VPN Access Request Form
Version 1.3 – Effective 10/31/2021

In accordance with SRSU's Information Security Policy (APM 7.01), Hardware Standards Policy (APM 7.10), and OIT's Guidelines and Standards (https://www.sulross.edu/oit-guidelines-and-standards), all requests for Virtual Private Network (VPN) access credentials must be evaluated and approved by the Office of Information Technology (OIT). VPN access credentials will allow you to access various SRSU software, systems, and files remotely. Please provide the information requested below and email the completed form to ltac@sulross.edu and include "VPN Access" in the subject line.

Requester Info:

Name:	
"A" Number:	
Lobo ID:	
SRSU Email:	
Department:	

Non-SRSU faculty and staff must additionally provide the information requested below:

Company Name:	
Company Email:	
Cell Phone Number:	
Workstation (Win/Mac):	
Workstation OS Version:	
Anti-Virus Software:	
Anti-Virus Software Version:	
Cell Phone (iOS/Android):	
Cell Phone OS Version:	

Please briefly describe and justify your request for VPN access credentials. You may also note the intended purpose/use for the credentials.:

```
[                                                                    ]
[                                                                    ]
[                                                                    ]
[                                                                    ]
```

Terms of Use

By submitting this request, you acknowledge that you understand and agree with the terms of use for VPN access:

- VPN access credentials may be audited for compliance by OIT at any time.
- VPN access may only be granted approval for use on university owned and managed devices.
- Requests for VPN access for use on non-SRSU devices may be reviewed on a case-by-case basis by the CIO, ISO, and/or their designees.
- All workstations used for VPN access must have up to date operating systems, security updates/patches, and anti-virus software. VPN access credentials may be revoked if it is determined that a user is accessing VPN on non-supported operating systems or end-of-life devices.
  Examples of supported and up to date systems, software, and devices are noted below:
    - Windows workstations with operating system 8.1 or higher.
    - Mac workstations with operating system 10.15 or higher.
    - iPhone 6S or newer, Android phone 8.1.x or newer.
    - Licensed anti-virus software from McAfee, Norton, Kaspersky, Bitdefender, Webroot, ESET, Malwarebytes, Microsoft Defender, Trend Micro, Avast, or Sophos may be acceptable.

Requestor Signature:

Date:

THIS SECTION TO BE COMPLETED BY OIT			
Approval Block:			
OIT Director:		**Information Security Officer:**	
Date:		**Date:**	
Chief Information Officer:			
Date:			
LTAC Ticket #:			