrative folders and reports.</td>
<td>Internal Folder Access form</td>
</tr>
<tr>
<td>Document imaging -- access to the imaging applications in the Banner environment</td>
<td>Banner Document Imaging form</td>
</tr>
<tr>
<td>Access to enable upload or download to administrative systems and to input or output files from the WebFTP server.</td>
<td>FTP Access form</td>
</tr>
</tbody>
</table>

Inquiries regarding Cognos access should be directed to Cindy Roberts, Cognos Lead Applications Developer, at (330) 672-8630.

10. Request Access to FAMIS, BRM, GPS, and more

All forms available from [https://www.kent.edu/it/systems-access](https://www.kent.edu/it/systems-access)


BRM Access - Complete a Request for Access to BRM form (Banner Relationship Management) to manage your campaigns or view results. Direct inquiries to Barb Boltz, Project Director, Student Affairs at 330-672-1306.

GPS System Access -- Complete a Request for Access to GPS System form to gain access to GPS Audits and Plans. Joanna Liedel, Associate Director, University Advising 330-672-4202.

Other access request forms available include 3rd party email, FTP directory access, FortiClient VPN, direct access to administrative databases, advisor assignment application, and Guest Accounts.
11. Request Access to Banner

Ellucian Banner is a multifaceted administrative data system used at KSU. It is also referred to as ‘the ERP,’ an abbreviation of Enterprise Resource Planning system.

The university maintains several copies or ‘instances’ of the Banner system, for different purposes. The real-time instance that is used to conduct everyday business is called the production instance. There are also test, development, and training instances.

Contact the Banner Data Steward for an area to discuss special access needs.

- Use a paper form to request access to test instances. The forms can be found at:
  
  [https://www.kent.edu/it/systems-access](https://www.kent.edu/it/systems-access)

**Banner Data Stewards**


Finance - Tammy Slusser, University Comptroller, (330) 672-8328.

HR and Payroll - Tia Laughlin, Manager, Human Resources Records, (330) 672-8374.

Student - Barbara Boltz, Project Director Student Affairs, (330) 672-1306.

Student Financial Aid - Steven Minnich, Manager, Student Financial Aid System, (330) 672-0527.
12. The Banner Security Workflow

Ellucian Banner is an administrative data system used at KSU. Departmental Security Administrators use the workflow described in this document to request access to Banner (production) on behalf of department employees. The workflow is also used to request discontinuation of access when an employee’s work assignment changes.

A workflow form is delivered instantly to the next-level reviewer and cannot be lost. It is stored with a time- and date-stamped record of approvals and can be viewed later.

Use the workflow to request access to Banner production forms and groups of forms in these functional areas:

Use the Banner Security workflow to request access to Banner 9 production Admin Pages forms and groups of forms used by these security areas:

<table>
<thead>
<tr>
<th>Admissions</th>
<th>Advancement</th>
<th>Bursar</th>
</tr>
</thead>
<tbody>
<tr>
<td>Finance</td>
<td>Financial Aid</td>
<td>Health Center</td>
</tr>
<tr>
<td>Human Resources</td>
<td>Judicial Affairs</td>
<td>OneStop</td>
</tr>
<tr>
<td>Provost</td>
<td>Registrar</td>
<td>Residence Services</td>
</tr>
<tr>
<td>Student Disability Services</td>
<td>Student Financial Aid</td>
<td></td>
</tr>
</tbody>
</table>

The Banner Security Workflow User Guide and printable forms are available from:

https://www.kent.edu/it/systems-access
13. Job Change or Separation Procedure

Q. What should I do when an employee changes departments?

A. If an employee leaves your department, please submit a request form to have all of their access removed. The Security Administrator in their new department will request access which is appropriate to the employee’s new position.

- Use the same paper form or workflow that you would to add access.
- Only one Banner Security workflow form is needed to remove all Banner access.
- Indicate the date that this should take effect.
- Do not submit a HelpDesk ticket for this type of request.

Q. What should I do when an employee leaves the University?

A. If a separation workflow form has been initiated for the departing employee, no further action is needed by the DSA. Access Management receives workflow notification, and will remove all of the employee’s access as of the first working day after the employee has left.

If you do not know whether a separation workflow form has been submitted for the employee, please email Access Management the date upon which you want the access to be removed. Do not open a Helpdesk ticket for this type of request.
Appendix A. Document Imaging Reference Guide

1. LOGGING INTO APPXTENDER WEB ACCESS

Open a web browser.

**For Production:** in FlashLine on the My Actions Tabs there is a link in the Workflow and Utilities section (Banner Integrated Document Imaging Applications (Admissions and Procurement) or go directly to Xtender with the following URL - https://axprod.kent.edu/AppXtenderAdmin/account/login

   a. Enter your FlashLine User Name and Password

   b. ‘Request Full Text Search Support’ should be unchecked.

   c. Click Login

NOTE: Password must be synchronized with banner before this login will work (see section 1.1).

2. APPXTENDER WEB ACCESS NAVIGATION **

Documentation for the AppXtender Imaging Resource may be found at:

https://support.kent.edu/appxtender

**NOTE:** Depending on the privileges that were granted to you, you may not be able to use or see each function from the AppXtender Web Access Navigation Menu.

3. LOGGING OUT OF APPXTENDER WEB ACCESS

To Logout of AppXtender Web Access, go the File | Logout or click the logout button.

Be sure to always logout of your session and not just close your web browser so the license is available for the next user.

If your session is inactive for 15 minutes you will be automatically logged out.
Appendix B. Security Reports Search Guide

To view the security access reports, open a browser and go to this address:

https://webservices.kent.edu/BannerSecurity/

Log in using your full @kent.edu email address as the Username, and your FlashLine password.

There are two ways to run reports:

1) Click the link “View Cognos Security Reports” to select a security class, and view a list of users who have access to that security class.

2) Select a Report Name from the drop menu.

Search Terms and Search Examples

**Count Classes** – The number of Security classes in a Banner module

**Count Users** – The number of users with access to a security class

**Users by Class** – Maps a user ID to the Classes to which the user is assigned

Example 1: Search by **User ID** – JSMITH returns:

BAN_ALL_USERS_C
BAN_ALL_USERS_INB_C
Etc. and displays the person name and department

Example 2: Search by **Class** – BAN_ALL_USERS_C returns:

ASMITH
BSMITH
Etc. and displays user names and departments

**Objects by Class** – Maps the Class name to the Objects to which it provides access

Example 3: Search by Class – BAN_ALL_USERS_C, returns

OBJECT1
OBJECT2
Etc. and shows whether each object has write (BAN_DEFAULT_M) or read-only (BAN_DEFAULT_Q) access
Example 4: Search by Object – SPAIDEN, returns

BAN_CLASS_1_C
BAN_CLASS_2_C
Etc. and shows whether the object has write (BAN_DEFAULT_M) or read-only (BAN_DEFAULT_Q) access within each class

**Direct Grants** – Rare. Used when someone is directly assigned access to an object but not to the class of which the object is a member. Direct Grants are given only on a temporary basis.

**User ID** or **Object name** -- will show whether the person is granted write access (BAN_DEFAULT_M) or read-only access (BAN_DEFAULT_Q) to the object.

**Objects to Users** – Maps across User ID, Class, and Object assignment

Example 5: Search for User ID JSMITH, returns

User, Class, Object – (a person has access to object X because they are a member of class Y) and displays write or read-only access, and the person name and department.

Example 6: Search for Class BAN_ALL_USERS_C, returns

User, Class, Object – for each object in BAN_ALL_USERS_C, and for each User ID that is a member of BAN_ALL_USERS_C and displays write or read-only access.

Example 7: Search for Object SPAIDEN, returns

User, Class, Object for all of the classes that provide access to SPAIDEN, and all of the users who are a member of those classes

**Advanced Searches**

**Business Profiles** (appears on the student form)

This search term can be search in place of User ID. It displays the classes and objects which belong to a business profile. Does not display User IDs of members of that business profile

**View Cognos Security Reports**

Click to view the list of Groups.

Click on a group to view the list of user names who are members of that group.

Click on a user name to view the groups to which the user belongs.
Appendix C. Paper Security Access Forms Guide

Note: Paper forms are not used for Banner 9 Admin Pages in the production environment. Submit these requests using the Banner Security Workflow.

Section 1. (A) Employee Information

All employee information should be filled in.

The information required for access to be granted is:

- Employee Name
- FlashLine User ID
- Banner ID#

Section 1. (B) Access requirements

Request Type: check one only

- Add User: Create a new account. Use for an employee who does not have an existing account.
- Remove User: Remove all access which the employee currently has, or remove the access from any security class with a checked box.
- Replace Permissions: Remove ALL existing access and replace it with the access marked on the form. This removes all access from all areas that the employee may currently have, and provisions the new permissions.
  *NOTE* If no access is marked then all access will be removed.
- Additional Access: To add new permissions to the employee’s current access profile.

Purpose for access: Describe the access that is needed. The Data Steward will determine which boxes to check on form, or verify that the ones you marked are correct.

Access to (check all that apply):

- Production (ePROD)
- Test (indicate which instance is being used)
  - eTEST
  - eDEVEL
  - ePPRD
  - eQA
  - eQA
  - eBUDD
  - eMock
Section 1. (C) Unit Security Admin Name & Signature

The Data Security Administrator must sign the request form.

Section 2: Security Classes

If you know what boxes need to be checked in Section 2, you can go ahead and check them, they will be reviewed and approved by the Data Steward.

If you are not sure what boxes need to be checked, you can 1) contact the Data Steward and discuss the matter, or 2) describe the access you would like in the Purpose for access comment field in Section 1. (B), and submit the form. The Data Steward will check the appropriate boxes for access.

In Section 2 you will see the name of the Data Steward & Unit displayed in the highlighted box which appears above the access area which they approve.

Send the completed request form to the appropriate Data Steward for their approval.

The Data Steward will send the signed form to Access Management for processing.

Access Management will send an email to the Security Admin and Data Steward when the request is fulfilled. The email lists the access that was granted to the employee. The Security Administrator will notify the employee that access has been granted.

You may wish to save these messages for later reference, or to copy the access that was given to the user into an Excel spreadsheet or other document, for your records.

IMPORTANT NOTES:

- DO NOT send in two-sided forms. Completed forms are scanned and the scanner will not pick up the reverse side of form pages.

- Be sure to send ALL pages of a request form even if you only write on the first page. This confirms to Access Management that no pages are missing from the request.

- Access Management will complete Section 3 of the form when the request is completed.