Auburn University at Montgomery
Policies and Procedures

Title: VPN Remote Access Policy

Responsible Office: Information Technology Services (ITS)

I. PURPOSE

The purpose of this policy is to define mandatory standards for connections to the Auburn University at Montgomery (AUM) network from any external source using Virtual Private Network (VPN) technology.

II. POLICY

Increased mobility of AUM faculty and staff have made remote access to centralized University assets increasingly important. Approved AUM users may utilize the privileges of a VPN. VPN access is granted for the sole purpose of completing authorized functions in compliance with all applicable AUM policies and procedures.

The standards set forth in this policy are designed to minimize the potential exposure to AUM from damages which may result from unauthorized use of AUM resources. Damages include the loss of university data, intellectual property, damage to public image, or damage to critical AUM systems.

III. EFFECTIVE DATE

May 1, 2023

IV. APPLICABILITY

This policy applies to all departments, faculty, staff, and student workers, as well as contractors and vendors who remotely access or use AUM information technology resources.

V. RESPONSIBILITY

ITS implements and administers the policy/procedure in detail.

Policy Responsible Office: Information Technology Services
Policy Responsible Executive: Chief Information Officer (CIO)

VI. DEFINITIONS

A **Virtual Private Network (VPN)** is a communications network tunneled through another network and dedicated for a specific network. VPN provides a mechanism to secure communications through the public internet. Use of VPN allows members of the AUM community to securely access AUM network resources as if they were on the campus.

VII. PROCEDURES

General VPN Access Rules and Procedures:

- User access to VPN is subject to an approval process and may only be granted with the combined authorization of the requestor's dean or department head, the custodian of the resources to be accessed, the CIO, and others as needed. The review will determine if VPN access is appropriate for fulfillment of the user's job responsibilities or academic needs and consistent with university data security policies.

- VPN service requires multifactor authentication authorized and provided by ITS.

- It is the responsibility of the user with VPN privilege to ensure that unauthorized persons are not allowed access to their VPN session or credentials.

- All individuals and machines, while using AUM's VPN technology, including university-owned and personal equipment, are an extension of the AUM network and are subject to the University's Information Technology Acceptable Use Policy.

- Normally, AUM does not allow user-owned computers to connect to VPN service. AUM will issue technology resources necessary that are subject to university policies and will employ normal data security practices.

- All network activity during a VPN session is subject to AUM's policies.

- VPN users will be automatically disconnected from the AUM network after 30 minutes of inactivity. The user must then login again to reconnect to the network.

- VPN access and use by contracted personnel, and/or individuals authorized by affiliated institutions and organizations who access or use AUM information technology resources requires a written agreement defining the rules security controls that must be maintained and the terms and conditions for sharing data and information resources.

- VPN accounts shall be reviewed by ITS each semester.

- ITS reserves the right to disable VPN access for users who have not used VPN within the last 6 months.

- VPN access may be terminated at any time for reasons including, but not limited to, termination of service provided agreements, changes in or termination of employment, request by the system/data owner, non-compliance with IT policies, negative impact on overall network performance attributable to VPN communications, or at the discretion of senior administration.

- VPN access and authentication shall comply with normal network access policies and procedures.

VPN Request Procedures:

- Detailed VPN Request Procedures can be found on the ITS SharePoint site.

VIII. SANCTIONS

Employee violations of this policy or the protection standards created to implement this policy may be considered a Group I infraction under the University Personnel Manual and may be subject to disciplinary action, up to and including dismissal. Violations may others may be subject to other sanctions, including termination of contractual relationships.

IX. EXCLUSIONS

NONE

X. INTERPRETATION

The AUM Chancellor has the authority to interpret this policy.

APPROVAL TO PROCEED: ____________________ **DATE:** 4/18/23

APPENDICES

NONE