Texas A&M Identity Services CAS Request

This form should only be completed for websites that are **not** in the tamu.edu domain.

For help with completing this form contact 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: Data access via CAS.

Application Details:

1 Name and description of third-party application or service that will use Texas A&M Identity Services data (only one per access request).

2 Is a SPECTRIM assessment conducted for this application/service?   ☐ Yes   ☐ No

3 Enter application URL here ▶ _____

4 Protocol type: https is only protocol allowed for non-tamu.edu sites

5 Application type: ☐ Production (register with cas.tamu.edu)   ☐ Development (register with cas-dev.tamu.edu)

Data Details:

6 CAS Payload: Check only one option

☐ tamuEduPersonNetID and tamuEduPersonUIN (Default)

☐ tamuEduPersonNetID, tamuEduPersonUIN and authenticationMethod (Applications use authenticationMethod to determine if a user is logging in with one-factor or two-factor authentication)

7 Target population.

Role. Check at least one box.	Location. Check at least one box.
☐ Faculty	☐ TAMU-CS main campus
☐ Staff	☐ TAMU-CS School of Law
☐ Students (enrolled in current semester)	☐ TAMU-CS Health Science Center
☐ custom: Enter description below ▼	☐ TAMU-GV campus
	☐ TAMU-QT campus
	☐ custom: Enter description below ▼

8 For each data element received, describe usage by application.

tamuEduPersonNetID:

tamuEduPersonUIN:

Contact Details:

11 Contacts for application/service:
Contact must be an active faculty or staff employee of Texas A&M University.

	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.

13 Will data be stored locally in any way?

☐ **Yes** Go to item 14.

☐ **No** Skip items 14-16

14 Why is storage of the data necessary?

15 In what form will the data be stored?

16 How long will the data be stored?

Compliance:

17 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

18 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

19 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

20 The third-party application provides language similar to the information on the tamu.edu site (https://www.tamu.edu/statements/privacy) about privacy and security. ☐ Yes ☐ No

Enter URL here ▶ _____

21 The third-party application contains a published statement, visible to the NetID account holder before login, that:
   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.**

☐   ☐ No

Enter URL here ▶ _____

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 Texas A&M 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 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:	