Remote Access
Campus Policy 833.0
Information Technology

I. Purpose and Scope

The purpose of this policy is to provide guidelines for Remote Access (VPN) connections to the UACCB campus network. These guidelines are intended to reduce security risks that may cause potential harm to the UACCB network or assets due to unauthorized use of the UACCB resources.

This policy applies to all UACCB employees, contractors, consultants, temporary/contingent workers, and other workers including all personnel affiliated with third parties utilizing VPN to access the UACCB network. The VPN user will also be subject to the conditions and performance constraints of their chosen Internet Service Provider (ISP).

II. Definitions

A VPN is a secured private network connection built on top of a public network. It provides a secure encrypted connection, or tunnel, over the internet between an individual computer/device and a private network such as UACCB. Use of a VPN allows authorized users to securely access UACCB resources from off campus.

Multi-factor Authentication (MFA) is a multi-step login process that requires users to verify their identity using two or more distinct authentication methods, defined as something they know, something they own or something they are, before accessing a system or application. This approach increases security compared to relying solely on a password.

III. Procedure

Approved UACCB employees and authorized third parties (vendors, contractors, consultants, etc.) may utilize UACCB's VPN or other approved remote access tools, which is a "user managed" service. This means that the user is responsible for selecting an Internet Service Provider (ISP), coordinating installation, installing any required software, unless installed by the Information Services dept, and paying associated fees.

Users must abide by the following guidelines as well as the Acceptable Use Policy:

- All users utilizing the VPN must use multi-factor authentication (MFA).
- Users with VPN access are responsible for ensuring that unauthorized users are not allowed access to the UACCB network, resources, and associated content. Authorized users will protect their login and password, and associated multi-factor information.

- Users are responsible for security and privacy precautions to protect against computer viruses, computer attacks, and theft which may result in loss of data, unintentional release of personal information, or negative impact on UACCB's technology services.

- All devices connected to UACCB's internal network via VPN or any other technology must use the most up-to-date anti-virus software, are patched and updated with respect to operating system, any applications are up to date and firewalls are enabled, if possible.

- By using VPN technology with personal equipment, users must understand that their machines are a de facto extension of UACCB's network, and as such are subject to the same acceptable use and security policies that apply to UACCB-owned equipment.

- Any solutions that circumvent routing and security measures shall be identified and disabled.

IV. Enforcement

Anyone found to have violated this policy may be subject to disciplinary action according to personnel policies and procedures. A violation of this policy by a vendor, consultant or contractor may result in termination of their contract or assignment with UACCB.

Forgery or other misrepresentation of one's identity via electronic or any other form of communication is prohibited regardless of intent.

V. Related Information

UA System Policy 285.1 Cybersecurity; UACCB Acceptable Use Procedure 810.0, UACCB Progressive Discipline Procedure 409.0; Faculty Handbook, Staff Handbook

Continuous improvement. The content of this document is subject to regular review based on input from UACCB Information Services staff and the campus community. Suggestions for improvement should be directed to the Director of Information Services.

VI. Revision History

Effective Date: May 14, 2025
Revised Date:
Review Date: