## **Texas A&M NetID PRO/IT Resource Account Request**



A NetID IT Resource Account is an account for a thing: an application, server, printer, or other device. PRO/IT Resource Accounts are also used for providing resources to an organizational unit or role. For help with completing this form, contact <a href="mailto:idm-support@tamu.edu">idm-support@tamu.edu</a>.

2 Official name (title) for account  3 Preferred account identifier  4 Required functionality				
2 Official name (title) for account  3 Preferred account identifier  4 Required functionality Contact/notification address for account ▶	unt Details:			
3 Preferred account identifier  4 Required functionality Contact/notification address for account ▶	1 Purpose for acc	count.		
3 Preferred account identifier  4 Required functionality Contact/notification address for account ▶				
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 linked mailbox □ Exchange resource account □ Authentication Credentials.  Describe how credentials will be used (why they are necessary):  6 Contacts for IT Resource account:	2 Official name (	title) for account		
S 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 linked mailbox   Exchange resource account   Authentication Credentials.   Describe how credentials will be used (why they are necessary):    Single Factor Authentication (Password only)   Two Factor Authentication (Password + Duo Security)    6 Contacts for IT Resource account:   Administrative sponsor   Technical contact(s)   Service Security Contact     Name   UIN     Email     Title     Department     Telephone     Service Account Security (Account Proxies):   7 Who will have access to the PRO/IT Resource account? Attach sheet with additional personnel information if needed.	3 Preferred acco	unt identifier		
S 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 linked mailbox   Exchange resource account   Authentication Credentials.   Describe how credentials will be used (why they are necessary):    Single Factor Authentication (Password only)   Two Factor Authentication (Password + Duo Security)  6 Contacts for IT Resource account:   Administrative sponsor   Technical contact(s)   Service Security Contact     Name	4 Required funct	ionality		
⊕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 linked mailbox     Exchange resource account     Authentication Credentials.   Describe how credentials will be used (why they are necessary):    Single Factor Authentication (Password only)   Two Factor Authentication (Password + Duo Security)    6 Contacts for IT Resource account:   Administrative sponsor   Technical contact(s)   Service Security Contact     Name	Contact/notific	cation address for account		
⊕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 linked mailbox     Exchange resource account     Authentication Credentials.   Describe how credentials will be used (why they are necessary):    Single Factor Authentication (Password only)   Two Factor Authentication (Password + Duo Security)    6 Contacts for IT Resource account:   Administrative sponsor   Technical contact(s)   Service Security Contact     Name   UIN     Email     Title     Department     Telephone     Telephone     2 Who will have access to the PRO/IT Resource account? Attach sheet with additional personnel information if needed.	5 Additional fund	ctionality (select as many as appro	priate)	
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 linked mailbox  Exchange resource account  Authentication Credentials.  Describe how credentials will be used (why they are necessary):  Single Factor Authentication (Password only)  Two Factor Authentication (Password + Duo Security)  6 Contacts for IT Resource account:  Administrative sponsor  Technical contact(s)  Service Security Contact  Name  UIN  Email  Title  Department  Telephone  esource Account Security (Account Proxies):  7 Who will have access to the PRO/IT Resource account? Attach sheet with additional personnel information if needed.	☐ @tamu.edı	u email delivery.		
Same as contact/notification address  □ Different destination address □ Publicly searchable in Campus White Pages Directory Search (Departmental) □ Exchange shared mailbox □ Exchange linked mailbox □ Exchange resource account □ Authentication Credentials. Describe how credentials will be used (why they are necessary): □ Single Factor Authentication (Password only) □ Two Factor Authentication (Password + Duo Security)  6 Contacts for IT Resource account:				
□ Different destination address □ □ Publicly searchable in Campus White Pages Directory Search (Departmental) □ Exchange shared mailbox □ Exchange linked mailbox □ Exchange resource account □ Authentication Credentials.  Describe how credentials will be used (why they are necessary): □ Single Factor Authentication (Password only) □ Two Factor Authentication (Password + Duo Security)  6 Contacts for IT Resource account:  Administrative sponsor Technical contact(s) Service Security Contact Name □ UIN □ Email □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □				
Publicly searchable in Campus White Pages Directory Search (Departmental)   Exchange shared mailbox   Exchange linked mailbox   Exchange resource account   Authentication Credentials.   Describe how credentials will be used (why they are necessary):   Single Factor Authentication (Password only)				
Exchange shared mailbox  Exchange linked mailbox  Exchange resource account  Authentication Credentials.  Describe how credentials will be used (why they are necessary):  Single Factor Authentication (Password only)  Two Factor Authentication (Password + Duo Security)  6 Contacts for IT Resource account:  Administrative sponsor  Technical contact(s)  Service Security Contact  Name  UIN  Email  Title  Department  Telephone  Resource Account Security (Account Proxies):  7 Who will have access to the PRO/IT Resource account? Attach sheet with additional personnel information if needed.				
Exchange linked mailbox  Exchange resource account  Authentication Credentials.  Describe how credentials will be used (why they are necessary):  Single Factor Authentication (Password only)  Two Factor Authentication (Password + Duo Security)  Contacts for IT Resource account:  Administrative sponsor  Technical contact(s)  Service Security Contact  Name  UIN  Email  Title  Department  Telephone  Describe how credentials will be used (why they are necessary):  Two Factor Authentication (Password + Duo Security)  Service Security Contact  Name  UIN  Email  Title  Department  Telephone			rectory Search (Departmental)	
□ Exchange resource account □ Authentication Credentials.  Describe how credentials will be used (why they are necessary): □ Single Factor Authentication (Password only) □ Two Factor Authentication (Password + Duo Security)  6 Contacts for IT Resource account:  Administrative sponsor Technical contact(s) Service Security Contactor Name □ UIN □ Email □ Title □ Department □ Telephone □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □	☐ Exchange s	hared mailbox		
□ Authentication Credentials.  Describe how credentials will be used (why they are necessary):  □ Single Factor Authentication (Password only) □ Two Factor Authentication (Password + Duo Security)  6 Contacts for IT Resource account:  Administrative sponsor Technical contact(s) Service Security Contactors  Name  UIN  Email  Title  Department  Telephone  1 Department  Telephone  1 Describe how credentials will be used (why they are necessary):  1 Describe how credentials will be used (why they are necessary):  1 Describe how credentials will be used (why they are necessary):  1 Describe how credentials will be used (why they are necessary):  2 Describe how credentials will be used (why they are necessary):  2 Describe how credentials will be used (why they are necessary):  2 Describe how credentials will be used (why they are necessary):  2 Describe how credentials will be used (why they are necessary):  2 Describe how credentials will be used (why they are necessary):  3 Describe how credentials will be used (why they are necessary):  3 Describe how credentials will be used (why they are necessary):  4 Describe how credentials will be used (why they are necessary):  4 Describe how credentials will be used (why they are necessary):  5 Describe how credentials will be used (why they are necessary):  6 Describe how credentials will be used (why they are necessary):  8 Describe how credentials will be used (why they are necessary):  9 Describe how credentials will be used (why they are necessary):  9 Describe how credentials will be used (why they are necessary):  9 Describe how credentials will be used (why they are necessary):  9 Describe how credentials will be used (why they are necessary):  9 Describe how credentials will be used (why they are necessary):  9 Describe how credentials will be used (why they are necessary):  9 Describe how credentials will be used (why they are necessary):  9 Describe how credentials will be used (why they are necessary):  9 Describe how credentials will be used (why they are ne	Exchange li	nked mailbox		
Describe how credentials will be used (why they are necessary):    Single Factor Authentication (Password only)   Two Factor Authentication (Password + Duo Security)    6 Contacts for IT Resource account:	Exchange r	esource account		
Describe how credentials will be used (why they are necessary):    Single Factor Authentication (Password only)   Two Factor Authentication (Password + Duo Security)    6 Contacts for IT Resource account:	☐ Authentica	tion Credentials.		
Single Factor Authentication (Password only)  Two Factor Authentication (Password + Duo Security)  Contacts for IT Resource account:  Administrative sponsor  Technical contact(s)  Service Security Contact  Name  UIN  Email  Title  Department  Telephone  Cesource Account Security (Account Proxies):  7 Who will have access to the PRO/IT Resource account? Attach sheet with additional personnel information if needed.	Describe h	ow credentials will be used (why th	nev are necessary):	
6 Contacts for IT Resource account:  Administrative sponsor Technical contact(s) Service Security Contact  Name  UIN  Email  Title  Department  Telephone  Department  Telephone  Resource Account Security (Account Proxies):  7 Who will have access to the PRO/IT Resource account? Attach sheet with additional personnel information if needed.				
Administrative sponsor Technical contact(s)  Name  UIN  Email  Title  Department  Telephone  Descripted (Account Proxies):  7 Who will have access to the PRO/IT Resource account? Attach sheet with additional personnel information if needed.	ų.	·	nly)	tion (Password + Duo Security)
Name UIN Email Title Department Telephone  esource Account Security (Account Proxies): 7 Who will have access to the PRO/IT Resource account? Attach sheet with additional personnel information if needed.	6 Contacts for		Technical contact(s)	Service Security Contact(
Email Title Department Telephone	Name	•	( )	
Title Department Telephone  esource Account Security (Account Proxies): 7 Who will have access to the PRO/IT Resource account? Attach sheet with additional personnel information if needed.	UIN			
Department Telephone  esource Account Security (Account Proxies): 7 Who will have access to the PRO/IT Resource account? Attach sheet with additional personnel information if needed.	Email			
Telephone  esource Account Security (Account Proxies): 7 Who will have access to the PRO/IT Resource account? Attach sheet with additional personnel information if needed.				
esource Account Security (Account Proxies): 7 Who will have access to the PRO/IT Resource account? Attach sheet with additional personnel information if needed.				
7 Who will have access to the PRO/IT Resource account? Attach sheet with additional personnel information if needed.	Telephone	<u> </u>		
7 Who will have access to the PRO/IT Resource account? Attach sheet with additional personnel information if needed.				
			-	
Name OIN Role/Responsibilities			The state of the s	
		vame UIN	I KOI	2/ Kesponsibilities

## 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 Division of IT Identity 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 Division of IT Identity 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.

Requestor Name (Printed)	Supervisor Name (Printed)  Supervisor Title		
Requestor Title			
Requestor Department	Supervisor Department		
Requestor Signature Date	Supervisor Signature	Date	
For Division of IT Identity Services Use Only			
Notes:  Data custodian notes:			
Signatures:			
ignatures: IT Security Approval Date	CISO Signature	Date	
Signatures: IT Security Approval Date	CISO Signature	Date	
	CISO Signature  Request Number	Date	