

CLARK ATLANTA UNIVERSITY

14.9 Remote Access Policy



CLARK ATLANTA UNIVERSITY		
Policy and Procedures	Subject: Remote Access Policy	
Department: Office of Information Technology and Communications (OITC)	Review Date: 06/04/20	Issued By: Chief Information Officer
	Effective Date: 06/15/2020	
Distribution: All University employees	Required Approval: University President	No. of Pages: 4
Signature: Original signed by George T. French, Jr., Ph.D.		Date: 06/15/2020

TABLE OF CONTENTS

	<u>Page(s)</u>
1.0 Policy Statement.....	1
2.0 Procedures Narrative.....	1
3.0 Entities Affected by this Policy.....	2

14.9 Remote Access Policy – Clark Atlanta University

1.0 Policy Statement

The purpose of this policy is to define rules and requirements for connecting to Clark Atlanta University's network remotely (i.e. connecting to or accessing CAU's network from any host computing device not located on CAU premises). These rules and requirements are designed to ensure that CAU working remotely have the ability to securely connect to the University network without fear of threat, to provide CAU with an additional means of monitoring and controlling access to the internal network, and to minimize Clark Atlanta University's potential exposure to damages which may result from unauthorized use of Clark Atlanta University resources.

2.1 Procedures Narrative

It is the responsibility of Clark Atlanta University staff, faculty, students, and partners with remote access privileges to Clark Atlanta University's corporate network to ensure that their remote access connection is given the same consideration as the user's on-site connection to the University.

General access to the Internet for recreational use through the Clark Atlanta University network is strictly limited to Clark Atlanta University staff, faculty, students, and partners (hereafter referred to as "Authorized Users"). When accessing the Clark Atlanta University network from a personal computer, Authorized Users are responsible for preventing access to any Clark Atlanta University computer resources or data by non-Authorized Users. Performance of illegal activities through the Clark Atlanta University network by any user (Authorized or otherwise) is prohibited. The Authorized User bears responsibility for and consequences of misuse of the Authorized User's remote access and will be subject to *Clark Atlanta University 14.7 Acceptable Use Policy*.

Authorized Users are prohibited from using Clark Atlanta University networks to access the Internet for non-CAU related business interests or purposes.

2.1.1 Requirements

- 2.1.1.1 Secure remote access will be strictly controlled with encryption [e.g., Virtual Private Networks (VPNs)] and strong pass-phrases. For further information, see *Clark Atlanta University 14.5 Password Policy*.
- 2.1.1.2 Authorized Users shall protect their login and password, even from family members.
- 2.1.1.3 While using a Clark Atlanta University-owned computer to remotely connect to Clark Atlanta University's network, Authorized Users shall ensure the remote host is not connected to any other network at the same time, with the exception of personal/home networks that are under their complete control or under the complete control of an Authorized User or Third Party.
- 2.1.1.4 Use of non-CAU issued devices to conduct Clark Atlanta University business must be approved in advance by OITC and the appropriate business unit manager.

All host computing devices, including personal computers, that are connected to Clark Atlanta University internal networks via remote access technologies must use the most up-to-date anti-virus software and includes personal computers. Any third party system or network connections that request access to the CAU internal network must comply with requirements provided by OITC and the appropriate business unit manager.

14.9 Remote Access Policy – Clark Atlanta University

3.0 Entities Affected by this Policy

This policy applies to all Clark Atlanta University staff, faculty, students, and partners with a Clark Atlanta University-owned or personally-owned computer or workstation used to connect to the Clark Atlanta University network. The use of the university's network and system resources is a privilege, not a right. This privilege can be revoked or amended when justified. Failure to comply with this policy may result in disciplinary action as outlined in the *Clark Atlanta University 2.4.0 Code of Ethical Conduct Policy*.