IAM Integration Onboarding Request

## Introduction to the IAM Integration Request Form

*This form is intended for the contracted* ***vendors*** *of university departments whose software requires EID authentication or access to directory information.*

*The* ***requestor*** *must be a university employee. This form should be filled out by the* ***vendor*** *and returned to the* ***requestor*** *for submission.*

 *Fields marked \* are required. Failure to fill out these fields will result in delays in the processing of your request.*

Contact Details

**Technical Contact(s):** The main developer and others knowledgeable about the technical implementation. These are the point people for integrating your application with IAM services and points of contact in the event of a technical incident. \*

* Name \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
* Department \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
* Email Address \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Provide a second technical contact.

* Name \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
* Department \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
* Email Address \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

## About Your Application - The Basics

What is the name of your application? \*

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

What is the public-facing name of your application (if it differs from the field above)?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Please describe the purpose of your application: \*

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

What is the anticipated go-live for the authentication integration for this application? \*

*Please note that the typical turnaround time to onboard a new authentication integration is 4-6 weeks. This time may increase to 10-12 weeks during times of high demand (e.g., before the start of a new semester).*

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

## About Your Application - Vendor Information

What is the name of the vendor?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

## Application Administration - Your Customers

Please describe the user populations your application will serve (e.g., alumni, students, UT faculty, etc.): \*

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Will your application authenticate guests (e.g., external users from other universities, prospective students, summer camp attendees, etc.)? \*

* Yes
* No

## Application Administration - Integration Technologies

Our supported authentication protocol is Security Assertion Markup Language (SAML) v2.0. Is this acceptable? \*

* Yes
* No

|  |
| --- |
| If Security Assertion Markup Language (SAML) v2.0 is not acceptable, please explain why.\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |

## Application Administration - Customer Identifier

*We offer the following primary identifiers:*

***UT EID*** *- The official public records identifier for the university.
Format: 2-8 characters, alphanumeric as well as hyphen (-), underscore (\_), and period (.).*

***eduPersonPrincipalName (ePPN):*** *Part of the* [*eduPerson*](https://refeds.org/eduperson) *LDAP schema.
Format: <eid>@utexas.edu*

***Institutional Identifier (IID):*** *Designed for use with cloud-based services whose usernames are e-mail addresses. When used as an email address, will forward to the user's email address on record. Not available for guest-class EIDs unless they possess a special entitlement.
Format: <eid>@eid.utexas.edu*

Which primary identifier do you want to use? \*

* UT EID
* eduPersonPrincipalName (ePPN)
* Institutional Identifier (IID)
* None of the above

|  |
| --- |
| If you have selected “None of the above” please explain why:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |

*In the uncommon scenario where an end user changes their UT EID, this will cause the UT EID, ePPN, and/or IID we send you when this end user authenticates to be different. This may result in the end user becoming disconnected from their data or their authorizations in your system. Since this scenario can and does happen, it is important that you have considered how your system will handle this situation when it arises.*

**Acknowledgment:** I understand that EIDs can change and confirm that we will develop and document a process for addressing and accounting for changed or merged EIDs. \*

* I understand and confirm.

## Application Administration - Non-Person Accounts

Do non-person accounts need to authenticate? \*

*Non-person accounts include, but are not limited to: Service EIDs, Active Directory Service Accounts, Device EIDs, etc.*

* Yes, we will authenticate non-person accounts.
* No, we will only authenticate person accounts.

|  |
| --- |
| If non-person accounts will authenticate:Please explain how these accounts will authenticate. \*\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_If non-person accounts will authenticate, please acknowledge the following:**Acknowledgment:** I understand and confirm that we are using non-person accounts to authenticate, and we will therefore develop and document a process for managing non-person these non-person accounts. \** I understand and confirm.
 |

## Application Administration - Provisioning

How will user accounts be provisioned for this application? \*

*On-demand provisioning - Accounts will be created automatically the first time users log into the application.*

*Pre-provisioning - Accounts will be created manually by the vendor or application owner prior to users logging into the application.*

* Accounts will be provisioned "on-demand."
* Accounts will be pre-provisioned manually.

|  |
| --- |
| If you will pre-provision accounts manually, please acknowledge the below:**Acknowledgement:** I understand and confirm that we will develop and document a process for provisioning initial and future accounts. \** I understand and confirm.
 |

**Acknowledgement:** I understand and confirm that users will not be allowed to update their attributes within the application. \*

* I understand and confirm.

**Acknowledgment:** I understand that IAM does not deactivate or de-provision EIDs and I confirm that we will develop and document a process for de-provisioning accounts. \*

* I understand and confirm.

## Application Administration - Local Accounts

Will any accounts authenticate locally? \*

*For example, does your application have any accounts that will not use SAML to authenticate? This may include local administrator accounts.*

* Yes, at least one account will authenticate locally.
* No, no accounts will authenticate locally.

|  |
| --- |
| If at least one account will authenticate locally, please acknowledge the following:**Acknowledgment:** I understand and confirm that we will develop and document a process to manage access to local accounts and their credentials. \** I understand and confirm.

**Acknowledgment:** I understand and confirm that we will ensure that local passwords comply with UT password policies at documented at <https://security.utexas.edu/policies/irusp#standard15>. \** I understand and confirm.
 |

## Application Administration - Authorization

What groups of people will be authorized to use your application? \*

*For example: current students, staff, or faculty, prospective students, members of a certain department, etc.*

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

How will you validate that a user is authorized to use your application? \*

* SAML assertion
* LDAP query
* Matching against pre-provisioned accounts
* Other

|  |
| --- |
| If you selected “SAML assertion”, please answer the following:Q101 Is your application capable of making authorization decisions based on SAML attributes?* Yes
* No
 |

|  |
| --- |
| If you selected “Other”, please explain:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |

Can authorizations be managed through an external API? \*

* Yes
* No

|  |
| --- |
| If you indicated that authorizations can be managed through an external API, we recommend that you submit a request using the link below to determine if SailPoint can manage and audit authorizations programmatically for your application.  [https://ut.service-now.com/sp?id=ut\_bs\_service\_detail&sys\_id=c2033a1b37e3fec03952de7543990ed7](https://ut.service-now.com/sp?id=ut_bs_service_detail&amp;sys_id=c2033a1b37e3fec03952de7543990ed7) |

I understand and confirm that we have developed and documented a process for provisioning and reviewing authorizations on a regular basis.

* I understand and confirm.

I understand and confirm that we have developed and documented a process for responding to authorization audits.

* I understand and confirm.

## Requested Attributes - Overview

Regarding Attributes

The central identity management systems consolidate user attributes from a number of primary systems on campus. These attributes include identifiers, names, associations, student information (if applicable), employee information (if applicable), addresses, telephone numbers, credentials, and more.

Identifiers

If you only need an identifier for the end user, you will likely only need the UT EID, the eduPersonPrincipalName (ePPN), or the [Institutional Identifier](https://ut.service-now.com/sp?id=kb_article&amp;number=KB0011278) (IID).

|  |  |
| --- | --- |
| Identifier | Format |
| uid (utexasEduPersonEid) | *<ut\_eid>* |
| eduPersonPrincipalName | *<ut\_eid>*@utexas.edu |
| Institutional Identifier (IID) | *<ut\_eid>*@eid.utexas.edu |

**Note:** The Institutional Identifier can also be used as an e-mail address.

Additional Attributes

However, you may also need additional information. For example:

* **Display Name** - The full, preferred name for the user associated with the identifier. For example: Jane O Doe
* **UT EID Affiliation Code** - A multi-value field which represents how the holder is associated with the university (e.g., current student, former employee, future faculty, etc.) For example: 0SDCU The full list of available attributes is available on the [TED Directory Attributes](https://pages.github.austin.utexas.edu/eis1-iam/ted-schema/) article.

Commonly Requested Attributes

Here are some of the attributes commonly requested by our customers. These are explained in greater detail in the TED Directory Attributes article linked to above:

* **uid, utexasEduPersonEid** - The UT EID, the preferred public identifier for the university.
* **displayName** - The full, primary or "preferred" name.
* **utexasEduPersonAffiliation** - A list of affiliations with the university. For example: student-current, employee-former
* **utexasEduPersonAffCode** - The same as the above, but in an abbreviated format. For example: 0SDCU, 0EMFM.
* **eduPersonPrimaryAffiliation** - A single value field indicating the holder's primary affiliation with the university.
* **mail** - The holder's official email address on record. The Institutional Identifier (IID) is generally sufficient, and can be used as an email address for most individuals.
* **inetUserStatus** - The account status. For example: Active or Inactive.
* **utexasEduPersonAttrRestrict** - A list of attributes which the identity holder has restricted from public release.
* **utexasEduPersonRecordRestrict** - An attribute that indicates that the entire record has been restricted from public release.

### Restricted Data

Some of these attributes are available to you upon request. Others contain data which is owned by a particular unit at the university and will require their prior approval before we can release those attributes to you.

For example, information about an individual's Display Name can be released upon request, but the release of a student's class information will need to be approved by the Office of the Registrar in order to ensure that the business needs comply with university policies as well as local and federal law.

### Additional Reading

For more information regarding the data attributes available, please consult the following knowledge articles. Understanding the information in these articles is optional and not a prerequisite for completing this request:

* [TED Directory Attributes](https://pages.github.austin.utexas.edu/eis1-iam/ted-schema/)
* [KB0012250: Understanding the Data in TED](https://ut.service-now.com/sp?id=kb_article&amp;number=KB0012250)
* [KB0013301: TED Access Level, Restricted Data Access, and Query Limits](https://ut.service-now.com/sp?id=kb_article&amp;number=KB0013301)
* [KB0012261: Understanding the urn:mace:utexas.edu Namespace](https://ut.service-now.com/sp?id=kb_article&amp;number=KB0012261)
* [KB0012262: Understanding the urn:mace:utexas.edu:dir Namespace](https://ut.service-now.com/sp?id=kb_article&amp;number=KB0012262)
* [KB0012263: Understanding the urn:mace:utexas.edu:entl Namespace](https://ut.service-now.com/sp?id=kb_article&amp;number=KB0012263)

Requested Attributes - Select Attributes

**Tip:** If you **do not need** an attribute, please consider **not** requesting it. Less data = less risk.

Do you need any attributes other than UT EID/ePPN/IID? \*

* Yes
* No

|  |
| --- |
| If you need other attributes:**Acknowledgment:** As a recipient of attributes other than UT EID/ePPN/IID, I understand that data provided in the assertion must not be distributed beyond the local system and must only be used for the purpose requested in this application. \** I understand.

Select the attributes which you would like to have released to your application. **Please note that any attributes categorized as Public, Auth, or Standard can be selected without any further steps. All other attributes require the data owner’s approval.*** uid, utexasEduPersonEid: Current UT EID
* utexasEduPersonUin: Current UIN
* displayName: Preferred or primary name
* utexasEduPersonAffiliation: Current detailed affiliation
* utexasEduPersonAffCode: UT component code + affiliation code
* eduPersonAffiliation: Current high-level affiliation
* eduPersonPrimaryAffiliation: Current primary affiliation
* inetUserStatus: Status of authentication account
* utexasEduPersonAttrRestrict: Data attributes marked “do not release”
* utexasEduPersonRecordRestrict: Blanket release restriction on record
* utexasEduPersonEntitlementCode: Code values for eduPersonEntitlement
* utexasEduPersonEidClass: EID Class

Additional attributes (please specify):\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |

## Requested Attributes - Requesting Restricted Data

*Restricted data comes in two forms: restricted records and restricted attributes. If an identity has a restricted record, unauthorized systems will not be able to see the entire record - functionally, it will be as if the record does not exist. If an identity has a restricted attribute, unauthorized systems will otherwise be able to see the record, but will not be able to see any restricted attributes - functionally, those attributes will be null.*

Do you need access to restricted data (e.g., student data that has been restricted from public release, access course/class enrollment, employee data that has been restricted from public release)? \*

 **Please note that any restricted data requires the approval of the data owner.**

* Yes, I need access to restricted records and/or attributes.
* No, I do not need access to restricted records and/or attributes.

|  |
| --- |
| If you have indicated that your application requires authorization for restricted records and/or attributes:  **Please describe the business need for this request. \***\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |

## Requested Attributes - Attribute Storage

Please fill this section out if you have requested any attributes beyond EID/ePPN/IID:

Will attributes be stored in a database? \*

* Yes
* No

|  |
| --- |
| If the attributes will be stored in a database, please acknowledge the following:**Acknowledgment:** I understand and confirm that we have developed and documented a process for producing log information in response to an audit. \** I understand and confirm.
 |

## Application Administration - Risk Mitigation

Enter your Identity Assurance Framework Survey ID # \*

If you have not done so already, please complete the [Identity Assurance Risk Assessment Questionnaire](http://iamservices.utexas.edu/integration/identity-assurance-framework/).

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

The Information Resource Use and Security Policy § 4.6 states that administrative functions should be protected by two-factor authentication (2FA). How do you plan to implement this protection? \*

*For more information, see the* [*Approved Multi-Factor Authentication Methods*](https://security.utexas.edu/iso-policies/approved-mfa-methods)*.

Additionally, if your Identify Assurance Framework Survey ID recommends 2FA and you do not want to enable 2FA, the UT Information Security Office (ISO) must review and approve this decision.*

* \*Duo Security (Duo is our recommended two-factor authentication method)
* Another 2FA method
* I do not plan to enable Duo. I understand that this may require ISO review and approval.

|  |
| --- |
| If you chose an option other than Duo Security, please explain.\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |

|  |
| --- |
| If you chose Duo Security, is your Service Provider able to request a custom authentication context?* Yes
* No
 |

##

## Application Administration - Logging and Auditing

What user and system activity logs does the system provide? \*

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

How will logs be shared for security review? For example: manual export (e.g., a zip of logs) or available through an API (e.g., through an integration with Splunk)? \*

*The goal of this question is to determine how your application will export logs to external GRC (governance, risk, and compliance) or SIEM (security incident and event management) systems.*

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Acknowledgment:** I understand and confirm that we have developed and documented a process for producing log information in response to an audit. \*

* I understand and confirm.

## Additional Security Details

What are the security risks associated with your application? \*

*Consider:*

* *Are you storing Personally Identifiable Information (PII)?*
* *Are you dealing with data protected by law or policy (e.g., HIPAA, FERPA, ITAR, etc.)?*
* *How are you protecting the data entrusted to your application?*
* *Who has access to your application?*
* *Who has administrative access?*
* *What are the potential ramifications if an individual obtains access to which they are not entitled?*

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

How would you categorize the data that is handled by your application? \*

*For more information, see the* [*Data Classification Standard*](https://security.utexas.edu/policies/data_classification)*.*

* Classified (formerly Category-I)
* Controlled (formerly Category-II)
* Published (formerly Category-III)

Who is administering your application (i.e., granting access rights)? \*

* Administered by UT personnel
* Administered by a third-party

Where is your application hosted? \*

* Hosted on-premise
* Hosted in a hybrid on-premise/cloud environment
* Hosted in a cloud environment
* Hosted remotely by a third-party

Does your application share infrastructure with any other applications or services? Please include shared services such as a shared MySQL database or a container service. \*

* Yes
* No
* I don't know

Does your application store data on a shared database? \*

* Yes
* No
* I don't know

|  |
| --- |
| If you indicated above that your application stores data on a shared database, please provide more information:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |

Does your application store passwords? \*

* Yes
* No

|  |
| --- |
| If you indicated that your application stores passwords, how are these passwords encrypted and protected?\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |

## Additional Technical Details

Is your application in the [InCommon Federation](https://incommon.org/federation/)?

* Yes
* No

Provide your application's entity ID(s):

*For example: https://huit.UT.edu/cadm\_huit\_identityaccessmgmt/ourCoolRegistrationApp/sp*

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Is your application able to meet our Metadata Requirements?

* Yes
* No

|  |
| --- |
| If your application is unable to meet our Metadata Requirements, please explain why not:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |

*Your metadata file should be hosted online, typically on the web server running your Service Provider software. Please provide us with a publicly-accessible URL (or URLs) where your metadata file can be found.

(****Note:*** *If your Service Provider does not support hosting its own metadata (i.e., only provides a static metadata file), you may be able to host it on a* [*Departmental UT Box*](https://ut.service-now.com/sp?id=ut_bs_service_detail&amp;sys_id=9b345b104f36de0031eb7bcd0210c71b) *and* [*provide us with the link*](https://community.box.com/t5/Using-Shared-Links/Creating-Shared-Links/ta-p/19523)*.)*

* Production instance \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
* Qual instance \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
* Test instance \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
* Additional instance(s) \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

## Vendor Instructions

Please return a completed copy of this form to your contact at The University of Texas at Austin. They will transcribe your responses into a request form to the university’s Identity and Access Management Team.