SYSTEMS ACCESS REQUEST
BUSINESS PROCESS GUIDE

REVISION CONTROL

Date	By	Action	Page
7/23/09	M D'Arpino	Added the Hyperion Grandfathered Rule	2
8/6/09	M D'Arpino	Updated List Serv names and purposes	9
8/6/09	M D'Arpino	Updated the ARF Folder access description.	10
8/12/09	M D'Arpino	Revised the Audit section	11
8/14/09	M D'Arpino	Added "Any" to New Process item 1e	4
8/14/09	M D'Arpino	Added "ITS mail server" to New Process 7a to be consistent with the Change and Disable processes	5
9/8/09	M D'Arpino	From the Overview diagram – Added Functional Security Administrator's figure next to the Administratively Complete process and removed the line connecting the Verify Form Completeness and Administratively Complete processes (per A Kircher review)	1
9/8/09	M D'Arpino	Remove reference to Developer access process (per A Kircher review)	2
9/8/09	M D'Arpino	Added Finance Signature Authority exception process (per M Haynes Swank)	2
9/8/09	M D'Arpino	Changed New Process Step 2b to state that the Confidentiality Agreement need only to have been forwarded to the Vice-President of Administrative Affairs (signature and on file with HR is not necessary – per A Kircher)	4
9/8/09	M D'Arpino	Changed the New Process Step 2b to state that the Signature Authority form only needs to be sent to Procurement (per A Kircher)	4
9/8/09	M D'Arpino	Modified the Change process so that it can be used when a person leaves a department, but not the university and modified the Disable process so that it only applies to separations	6
9/8/09	M D'Arpino	Updated the Access Created E-mail Notifications	7 and 8
9/8/09	M D'Arpino	Updated the PS Security List Members	10
9/9/09	M D'Arpino	Define "Requester" as "User or Department Representative" (per M Haynes Swank)	4 and 6
9/9/09	M D'Arpino	Added "If you have technical difficulties, please contact the ITS Help Desk at x4357 or help@humboldt.edu. If you have questions about how to use the system, please refer to the Training and Job Aids below or contact the appropriate business department <URL for the Finance, HR, or CS group>" to the Notification messages. (per M Haynes Swank)	7 and 8
9/9/09	M D'Arpino	Change PS Security List-Procurement to "Needs to know who is approving Requisitions as part of the Signature Authority process "(per M Haynes Swank)	10
9/9/09	M D'Arpino	Modified for incorporation into the ITS ticketing system (KBox)	15
9/9/09	M D'Arpino	Modified the Signature Authority exception process for KBox	6
11/30/09	M D'Arpino	If person is both the Submitter AND the Access Grantor, then the person's wet signature on the ARF is sufficient for access approval. FSA will change the System Status to "Data Manager Approved" and add a comment.	15
11/30/09	M D'Arpino	Disable Process – If the request is from SPF, FSA to look up the user's PeopleSoft Job Data to see if the person is working for a campus department. If yes, then add a comment to make the TSA aware that they should only remove the SPF access.	10
1/13/10	M D'Arpino	Added Contact to the Access Request Form – Now the User's Supervisor can designate someone else to receive status updates. Both the Contact and User will receive e-mails from CMS Access	8, 11

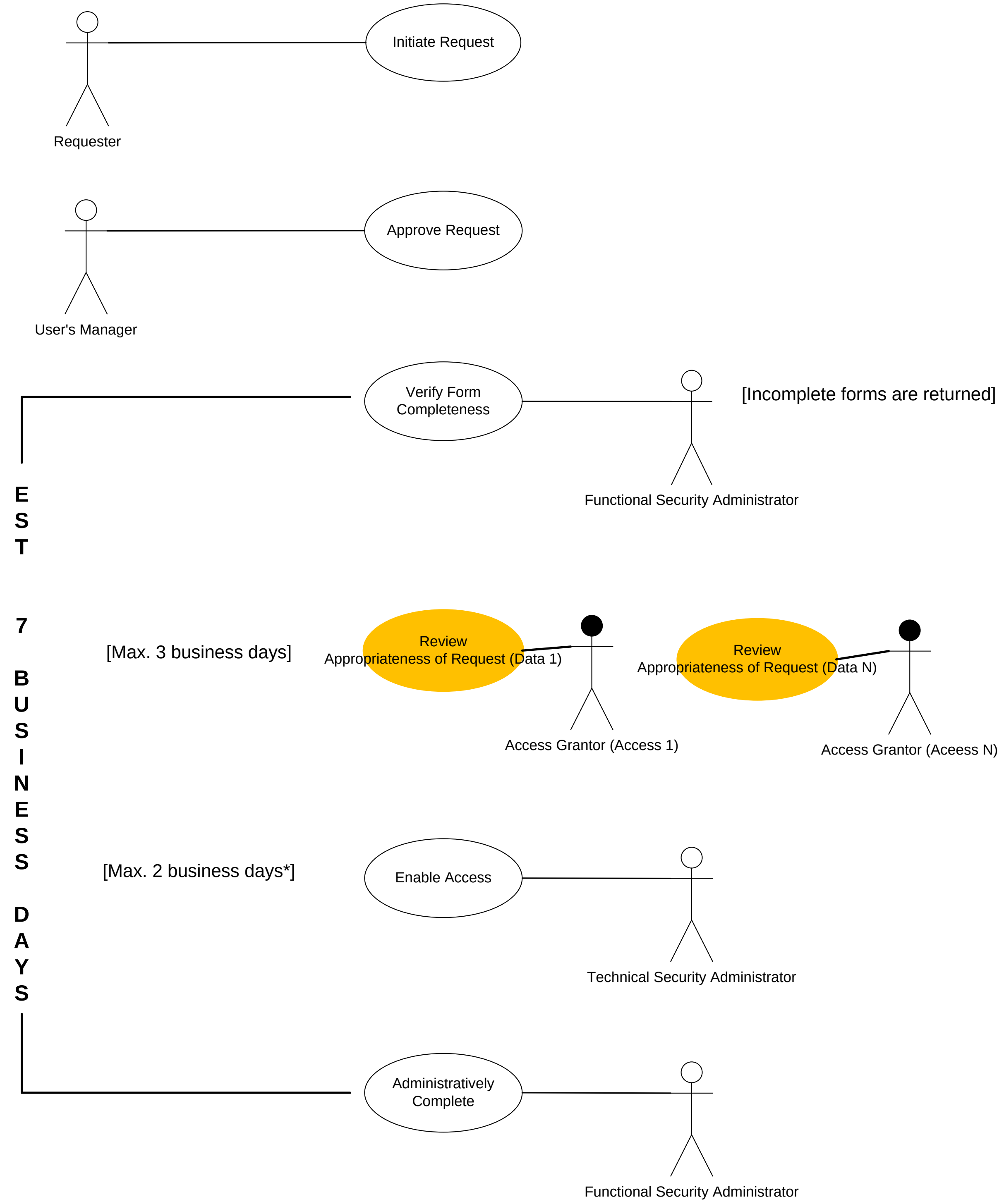
Date	By	Action	Page
		Request when the Access Request is received by the CMS Project Office, the Access Grantor Review(s) is completed, and after the access is set up. If no Contact is designated, then the User and the User’s Supervisor will receive the status updates.	
1/13/10	M D’Arpino	Changed “Data Manager” to “Access Grantor” on the Access Request Form and Instructions – This is consistent with the latest terminology used on Campus. The Access Grantor is responsible for reviewing the Access Request and approving access when appropriate for the User’s job. If the access requested is for multiple business areas or organizations, more than one Access Grantor may need to review (your completed Access Request form will automatically populate the required Access Grantor names and they are also listed in the Access Request Instructions).	Various
1/13/10	M D’Arpino	Modified the Access Grantor Notification Process – An Access Grantor now receives an email only when there is an Access Request to review.	9
7/13/10	P Stewart	Updated all URLs to reflect move to new server. Updated information regarding navigation on the CMS web site to reflect new web site’s layout. Added sentence directing those who need more information about filling out the ARF to the instructions on the Forms site. Changed the Dept ID verification process because the previous process did not work. Change step 4f to indicate that the FSA will send the access grantor a reminder e-mail within three days, not one week as previously stated. Update Change Process to be Modify Process. Replaced Cortney Koors on the PS Security List Members with Sharie Parrott and replaced Denise Gentry with Stephanie Steffen. Under Appendix E, removed the link directing readers to the CSU policy regarding audits because the document no longer appears to there. Finished incomplete sentence regarding the systems status category.	Various 6 8 8 9 10 14 14 15
7/21/10	P Stewart	Remove Melinda Haynes Swank, Colby Smart, and Denise Gentry from the ps_security listserv.	10
9/10/10	M D’Arpino	Added Generic Batch Account process	8
9/10/10	M D’Arpino	Replaced overview diagram with the newer version	1
9/10/10	M D’Arpino	Replaced detailed process diagram with a newer version	4
9/27/10	S Parrott	Added Listserv instructions detail	11
9/27/10	S Parrott	Added Create Ticket Instructions detail	17
10/08/10	M D’Arpino	Updated Generic Batch Account process	
2/15/11	S Parrott	Replaced Hyperion with OBI	Various
2/15/11	S Parrott	Update Appendix I –Ticket Systems and Categories	16
3/7/11	S Parrott	Update List Serve Process	11
6/9/11	S Parrott	Update Exceptions to the Access Request Process from Hyperion to OBI	3
6/28/11	S Parrott	Included OBI update (same as above) in the Comments section of Appendix F	13
10/12/11	S Parrott	Update OBI process	3, 13
7/29/12	J Hansen	Update PS Security List Membership, Add J Hansen, J Clarke, remove P Johnson, J Stebbins, C Webb, S Parrott Replace CMS office with ITS Project Office references	12, Various,
12/7/12	C Koors	Removed Exception section for Signature Authority. The 2009 customization was removed with the 2010 CFS project.	3
12/7/12	C Koors	Added exception section for Finance Requests	3
12/18/12	C Koors	Updated link to Procurement Signature Authority Form for operating funds and trust funds	5,7

Date	By	Action	Page
1/14/13	C Koors	Add OBI APS to Appendix I	17
1/15/13	C Koors	Update TSA access grantor review step	6
3/18/2013	C Koors	Update ARF Folder access instructions	15
3/18/2013	C Koors	Replace CMS and Common Management with Enterprise Systems	All
3/18/2013	C Koors	Remove Banner, Add Nolij	1
3/18/2013	C Koors	Removed Signature Authority form wording	5, 6
3/18/2013	C Koors	Revise sentences, Fix formatting	All

Review/Approval History

Date	By	Action	Page
9/3/09	A Kircher	Requested changes	1, 2, 4, 6, 7, 10
9/9/09	M Haynes Swank	Requested changes	4, 6, 7, 8, 10

OVERVIEW


Requester
Initiate Request
User's Manager
Approve Request
Verify Form Completeness
Functional Security Administrator
[Incomplete forms are returned]
EST 7 BUSINESS DAYS
[Max. 3 business days]
Review Appropriateness of Request (Data 1)
Access Grantor (Access 1)
Review Appropriateness of Request (Data N)
Access Grantor (Aceess N)
[Max. 2 business days*]
Enable Access
Technical Security Administrator
Administratively Complete
Functional Security Administrator

The Access Request process is used to create, modify, or inactivate a person's access to Enterprise Systems, including:

- PeopleSoft*: Human Resources, Campus Solutions, or Finance
- Select systems Interfaced to PeopleSoft
- OBI (data warehouse) reporting enterprise applications
- Hobsons Permission
- NOLIJ
- DARWIN (DARS)

*Students, Faculty, Advisors, and Staff are excluded from the ARF process only for PeopleSoft Self Service access. Their access is controlled by separate User Profile Mass Creation processes.

HSU's Functional Security Administrator (FSA from the ITS Administrative Support department) coordinates the access request process, the Access Grantor reviews/approves access to the data, and the Technical Security Administrator manages the access.

The Access Request form, business process guide, instructions (with a list of applications/roles), and FAQ are available on http://www.humboldt.edu/its/po-accessrequest.

The User Mass Creation access request is similar to the Access Request process except:

A spreadsheet is submitted with a list of employees requiring access.

The Generic Batch Account process is similar to the Access Request process except:

The account is for a system (or system/module), not a person.
Access Grantors signs the ARF.

Per the CSU Access Control Policy (8060) http://www.calstate.edu/icsuam/sections/8000/8060.0.shtml, '… Users experiencing a change in employment status (e.g., termination or position change) must have their logical access rights reviewed, and if necessary, modified or revoked.' This review is also necessary if position duties change.

Additional actions for managers of separating employees are published in the Manager's digital resources checklist for separating employees.

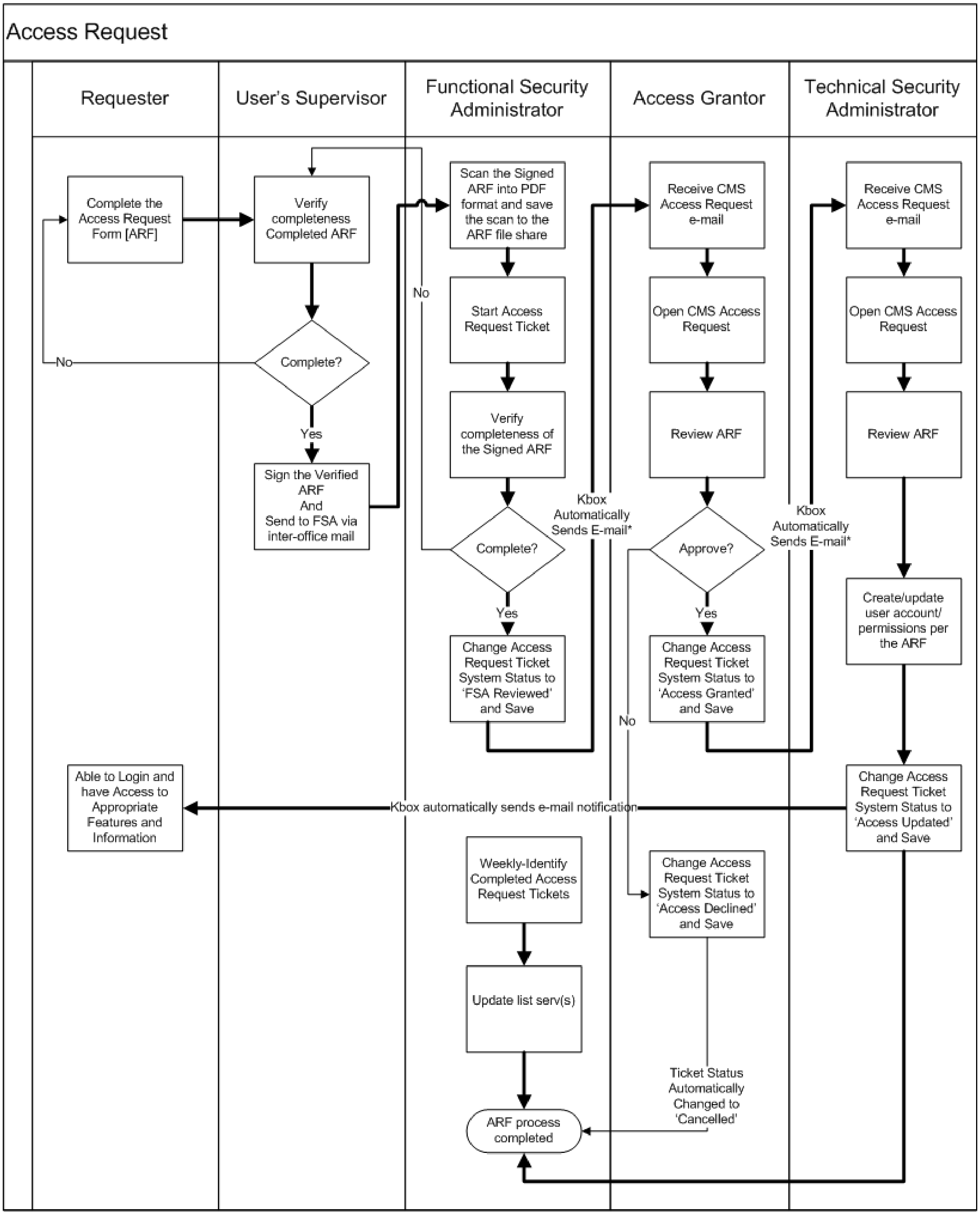
We attempted to make this process compliant with the Oct. 27, 2008, (draft) CSU System-wide Information Security Policy and Standards. Ideally, this process would be incorporated into the Human Resources Hiring, Change, and Separation processes.

EXCEPTION TO THE ACCESS REQUEST PROCESS

Finance Access Requests

PeopleSoft and CashNet access for Finance department users are handled within Finance using an internal Finance Access Request Process.

DETAILED PROCESS



Access Request
Requester
User's Supervisor
Functional Security Administrator
Access Grantor
Technical Security Administrator
Complete the Access Request Form [ARF]
Verify completeness Completed ARF
Complete?
No
Yes
Sign the Verified ARF And Send to FSA via inter-office mail
Scan the Signed ARF into PDF format and save the scan to the ARF file share
Start Access Request Ticket
Verify completeness of the Signed ARF
Complete?
No
Yes
Change Access Request Ticket System Status to 'FSA Reviewed' and Save
Kbox Automatically Sends E-mail*
Receive CMS Access Request e-mail
Open CMS Access Request
Review ARF
Approve?
Yes
No
Change Access Request Ticket System Status to 'Access Granted' and Save
Kbox Automatically Sends E-mail*
Receive CMS Access Request e-mail
Open CMS Access Request
Review ARF
Create/update user account/ permissions per the ARF
Change Access Request Ticket System Status to 'Access Updated' and Save
Kbox automatically sends e-mail notification
Able to Login and have Access to Appropriate Features and Information
Weekly-Identify Completed Access Request Tickets
Update list serv(s)
Change Access Request Ticket System Status to 'Access Declined' and Save
Ticket Status Automatically Changed to 'Cancelled'
ARF process completed

*KBox also notifies the User and Submitter of each change to the CMS Access Request

NEW PROCESS

The New Process is used to create a new account in one or more of the enterprise applications. New is used when a department has a new employee or contractor. The access will be for the Production instance unless instructed otherwise. If the request is for a Generic Batch Account, follow that process.

The Requester (the User or Department Representative) is responsible for filling out a portion of the form. The Employee/Contractor's Supervisor/Manager is responsible for the accuracy of that information as well as ensuring that the Employee/Contractor has a signed Confidentiality Statement on file. (Form available at http://www.humboldt.edu/hsuhr/forms/).

The detailed steps to process a New Access Request are:

1. User/Requester fills out the following form sections:
    a. User Information
    b. Request: Select "New Employee"
    c. Employee
    d. Roles
    e. Any additional Description of Access Needed
    f. If transferring from a different department on campus or changing positions or duties in your current department, verify a disable ARF has been submitted for previous position.

   (More information about how to fill out the Access Request Form is available at https://humboldt.edu/forms/node/44 .)

2. Employee/Contractor's Supervisor/Manager:
    a. Reviews the sections completed by the Requester for completeness and accuracy, including HSU username and requested department(s).
    b. Enters the Contact person, if not the User's Supervisor. The Contact, along with the User will receive the e-mail updates.
    c. Verifies that the Employee/Contractor's Confidentiality Statement was forwarded to the Vice-President of Administrative Affairs (or as appropriate, the President). Types/prints his/her name and then signs and dates the completed Access Request form
    d. Emails completed Access Request form to arf@help.humboldt.edu for processing.

3. Functional Security Administrator:
    a. Receives email notification that ARF has been submitted and follows link to KBOX ticket.
    b. Verifies the completeness of the form, sets ticket status to pending, adds systems and cc: Access Grantors, and adds username.

4. Access Grantor:
    a. Receives a system generated e-mail alerting the Access Grantor that there is an Access Request requiring the Access Grantor's approval. [The Access Grantor does not receive any other e-mails.]
    b. Clicks on the Ticket link within the e-mail.
    c. Logs into the Ticketing System.
    d. Opens and reviews the Access Request Form attachment
        i. Changes the appropriate System Status from 'FSA Reviewed to 'Access Grantor Approved.' Refer to Appendix I for a list of the systems. [Business Rule: Within three business days of e-mail receipt]The KBOX ticket is a vehicle to move the form through the approval process and is not meant to be a duplication of the information on the form. As noted in appendix F, if Business Unit, Enterprise System, and Access Grantor are the same with more than one role, only one System line is needed.

    e. Saves the changes. If there is more than one Access Request to review, then click on ‘Back to Tickets,’ click on the next ticket in the Access Grantor view, and then repeat Steps 4d through 4f. [Ticket Owner is automatically changed to ‘Technical System Administrator’ and e-mail sent to Security Google Group, User and User’s Supervisor once all Access Grantors have approved. System removes the Access Grantor(s) from the Ticket Cc List. If one Access Grantor declines, then the Ticket Status is automatically changed to ‘Cancelled.’ If Access Grantor has not ‘Approved’ or ‘Declined’ the Access Request within three days, then the Functional Security Administrator will send a reminder e-mail.]
    f. Logs out of the Ticketing System.

        i. If Access Grantor approves incorrect system before the ticket has changed ownership to the Technical Security Administrators, log into the ticket and change status of incorrect system back to ‘FSA Reviewed’ and update status of the correct system to ‘Access Grantor Approved’.

5. Technical Security Administrator:
    a. Receives a system generated e-mail alerting the Technical Security Administrator that there is an Access Request needing attention.
    b. Clicks on the Ticket link within the e-mail.
    c. Logs into the Ticketing System.
    d. Opens and reviews the Access Request Form attachment, verifying access grantor has approved the correct system.
    e. Creates the Employee/Contractor access in the Enterprise System
    f. Changes the appropriate System Status from to ‘Access Grantor Approved’ to ‘Access Updated.’
    g. Saves the Ticket. [Once all selected systems’ statuses are changed to ‘Access Updated,’ then a system generated ‘Access Created’ Notification is sent to the User and User’s Supervisor or contact if listed. The Ticket Status is automatically changed to ‘Completed’ and the Ticket Owner changed to ‘Functional Security Administrator.’ A TSA’s are reminded once a week until the ticket is completed. Ticket Status is automatically changed to ‘Closed’ after fourteen days]
    h. Logs out of the Ticketing System.

6. Functional Security Administrator:
    a. Adds Employee/Contractor to the appropriate ITS mail server distribution list(s) (See Appendix B).

MODIFY PROCESS

The Modify Process is used to add or remove access for an Employee/Contractor who is in the same department as when his/her access was first created (select "Same Position – New Roles) or transferring to a different department on campus (select "Transferring"). The access will be for the Production instance unless instructed otherwise. If the request is for a Generic Batch Account, follow that process. If the request is for multiple users to the same role (typically when a new system/role is added to the ARF), submit a Mass Creation request spreadsheet with user's supervisors signature.

As with the New Employee Process, the Requester (the User or Department Representative) is responsible for filling out a portion of the form. The Employee/Contractor's Supervisor/Manager is responsible for the accuracy of that information as well as ensuring that the Employee/Contractor has a signed Confidentiality Statement forwarded to the Vice President of Administrative Affairs (Form available at http://www.humboldt.edu/hsuhr/forms).

The detailed steps to process a Modify Request are the same as for New Employee except:

1. Requester identifies whether the request is for a "Same Position-New Roles" or "Transferring" and which Role(s) to Add or Remove.

2. Technical Security Administrator adds or removes System access.

3. Functional Security Administrator may add or remove the Employee/Contractor from the ITS mail server distribution list.

SEPARATION PROCESS

The Separation Process is used to remove access when an Employee/Contractor has separated from the university. Access will be removed for all instances.

It is the manager's responsibility to promptly submit ARF requests to modify or remove access for employees experiencing a change in employment status or position duties. As with the New Process, the Requester (the User or Department Representative) is responsible for filling out a portion of the form. The Employee/Contractor's Supervisor/Manager is responsible for the accuracy of that information.

The detailed steps to process a Separation Request are the same as for New Access except:

1. Requester does not need to identify which Enterprise System and Role(s) to disable.

2. Access Grantor step is excluded.

3. Technical Security Administrator removes System access.

4. Functional Security Administrator removes the Employee/Contractor from the ITS mail server distribution list.

USER MASS CREATION PROCESS

User mass creation is typically used when a new system or role is added to the Access Request Process and multiple users require access to that system. A Mass Creation spreadsheet is completed, signed, and submitted by the supervisor. The Mass Creation spreadsheet may also be emailed by the supervisor to arf@help.humboldt.edu. Once received by the Functional Security Administrator, the spreadsheet follows the same process as the Access Request Form (ARF), except that all users are included in one ticket. The

HSU User Name field in KBOX is replaced by the submitter's username and all usernames are pasted into the comments section for tracking purposes.

The spreadsheet can be found at http://www.humboldt.edu/its/po-accessrequest.

GENERIC BATCH ACCOUNT PROCESS

A Generic Batch Account (GBA) is used to run module-specific automated processes. Currently, this process applies only to PeopleSoft HCM. These accounts will be *owned* by the access grantor and distributed for use within their department as the access grantor sees fit. The access grantor/owner is responsible for keeping track of who they have assigned use of the batch account to and to request reset of the password upon departure of any batch account user. Passwords will be reset every 90 days, with the new password issued to the access grantor/owner for distribution to whomever they have currently granted use of the account.

This Account Request process will use the same Access Request Form (ARF) as we do for a regular User Account, but will be recorded in a regular ITS Help Desk system ticket given that the account will not use a standard HSU User Name and so cannot follow the rules of the standard Systems Access Request ticket. The scanned ARF will be saved to an ARF subfolder named 'Generic Batch Account.'

The detailed steps to process a GBA are similar to a regular Account Request:

1. Requester completes an ARF
    a. Name: Name of the Generic Batch Account
    b. HSU ID#: Leave blank
    c. Position: Leave blank
    d. Effective Date: Enter date that access is required
    e. Username: GBA's login name
    f. Extension: Leave blank
    g. Dept Name: Enter Department Name that will use the GBA
    h. Department ID #: Enter the Department Number
    i. Request: Select New, Modify, or Remove
    j. Employee: Leave blank
    k. Roles: Select the Roles
    l. Contact: Optional
    m. Approval: Requester's Manager and Access Grantor
2. Requester submits the Completed ARF to the ITS Functional Security Administrator (GH 209).
3. Functional Security Administrator creates an ITS Help Desk Ticket:
    a. Title: Generic Batch Account <GBA Name>
    b. Impact: Use default
    c. Category: Business Systems | Campus Solutions | Generic Batch Account
    d. Status: Use default
    e. Owner: 4 Programmers
    f. CC List: Access Grantor
    g. Submitter: Requester
    h. Attachment: Scanned ARF
4. Requester and Access Grantor receive the generic automated e-mail notification that the ticket was opened.
5. Technical Security Administrator creates/updates the access and closes the ticket.
6. Requester and Access Grantor receive the generic automated e-mail notification that the ticket was closed.
7. Technical Security Administrator provides the password for the batch account to the Access Grantor.

Appendix A – Sample E-mails

General Ticket Generation E-mail (To Email Submitter)

From: Systems Access Request [arf@help.humboldt.edu -Automatically sent from KBox]

To: Email submitter (ticket owner, usually supervisor)

Subject: [TICK:######] Access Request Received

Content: Your Enterprise System Access Request has been received by ITS Administrative Support and will be processed within 24 hours. Once processed you can expect to receive access within 7 business days. For more information on the Access Request Business Process, please visit http://www.humboldt.edu/its/po-accessrequest.

General Ticket Generation E-mail (To FSA)

From: Systems Access Request [arf@help.humboldt.edu -Automatically sent from KBox]

To: Functional Security Administrator

Subject: [TICK:######] Access Request Received

Content: Access Request received for processing.

General Ticket Change E-mail

From: CMS Access Request [arf@help.humboldt.edu -Automatically sent from KBox]

To: Ticket Owner, User, and Cc List

Subject: [TICK:######] (REMINDER) <HSU Username> <System Abbreviation>

Content: Changed by, Change Date/Time, and Comments

Access Grantor Review Reminder

From: CMS@humboldt.edu [Manually]

To: Access Grantor(s) or their Back-up(s) identified on the ARF who have not approved/declined

Cc: User and User's Supervisor

Subject: CMS Access Request – Ticket 12345 Reminder

Content: A CMS Access Request requiring your review and approval was created several days ago. For complete details follow this link https://help.humboldt.edu/userui/ticket?ID=19829 .

If you need further assistance, please download the CMS Access Request Quick Reference for Access Grantors from http://www.humboldt.edu/its/sites/its/files/docs/cms/DM_QUICK_REF-vert.pdf or contact our office at 707-826-5080.

Thank you.

Sincerely,
The ITS Administrative Support Department

Ticket Completed

From: CMS Access Request [arf@help.humboldt.edu -Automatically sent from KBox]

To: Submitter and User

Subject: [TICK:######] <HSU Username> <System Abbreviation> Access Granted

Content: Your CMS Access Request was completed https://help.humboldt.edu/userui/ticket?ID=19829

For Login, Training, Job Aids, and other Enterprise Systems Information, please visit http://www.humboldt.edu/its/cms-accessrequest

PeopleSoft Finance and PeopleSoft HCM/CS passwords expire at regular intervals. For more information, visit the ITS Password Expiration page at http://www.humboldt.edu/its/security-passwordexpiration

Your ticket will close in one week except if you alert us to a problem.

Ticket Cancelled

From: CMS Access Request [arf@help.humboldt.edu -Automatically sent from KBox]

To: Submitter and User

Subject: [TICK:######] <HSU Username> <System Abbreviation> Cancelled

Content:

Your CMS Access Request https://help.humboldt.edu/userui/ticket?ID=19829 was cancelled because one or more Access Grantors declined to grant access OR the Access Request Form was incomplete. Please see the ticket comments for details.

Please submit a new CMS Access Request Form with the appropriate information. Download the Access Request Form from http://www.humboldt.edu/forms/node/44 and the instructions from http://www.humboldt.edu/its/cms-accessrequest.

Appendix B – Google Groups

Each list must have an owner who decides who should be on the list (outside of who is added/removed in the Access Request process. Each Google Group is owned by the Access Grantor (the Security Google Group is owned by the ITS Project Office).

Business Area	Google Group Name
Finance	hsufinuser
HCM (HR/CS) users	pshcminfo

After the Access Request is closed, the grantee is put on or taken off one of the above ListServs depending on the type of request (New, Modify, or Disable) and what role(s) was granted. Currently this process is done once a week for all of the closed ARFs.

1. Identify the Closed ARFs
   a. Open Kbox (https://help.humboldt.edu/admin)
   b. In the “View by:” drop down select “Switch to Queue” then select “CMS Access Request.”
   c. In the “View by:” drop down select “Custom View” then “Add to listservs.” [Note: The KBox System Administrator must give the user that view.]
   d. Click on the “Custom View” tab (below the search window)
   e. The Filter Name should be “Add to listservs.”
   f. Change the date to when the date prior to the last listserv was updated, then, “test view”.
   g. Click on “Time Opened” column so that the most current date is at bottom of list. Look to see if last ticket number is on list. You will start with the next ticket number on list. If it is, the click on “Save View” tabs.

2. Update the Mailing Lists:

   a. To become Google Groups manager, put in a Help Desk request.
   b. Go to Google Groups and add name(s) to the appropriate list(s)
   c. Google Groups can be found here:

   d. For help see Managing Your Groups (http://www.groups.google.com/support/?ctx=ausers&hl=en)

Appendix C – PS Security List Members

The following people are on the PeopleSoft (Oracle CRM and OBI) Security list serve:

Person	Department	Purpose
Cortney Koors	ITS Administrative Support Department	Functional Security Administrator
Mary Ann McCulloch	ITS Administrative Support Department	Functional Security Administrator (Back-up)
Patricia Ambrosini	Payroll	ARFs are an alternative way for Payroll to know if a staff person has been hired, transferred, or separated.
Sue Peck	Payroll	ARFs are an alternative way for Payroll to know if a staff person has been hired, transferred, or separated.(Back up)
Ken Rocha	ITS Specialized Apps	Technical Security Administrator (Finance)
Jesse Clark	ITS Application Development	Technical Security Administrator (Back-up for Finance)
Ken Thrift	ITS Application Development	Technical Security Administrator (Campus Solutions, CRM, Human Resources)
Liz Villarreal	ITS Application Development	Technical Security Administrator (Campus Solutions, CRM, Human Resources)
Cade Webb	ITS Specialized Apps	Technical Security Administrator (Back-up Finance) Why two backups for Finance? Remove?
Jeff Stebbins	EDM	Technical Security Administrator (OBI)
Peter Johnson		EDM Database Administrator
Holly Aitken	EDM	Technical Security Administrator (OBI)

Appendix D – ARF Folder Access

ARF folder access is limited to the ITS Administrative Support team. All ARFs that are scanned into this folder are also saved to their associated KBOX ticket and can be accessed by searching in the CMS Access Request queue. Any inquiries related to viewing ARFs in the folder can be directed to the Functional Security Administrator.

Appendix E – Quarterly Audit

System Access Review Procedures

Quarterly, the IT department will run queries that identify access to all Peoplesoft modules, including Finance and Human Capital Management by module (Student Financials, Financial Aid, Student Records, Admissions, Academic Personnel Services, Human Resources and Housing).

IT will send the queries showing system access to the appropriate Access Grantor and their designated department employee who will perform the review of access.

Once the department employee performs their review, they will send an email to the Access Grantor confirming that their review is complete and access to the module's information is appropriate.   If during the review process access is identified that needs to be modified, the department Access Grantor will work with IT and follow the Access Request Process (http://www.humboldt.edu/its/sites/its/files/docs/cms/CMS_AccessRequestProcess.pdf) to modify.

Appendix F – Create Ticket

Title: Leave blank since it is automatically generated. The format is: <Action> <HSU Username> <Application> (for example: ARF Modify JLJ7002 CS)

Category: Select New, Modify, or Remove (based on the ARF)

Status: Use default (Pending)

Priority: Use default (Medium) unless there is a valid business need to change to High

Owner: Unassigned (default). Owner is automatically changed to Functional Security Administrator once the ticket is saved.

System 1 – 7: Select up to seven different systems (see list in Appendix I). If two Access Grantors are needed for one System, put in a System line for each Grantor. If Business Unit, Enterprise System, and Access Grantor are the same with more than one role, only one System line is needed.

Status (for Systems 1-7): Select 'FSA Reviewed.' If User's Supervisor is also the Access Grantor, then select 'Access Grantor Approved' and leave a note in the comments box stating that the Access Grantor approved as the User's Supervisor.

HSU User Name: Enter the User's HSU Alpha//Numeric User Name i.e. abc123

Due Date: 'None' (default) unless a specific Due Date was identified on the ARF

CC List: Enter each Access Grantor (or Back-ups if the Access Grantors are unavailable)

Submitter: Select the Contact. If blank, use the User's Supervisor.

See Also: Use default

Referrers: Use default

Resolution: Use default

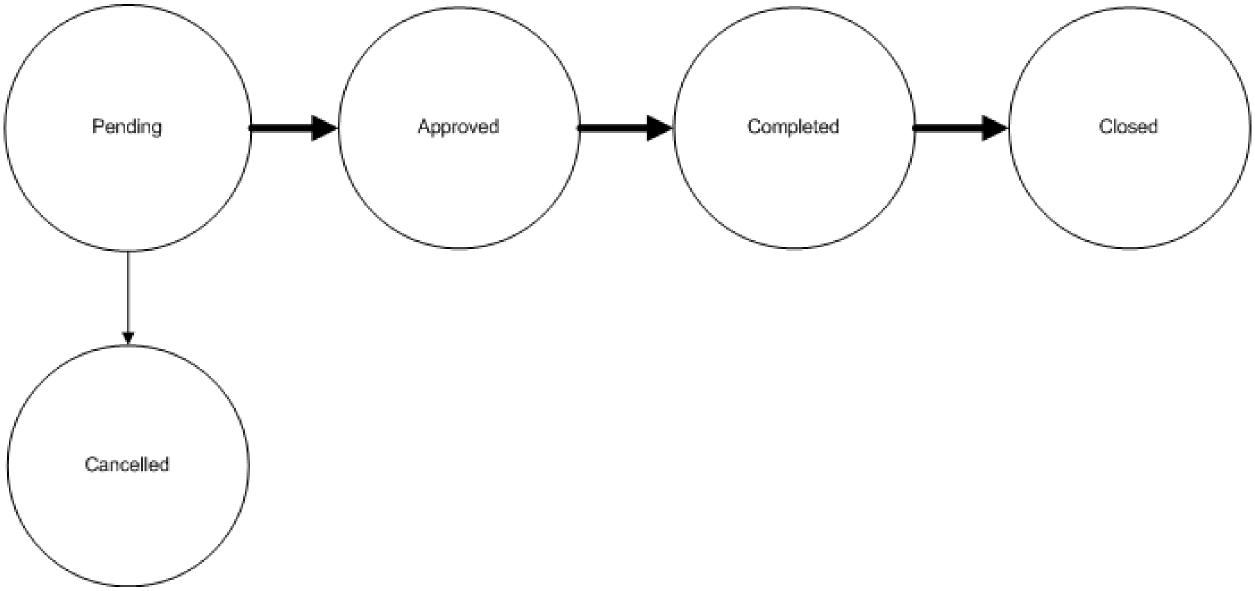
Owner's Only: Unchecked (default). Ignore-not used in the ARF process.

KB article lookup: Ignore-not used in the ARF process

Comment:

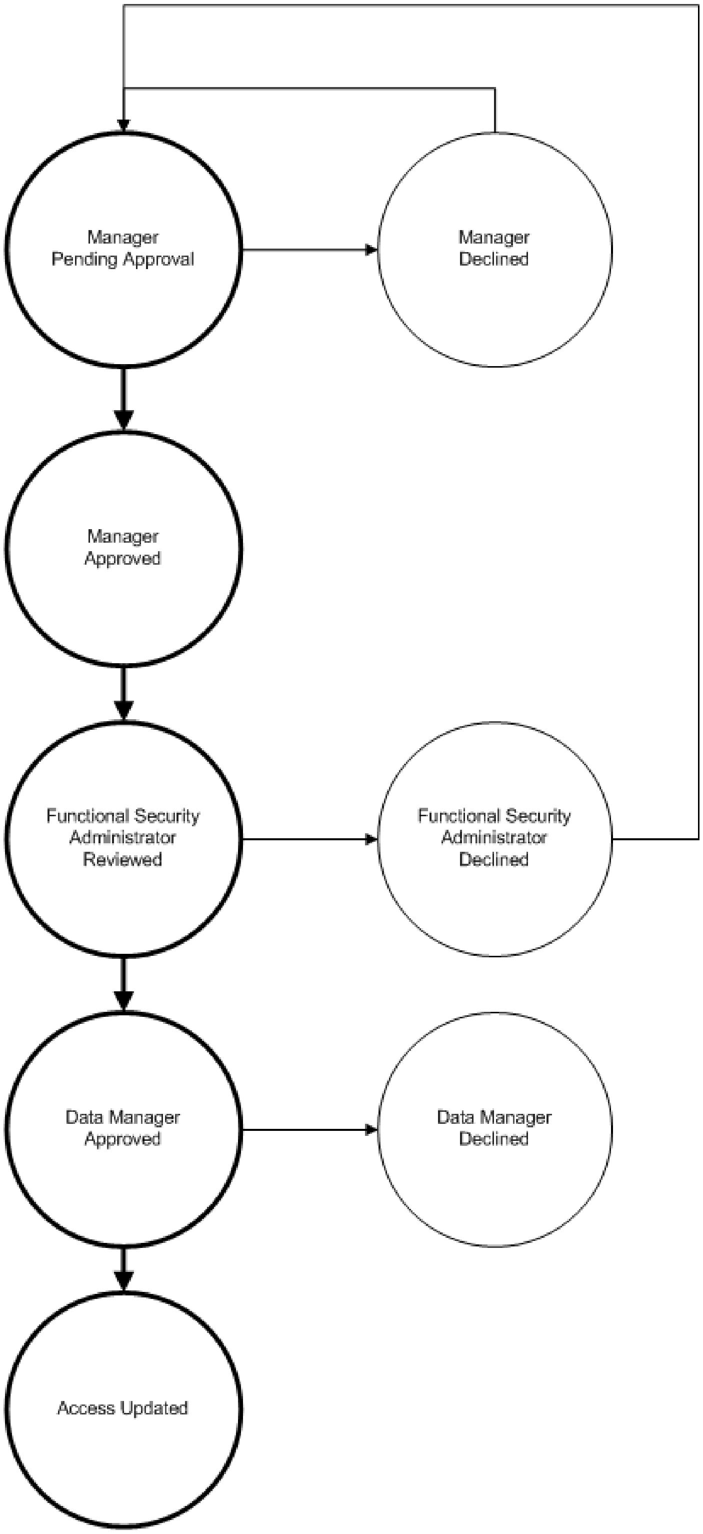
Attachment: Select the Scanned ARF from the Access Request folder

Appendix G – Ticket Status



1. **Pending:** Ticket Status from Ticket creation until either Approved or Cancelled by Access Grantor.
2. **Approved:** All Access Grantors have approved the request, ticket moves to Technical Security Administrator (Ken Thrift or Ken Rocha).
3. **Completed:** Ticket Status when all selected systems have Ticket Workflow status of 'Access Updated.'
4. **Closed:** Ticket Status automatically set fourteen days after the ticket was completed.
5. **Cancelled:** Ticket Status automatically set when any Access Grantor declines the request.

Appendix H – Ticket Workflow Status



Appendix I –Ticket Systems and Categories

This is the initial list of CMS systems and categories. The systems let the TSAs identify which Access Request tickets that they need to respond to. The System/Category combination lets the Access Grantors know which high-level access they need to approve (actual access is in the Access Request Form). Reference the ARF Access Grantors List (Final version October 2, 2009).

1. BAN - Banner
2. CS - Academic Personnel
3. CS - Admissions
4. CS - Financial Aid
5. CS - Housing
6. CS – Student Financial Services
7. CS - Student Records
8. DARS - Advising
9. FIN – Advancement
10. FIN - Finance
11. FIN – Sponsored Programs Foundation
12. HC – Health Center
13. HOB - Hobsons
14. HR - Academic Personnel
15. HR - Sponsored Programs Foundation
16. HR - Human Resources
17. OBI - DARS
18. OBI - OBI Finance
19. OBI – Finance ADV
20. OBI – Finance SPF
21. OBI - Human Resources
22. OBI - APS
23. R25 - Resource 25
24. NLJ – Nolij

Appendix J –Access Request Information

The following information is available via the FAQ link on the ITS Project Office's web site https://www.humboldt.edu/its/cms-accessrequest

Process Timing

It may take up to five business days to process an Access Request (From the time that the ITS Project Office receives the completed Access Request Form to the time that access is granted). The Access Grantors have up to three business days to review and approve the request and the Technical Security Administrators have up to two business days to create or modify the access.

Login

Go to the appropriate system (see links below) and then log in using your HSU user name and password.

PeopleSoft Finance

- Go to the CSU Portal https://portal.calstate.edu
- Select 'Humboldt' from the list of campuses
- Enter your HSU User Name and Password on the CSU Connect page
- Click on the Production link at the left hand side of the CSU Portal's Financial Services page (under the CFS Login heading).

PeopleSoft HCM (Campus Solutions, Human Resources, Student Center, Faculty Center)
https://cmsweb.humboldt.edu/psp/HHUMPRD/?cmd=login

OBI (Finance and Human Resources Data Warehouse)https://obi.humboldt.edu

Training and Job Aids

- **Training and Professional Development web site (classes and job aids)** http://training.humboldt.edu
- **Confidentiality Statement?**
- **Signature Authority**
- **Other security?**
- **Faculty / Advisors** – Faculty Center Help at http://humboldt.edu/facultycenter
- **Students -** – Student Center Help at http://humboldt.edu/studentcenter

Need more help?

- Submit a Support Request through the ITS Help Desk ticketing system http://help.humboldt.edu/
- If you have questions about how to use the system, please refer to the Training and Job Aids above or contact the appropriate business person:
  - Requisitions: Procurement at x3512
  - ProCard: Procurement at x3512.
  - Financial Services Business Department http://www.humboldt.edu/businessservices/
  - Human Resources http://www.humboldt.edu/hsuhr/employee/directory/
  - Academic Personnel http://www.humboldt.edu/aps/staff.html

- Campus Solutions http://humboldt.edu/studentcenter/depts.html

System Availability

- Check the current system availability, visit the ITS homepage at http://humboldt.edu/its/systat .
- Scheduled down times are listed at http://humboldt.edu/its/servermaintenance.
- Receive an email when a system is unavailable; Subscribe to Google group, see appendix B.

Password Expiration

Passwords expire at regular intervals. For more information, visit the ITS Password Expiration page at http://humboldt.edu/its/security-passwordexpiration.

GLOSSARY

Data Owner (from calstate.edu glossary http://www.calstate.edu/icsuam/glossary/def.shtml**)**
Person identified by law, contract, or policy with responsibility for granting access to and ensuring appropriate controls are in place to protect information assets. The duties include but are not limited to classifying, defining controls, authorizing access, monitoring compliance with CSU/campus security policies and standards, and identifying the level of acceptable risk for the information asset. A Data Owner is usually a member of management, in charge of a specific business unit, and is ultimately responsible for the protection and use of information within that unit.

Access Grantors are delegated by Data Owners or if there is no one delegated are the Data Owners themselves.