

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 domain configuration requires encrypted connections for any connecting clients or services.
- You understand that the trust is one-way, non-transitive trust to only the domain(s) requested.
- **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 domain controllers.**
 2. **To provide, on request, access to application logs of any service connecting to the domain controllers.**
 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.

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:

Signatures:

IT Security Signature Date	CISO Signature Date
---	--

Date Received	Request Number
Assigned Contact:	