Texas A&M NetID Special Purpose Account Request

A NetID Special Purpose Account is an account for a thing: an application, server, printer, or other device. Special Purpose Accounts are also used for providing resources to an organizational unit or role. For help with completing this form, contact idm-support@tamu.edu.

Requesting Office/Department: _____

Account Details:

1 Purpose for account.

2 Official name (title) for account

3 Preferred account identifier

4 Required functionality

Contact/notification address for account ▶ _____

5 Additional functionality (select as many as appropriate)

☐ @tamu.edu email delivery.

Destination address for email:

☐ Same as contact/notification address

☐ Different destination address ▶ _____

☐ Publicly searchable in Campus White Pages Directory Search (Departmental)

☐ Exchange shared mailbox

☐ Exchange resource account

☐ Google Apps for Education account

☐ Authentication Credentials.

Describe how credentials will be used (why they are necessary):

Notifications (password expiration alerts, etc.) will be sent to the destination address specified above for @tamu.edu email delivery.

☐ Single Factor Authentication (Password only) ☐ Two Factor Authentication (Password + Duo Security)

6 Contacts for special purpose account:

	Administrative sponsor	Technical contact(s)	Service Security Contact(s)
Name			
UIN			
Email			
Title			
Department			
Telephone			

Special Purpose Account Security (Account Proxies):

7 Who will have access to the special purpose account? Attach sheet with additional personnel information if needed.

Name	UIN	Role/Responsibilities

TEXAS A&M IDENTITY SERVICES USER AGREEMENT TO ACCEPT RESPONSIBILITY

- Use of University computing resources is restricted to authorized Texas A&M University business.
- Your directory configuration must use encrypted connections for any connecting clients or services.
- You understand that any trust is one-way and non-transitive.
- **You agree to NOT collect and store NetID passwords.**
- 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.
- **You agree to all of the following conditions related to logs and TAMU Directory Services personnel:**
  1. **To deliver, on request, security logs from the directory servers.**
  2. **To provide, on request, access to application logs of any service connecting to the directory servers.**
  3. **To participate in any event correlation/event monitoring solution in use by TAMU Directory Services personnel.**
- Violation of this agreement may result in disciplinary action or legal action or both.
- **If approved, access will need to be renewed annually.**

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 Texas A&M IT Use Only

Notes:

Data custodian notes:

Signatures:

HR Data Custodian Approval Date	Student Data Custodian Approval Date
IT Identity Services Approval Date	CISO Signature Date

Date Received	Request Number
Assigned Contact:	