

Attribute Access Request

August 14, 2006

Person making request: (Must be the Senior Business Officer, Chief Information Officer, or other appropriate senior-level administrator in the requesting department.)

Name	Title
Email address	Telephone number
Requesting Department	

Manager of the application for which data is requested:

Name	Title
Email address	Telephone number

Application

Name
Brief Description

Users - Affiliations/Roles entitled to use the application

Affiliations/Roles	In Requesting Dept Only	In Both Requesting Dept and Other Depts	Outside Requesting Dept
Faculty			
Staff			
Undergraduate Students			
Graduate Students			
Sponsored Users/Guests			
Department/Group/Shared Accounts			
Other, explain:			

Will there need to be exceptions to the categories above?

Please explain any <u>Inclusions</u> :
Please explain any <u>Exclusions</u> :
Who determines which exceptions are allowed?
Who will act as administrator for implementing those decisions (i.e., assigning roles and managing exception groups)?

Attribute Data Requested

List the attribute information for which access is requested:

How will the application use this information?

Will the application need to access FERPA-protected student information or other sensitive or private information about students or employees? Yes No

Technical Information

Discretionary Role Assignment:

- Is there a need to assign roles to individual account holders (e.g., department chairs having a higher level of access than other faculty)?
Yes No
- Will some account holders require multiple roles simultaneously?
Yes No

If yes, specify and explain the valid role values:

Policy Agreements

- The person making the request and the application manager assume personal responsibility for the enforcement of USC policies regarding the use of personal information.
- All communications to the directory must be over SSL.
- Service account name and password should be stored externally to the application, not embedded in code.
- Attributes retrieved from the directory cannot be published or searchable within the application.
- The service account name can only be used by the application to which it is assigned.
- If the security of a service account password is compromised it will be changed at first opportunity.
- Attribute release agreements will be reviewed at least every two years.
- Attribute release agreements may be terminated at any time if any of the policy agreements are broken.

Submission Procedure

To accept these Policy Agreements and submit this request, select one of the following options:

1. Email - The requester (not the administrator) submits the completed form as an attachment to an email message that contains the following language:

I am forwarding an Attribute Release Request from (name of department, school or other organization unit) for (application name). I have read and accept the Policy Agreements listed on page 3 of the request form.

The email message should be addressed to harringt@usc.edu.

2. Paper - The requester signs and dates the completed form at the bottom of page 3, and forwards it to Margaret Harrington, UGB 117, MC 8013.