Policy Name	Virtual Private Network
Policy Number	50000.011
Effective Date	March 19, 2019
Administrative Division	Division of Academic Affairs
Unit	Department of Information Technology
Revised Date	February 19,2021

1.0 Policy Statement

The establishment of this policy and procedures sets the standards for the usage of Remote Access Virtual Private Network (VPN) connections by Jackson State University employees.

2.0 Purpose

The purpose of this policy is to provide guidelines for Remote Access Virtual Private Network (VPN) connections to the Jackson State University (JSU) network.

3.0 Definitions

Virtual Private Network (VPN) - a secured private network connection built on top of a public network, such as the internet.

Internet Service Provider (ISP) - a company that provides Internet connections and services to individuals and organizations.

Net ID – a Network Identifier (NetID) number used to access university resources (ie. CANVAS, Xerox Copiers)

4.0 Employee Adherence

This policy applies to all JSU faculty and staff utilizing a VPN to access the JSU network. This policy also applies to implementations of VPN that allow direct access to the JSU network.

5.0 Policy

Approved JSU faculty and staff may utilize the benefits of a VPN, which is a "user-managed" service. This means that the user is responsible for selecting an ISP, coordinating installation, and installing the required software.

6.0 Implementation

6.1   The VPN is an IP only resource. Other protocols are not supported.

6.2   It is the responsibility of the employee with VPN privilege to ensure that unauthorized users are not allowed access to the JSU network.

6.3   VPN access is controlled using ID and password authentication. For Faculty and Staff, the ID is their Net ID and Password.

6.4   All traffic destined for JSU networks is logged and associated with the user, as permitted.

6.5   Only traffic destined for JSU networks will travel across the VPN tunnel, all other traffic will go through the user's ISP.

6.6   Users of this service are responsible for the procurement and cost associated with acquiring basic internet.

6.7 Users request access via email and receive instructions to download the VPN client software and activate your VPN access.

6.8 Users must have an active anti-virus software on the machine they are using to access JSU's VPN.

6.9 Only JSU employees are given access to the JSU VPN and those credentials are not to be shared.

6.10 Any unauthorized access to the JSU VPN by a user who is NOT a JSU employee but found using employee credentials is subject to loss of VPN access up to termination of employment.

6.11 SonicWall is providing the VPN service and the service is supported by the Division of Information Technology Office of Computing and Communications.

6.12 If a problem is encountered please report it to the by phone (**601-979-6400**) or by e-mail to umesh.r.reddy@jsums.edu, with the following information available:

  6.12.1 Net ID
  6.12.2 Date and time of problem
  6.12.3 Any error messages

7.0 Related Standards, Policies, and Processes
  ➢

8.0 Revision History
  ➢ Initial Draft: January 11, 2017
  ➢ Revised: February 13, 2019
  ➢ Revised: February 19, 2021
  ➢