Policy Title	Remote Access Policy
Responsible AIU Office (Higher Management/Directorate)	Chief Information Officer (CIO)
Policy Owner (Executive Department/Office)	Information Technology Department IT Security Office
Pertinent Dates	July 2022

I. SCOPE OF POLICY

The purpose of this policy is to define standards for the usage and establishing a secure remote access to computing resources hosted at Southern University using Virtual Private Network (VPN).
These standards are designed to minimize any security adversity that may cause any potential damage to AIU network or assets from which may result from unauthorized use of the university's resources.

This policy applies to all authorized users with a university owned or personally owned computer or workstation used to connect to the Southern University network through VPN.
This policy applies to remote access connections used to do work on behalf of AIU, including reading or sending email and viewing intranet web resources.
Remote access implementations that are covered by this policy include, but are not limited to, dial-in modems, frame relay, ISDN, DSL, VPN, SSH, cable modems etc.

II. DEFINITIONS

Remote Access - Methods allowing authorized users to interact with university information systems and networks via methods or networks not controlled by the university (e.g. the Internet). Examples of remote access include Virtual Private Networks (VPN), remote desktop and terminal sessions.

Virtual Private Network (VPN) - In order to access computing resources hosted at AIU from off-campus, the use of a Virtual Private Network (VPN) is required. A VPN is a secured private network connection built on top of a public network, such as the Internet. A VPN provides a secure encrypted connection or tunnel over the Internet between an individual computer and a private network. Use of a VPN allows authorized members of AIU to securely access the university network resources as if they were on campus.

III. POLICY STATEMENT

- All methods the university provides to offer remote access to services and information systems must be assessed for security, approved, documented and controlled. The university will permit external network access only to approved remote access end points.
- Remote access methods must employ appropriate security technologies to secure the session, as well as prevent unauthorized.

- It is the responsibility of all authorized users with VPN privileges to ensure that unauthorized users are not allowed access to internal university networks and computing resources.
- All individuals and computers, while using the University's VPN, including university-owned and personal equipment, are an effective extension of AIU's network, and as such are subject to the university's Acceptable Use Policy.
- All computers, university-owned and personally-owned, connected to the university's internal network via the VPN or any other technology must use a properly configured up-to-date operating system and configured up-to-date anti-virus software.
- Redistribution of the university's VPN installer or associated installation information is prohibited.
- All network activity during a VPN session is subject to the university's policies.
- All authorized users of the university's VPN will only connect to or gain access to machines and resources that they have permission and rights to use.

IV. RESPONSIBILITIES

- All AIU members are responsible for protecting remote access methods, devices and credentials assigned to them. Users are responsible for maintaining the security of computers and devices used to remotely access university resources.
- Information Security Engineers are responsible for documenting and implementing controls for all remote access methods implemented within their unit. ISMs are also responsible for monitoring of unit-implemented remote access methods for unauthorized use, and taking appropriate action upon discovery of unauthorized use, including notification of the Information Security Incident Response Team.
- The Chief Information Officer (CIO) is responsible for approval of remote access methods and resources.
- The and Chief Information Officer (CIO) is responsible for implementing systems and specifications to facilitate unit compliance with this policy.

V. POLICY STANDARDS AND PROCEDURES

- Secure remote access must be strictly controlled. Control will be enforced via one-time password authentication with AIU Username and password.
- Any AIU member or contractor who wishes to access any internal computing resource using remote access must obtain approval and authorization from IT Security.
- At no time should any AIU member provide their AIU username and password or email to anyone, not even family members.
- AIU members and contractors with remote access privileges must ensure that their university owned or personal computer or workstation, which is remotely connected to AIU's network, is not connected to any other network at the same time.
- AIU members and contractors with remote access privileges to AIU's network must use their AIU username and password to conduct AIU business, thereby ensuring that official business is never confused with personal business.
- Reconfiguration of a home user's equipment for the purpose of split-tunneling or dual homing is not permitted at any time.
- All hosts that are connected to AIU internal networks via remote access must use a properly configured up-to-date anti-virus software and operating system.
- Review the Information Security Policy and Securing University Resources and Services Policy for details for protecting information when accessing the corporate network via remote access methods.

VI. FORMS/INSTRUCTIONS (if applicable)

N/A

VII. APPENDICES (if applicable)

N/A

VIII. RELATED POLICIES

Information Security Policy
Securing University Resources and Services Policy
Incident Response Policy

VIV. CONTACT INFORMATION

Triggered by:	Name	Date	Sig.
Created by:	Name	Date	Sig.
Revised by:	Name	Date	Sig.
Approved by:	Name	Date	Sig.