POLICY STATEMENT: **NO. 13 30.00**

COORDINATED BY: **Offices of Business Affairs/ Department of Information Technology Services (ITS)**

SUBJECT: **VPN Acceptable Use Policy**

I. Purpose

This policy sets guidelines for Virtual Private Network (VPN) use and VPN connections to the LSUS network.

II. Definition

A VPN securely extends a private network across a public network. This allows secure access to select LSUS resources when not physically located on the LSUS campus.

III. Scope

This policy applies to all LSUS employees, students, contractors, consultants, and other workers including all personnel affiliated with third parties utilizing VPNs to access the LSUS network.

IV. Policy

Only approved LSUS employees, students, contractors, consultants, and other workers including all personnel affiliated with third parties may take advantage of a VPN to access the LSUS network. A user's VPN connection is solely managed by the user, meaning a user is responsible for having internet access, the required hardware, and software to establish a VPN connection.

Additionally,

1. It is the responsibility of authorized users with VPN privileges to ensure that unauthorized users are not allowed access to LSUS internal networks.
2. Remote access VPN use is to be controlled using LSUS ITS approved authentication methods.
3. VPN gateways will be set up and managed by LSUS network operational personnel.
4. All computers connected to LSUS internal networks via VPN or any other technology must use up-to-date anti-virus software.
5. VPN users will be automatically disconnected from the LSUS network after thirty minutes of inactivity. The user must then logon again to reconnect to the network.
6. The VPN concentrator is limited to an absolute connection time of 24 hours.
7. Users of computers that are not LSUS-owned equipment must configure the equipment to comply with LSUS VPN and Network policies.
8. Only LSUS approved VPN clients may be used.

9. By using VPN technology with personal equipment, users must understand that their machines are a de facto extension of the LSUS network, and as such are subject to LSUS Policy Statement 1 17 Computer Access and Usage.

V. Implementation

User will request VPN access by completing the VPN Access Service Request in the LSUS ITS Helpdesk system.

Remote access VPN use is to be controlled using LSUS ITS approved authentication methods.

Users with VPN access are charged with ensuring that unauthorized users are not allowed access to the LSUS network.

Internet traffic destined for LSUS resources will flow through the VPN. Any traffic not associated with LSUS resources will flow through the user's Internet Service Provider (ISP).

Users are responsible for their own ISP and all costs related.

Users must install the VPN client that LSUS provides for access.

Any VPN related issues should be reported to LSUS ITS through the helpdesk or by email to its@lsus.edu.

VI. Enforcement

This policy sets regulations for the use of all VPN services to the LSUS network. Users must comply with the LSUS Policy Statement No 1 17 Computer Access and Usage as well as this policy statement.

In an effort to maintain LSUS security, a user's VPN access may be suspended in the event that suspicious activity is detected. A user's VPN access will remain suspended until outstanding issues have been resolved. Any intentional violation of this policy or LSUS Policy Statement No 1 17 Computer Access and Usage may be subject to disciplinary action, up to and including termination of employment.

AUTHORIZED: Barbara Cummings 11/18/19

Vice Chancellor for Business Affairs **Date**

APPROVED: 11/18/19

Chancellor **Date**