



Texas A&M Identity Services Data Request

For help with completing this form see http://infrastructure.tamu.edu/identity/access/form_help.html or contact Division of IT Identity Services technical support at idm-support@tamu.edu.

Email the completed form to idm-support@tamu.edu, fax to 979.845.6090, or mail to Identity Management Office, MS 3374.

Requesting Office/Department: _____

Request Type:

Check only one box.

1 Data access via Shibboleth. Enter entityID here ▶ _____

Metadata: Attach or enter URL here ▶ _____

2 Data access via web services. Enter client identifier here ▶ _____

3 Data access via regular data feed.

4 Modify existing data access agreement. Enter existing agreement request number here ▶ _____

Data Details:

5 List data elements being requested. See http://infrastructure.tamu.edu/directory/enterprise_people.html to view a list of data elements stored in the directory. If other data elements are required, send an email to idm-support@tamu.edu with a description of the needed data to determine availability.

6 Target population.

Role. Check at least one box.

Faculty

Staff

Students (enrolled in current semester)

custom: Enter description below ▼

Location. Check at least one box.

TAMU-CS main campus

TAMU-CS School of Law

TAMU-CS Health Science Center

TAMU-GV campus

TAMU-QT campus

custom: Enter description below ▼

7 For each data element requested, describe usage.

Data Access Details:

8 Name and description of application or service that will use Division of IT Identity Services data (only one per access request).

9 Is an SPECTRIM assessment conducted for this application/service? Yes No

10 Data refresh frequency.

11 Contacts for application/service:

	Administrative sponsor	Technical contact/Data access contact
Name		
UIN		
Email		
Title		
Department		
Telephone		

Data Security:

12 Who will have access to the requested data? Describe in detail.

Fill out item 13 if any requested data elements are categorized as non-directory information.

13 Who will be directly responsible for the security of the data?

Data Security Contact(s)

Name	
UIN	
Email	
Title	
Department	
Telephone	

14 Will data be stored locally in any way?

- Yes Go to item 15.
 No Skip items 15-17 and go to item 18.

15 Why is storage of the data necessary?

16 In what form will the data be stored?

17 How long will the data be stored?

Compliance – if data is sent to third-party (externally hosted) application:

- 18 The third-party application is performing an institutional service for which the Local Education Agency (Texas A&M University) would otherwise use employees. Yes No
- 19 The third-party application is under the direct control of the Local Education Agency (Texas A&M University) with respect to the use and maintenance of education records and there is a signed agreement in place. Yes No
- 20 The third-party application is subject to the requirements in §99.33(a) of the FERPA regulations governing the use and re-disclosure of Personally Identifiable Information from education records. Yes No
- 21 The third-party application provides language similar to the information on the tamu.edu site (<http://www.tamu.edu/statements/privacy.html>) about privacy and security. Yes No

Enter URL here ► _____

- 22 The third-party application contains a published statement, visible to the NetID account holder before login, that: Yes No
- a. They have left the Texas A&M University network.
 - b. They are logging into a website hosted by <Service Provider> on behalf of <College/Division/Department> of Texas A&M University.

Enter URL here ► _____

Request Deadline:

Please be aware it takes 2-4 weeks after the request is submitted to Division of IT Identity Services for the request to be processed.

23 By what date do you need the data?

TEXAS A&M IDENTITY SERVICES USER AGREEMENT TO ACCEPT RESPONSIBILITY

- Use of University computing resources is restricted to authorized Texas A&M University business.
- You will be held responsible for any security breach traceable to you or your specific authorization. You will be held liable for any willful misuse or deliberate system damage traceable to you or your specific authorization.
- **Data obtained from Division of IT Identity Services are to be used for the specific purpose stated on this document. This authorization is not transferable to other parties or for purposes not identified by this document.**
- The department authorized for this data will assume the administrative costs to include development and on-going maintenance involved in supplying this data.
- Violation of this agreement may result in disciplinary action or legal action or both.
- **If automated access approved, access will need to be renewed every 2 years.**

The agreement is bound by the Texas A&M Identity Services Acceptable Use Policy, the University FERPA Policy and University Acceptable Use Guidelines

I HAVE READ, UNDERSTOOD AND AGREED TO THE ABOVE TERMS

Requestor Name (Printed)	Supervisor Name (Printed)
Requestor Title	Supervisor Title
Requestor Department	Supervisor Department
Requestor Signature Date	Supervisor Signature Date

For Division of IT Identity Services Use Only

Notes:

Data custodian notes:

Signatures:

HR Data Custodian Approval Date	Student Data Custodian Approval Date
IT Security Signature Date	CISO Signature Date

Date Received	Request Number
Assigned Contact:	