HARVARD UNIVERSITY
Information Technology
IDENTITY & ACCESS MANAGEMENT

Directory and Security Services

Confidential Information Access Request

Complete this form as the first step in gaining access to confidential information for your application or service.
Questions? Email iam_help@harvard.edu.

Customer Information

School/Business Unit: **Department:**

Requestor: Harvard employee requesting access to Harvard core system information.

Name: Harvard email:

Business Owner: The person who commissioned your application(s) and is responsible for defining scope; he/she works with app technical team and IAM in formulating what information is sent from IAM services to the application(s).

Name: Harvard email:

Application Owner: The lead contact specifically for the application(s).

Name: Harvard email:

Security Contact: The person responsible for managing security for your application(s).

Name: Harvard email:

Operations Contact: The individual responsible for day-to-day operations of your application(s).

Name: Harvard email:

Technical Contact: The person responsible for the overall architecture and implementation of your application(s).

Name: Harvard email:

Generic Email: A generic email address (for service-related notices) that will not change with turnover of personnel.

Email:

About Your Application(s)

If you are submitting details for multiple applications or services, please submit a separate form for each one.

What is your name for the application requiring confidential information?

Briefly describe your application and its purpose (i.e. intranet, web app for students, etc.)

Is this application used for people to see information about themselves or about others? ☐ Self ☐ Others ☐ Both

Does the application generate reports that others will see? ☐ Yes ☐ No

What data source will you be using? ☐ IdM System ☐ Other (specify):

(continued on page 2)

Which identity-related fields will the application need, and how are they to be used? *Check all that apply.*

Data Object IdM	Display info?	Need info?	User can see about others?	User passes on to others?
Name (official and/or listing)	☐	☐	☐	☐
Date of birth	☐	☐	☐	☐
Person detail (SSN, gender, special status)	☐	☐	☐	☐
HUID number	☐	☐	☐	☐
ID card reissue digit	☐	☐	☐	☐
ID card type, expiration date	☐	☐	☐	☐
Address (office, mail, residence)	☐	☐	☐	☐
Phone (voice, fax, office, residence, mobile)	☐	☐	☐	☐
Email (official, others)	☐	☐	☐	☐
Employee role (HR department, employee class, employee status)	☐	☐	☐	☐
Employee job code	☐	☐	☐	☐
Library borrower role	☐	☐	☐	☐
Person of Interest role	☐	☐	☐	☐
Student role (school, student status, expected graduation, last date of attendance)	☐	☐	☐	☐
Student details (degree, special program, board plan, house)	☐	☐	☐	☐
Privacy data	☐	☐	☐	☐
FERPA status	☐	☐	☐	☐

Can non-Harvard users use the application to view confidential information? ☐ Yes ☐ No

Does the application gather or modify personally identifiable information about Harvard people? ☐ Yes ☐ No

If yes, what information is collected? Is this info used to update Harvard core databases?

Does the application retrieve data in real time on an as-needed basis (i.e. LDAP), or does it cache the information locally?

☐ Real-time ☐ Cache ☐ Both

If there is a cache, how often is it refreshed?

Is the application in production? ☐ Yes ☐ No

(continued on page 3)

Authentication and Authorization

If your application is PIN-enabled, what is the name ("application code") by which the PIN server knows your app?

If your application is not PIN-enabled, what user authentication method is used ...

For normal users? ☐ Local password ☐ LDAP ☐ Other (specify):

For administrators? ☐ Local password ☐ LDAP ☐ Other (specify):

Do your passwords meet the most recent criteria set out in HUIT policy (*see http://security.harvard.edu/pages/password-rules*)?

☐ Yes ☐ No ☐ N/A

How do users who can see info about others become authorized to use this app? *Choose all that apply.*

☐ App owner adds users ☐ Directory information about users automatically authorizes

☐ Delegated authorization by owner ☐ Other (specify):

How do administrative users become authorized? Choose all that apply.

☐ App owner adds users ☐ Directory information about users automatically authorizes

☐ Delegated authorization by owner ☐ Other (specify):

Does authorization automatically change when the user's status changes? ☐ Yes ☐ No

If yes, choose a method: ☐ AuthProxy ☐ LDAP (real-time check) ☐ IdDB (at least daily check)

☐ Other (specify):

If no, please explain:

How do you expect to get data in an encrypted manner?

☐ TLS ☐ SSL ☐ SFTP ☐ SCP ☐ Other (specify):

When a user accesses data, is it encrypted? ☐ Yes ☐ No

If yes, choose a method: ☐ TLS/SSL ☐ Other (specify):

If no, please explain:

(continued on page 4)

Environment

Where is the server environment/who is responsible for server maintenance?

☐ UIS Ops Center at 60 Oxford ☐ FAS Computer Services ☐ Other (specify):

Who maintains the application?

☐ UIS ☐ FAS Computer Services ☐ Other (specify):

Names and IP addresses of the machines:

Development name:	Development IP:
Test name:	Test IP:
Production name:	Production IP:
Other name:	Other IP:

Does the network design and computer configuration/operation meet HUIT security setup and operational requirements (*see policy.security.harvard.edu/everyone#widget-1 and policy.security.harvard.edu/all-servers*)? ☐ Yes ☐ No

What individual roles (i.e. system administrator) will have accounts on the computer other than the application user?

Who will know the password for the application to retrieve the data from us? *List all names.*

Acknowledgement & Signature

I certify that the information described above is accurate to the best of my understanding and that, if any information changes at a later date, I am responsible for re-submitting an amended form as appropriate.

Signature of Harvard requestor (must be employee) **Date**

Submitting this form from a harvard.edu email account does not require a signature.