UNIVERSITY OF CENTRAL ARKANSAS | INFORMATION TECHNOLOGY

Remote Access Policy

Scope:

This policy applies to all UCA employees.

Definitions:

- Multi-factor Authentication (2FA) is a security program that requires a user to present a second form of authentication (such as a code or password) provided by SMS text, email, phone call, mobile app, or other means before accessing certain resources and/or services.
- Remote Access is the ability to gain access to a computer or a network from outside the organization through the use of an electronic device.
- Virtual Private Network (VPN) is defined as technology that allows a secure connection to the campus network and internal resources from a public Internet connection.

Purpose:

In order to protect the network and data infrastructure of the University, all UCA-owned computers have the ability to connect to the campus network via a VPN client. This client provides protection to the computer and its Internet connection by using UCA's firewall and gives the employee the ability to access sensitive internal resources while on a public Internet connection. This service is intended to extend the work environment for mobile employees beyond the physical boundaries of the campus in order to provide a more flexible working environment. However, in order to provide this level of flexibility, it is necessary to take appropriate security precautions.

Related Policies:

- UCA Board Policy 412
- UCA Mobile Device Security Policy
- UCA Computer User Outside the United States Policy
- UCA Password Policy
- UCA Network Security Policy
- UCA User Account Management Policy

Policy:

1. All UCA-owned computers will have the ability to make a connection to the VPN.

2. UCA-owned computers must be joined to Active Directory and maintained for patches, updates, and endpoint protection.

3. Any employee who wishes to use the VPN must attend a training session prior to using the service.

4. All computers that attempt to connect to the VPN must submit to an automated security compliance check. Computers that fail the required security check will not be permitted to connect to the VPN until the identified problems are remediated. The IT Help Desk can assist users in correcting security issues on UCA-owned computers.

5. VPN access may not be available when an employee is traveling internationally. Employees should be familiar with the applicable Export Control laws.

6. Employees must have a reliable connection to the Internet from off-campus locations. IT does not provide this connection nor does it provide technical support for off-campus Internet connections.

7. All employees connecting to the VPN must also use 2FA. The employee's college/department is responsible for the annual cost of the 2FA license. Information on 2FA costs will be maintained on the IT website.

8. Employees with VPN access are responsible for ensuring that unauthorized users are not allowed access to UCA networks, resources, and associated content. Authorized users will protect their login and password, and associated 2FA information, even from family members.

9. Printing of university data at the remote site is discouraged. When printed material is needed, employees are required to store them in a secure location and shred when no longer needed.

10. Service Requirements related to VPN Access to Sensitive Resources:

UCA Information Technology reserves the right to amend the Service Requirements at any time without prior notice and to take such further actions as may be necessary or appropriate to comply with other published policies and with applicable federal, state, and local laws and/or to protect the integrity and security of the University's network and data.

a. Sensitive resources should only be accessed from UCA-owned, Active Directory joined computers that are maintained for patches, updates, and endpoint protection.

b. Computers must have an encrypted hard drive. IT will perform the encryption process.

c. Computers may not access sensitive resources from locations outside the United States.

Enforcement:

Failure to comply with this policy will be investigated in accordance with established UCA disciplinary procedures. Noncompliance with this policy and/or its resulting procedures may be cause for disciplinary action.

Review/Revision Tracking

Date	Action
4-11-17	Adopted
6-6-17	Revised
9-5-17	Revised
2/20/24	Reviewed, edited for grammar / formatting
11/20/24	Revised