


Approved 12-15-20  


# Rogers State University

---

## Remote Access Policy

### 1. Purpose

---

This policy defines the standards for employees and contractors to connect to the RSU network from a remote location. These standards are designed to minimize potential risks and limit exposure to security concerns through a consistent and standardized access method.

### 2. Authority

---

This document is authorized by the President, IT Director, and Cyber Security Specialist

### 3. Scope

---

This policy is applicable to all departments and users of Rogers State University resources and assets.

### 4. Policy

---

The following policies and procedures apply to RSU employees and contractors that remotely connect to RSU's network.

- Staff VPN access requests must be submitted to ACS by the Vice President that oversees the staff member's department.
- Faculty VPN access requests must be submitted to ACS by the Dean that oversees the faculty member's department.
- Contractor VPN access requests must be routed through the Vice President that oversees the area that access is being requested for.
- The Director of Information Technology must approve of remote access before it is granted.
- Users are responsible for ensuring that the device they use to connect from has adequate security measures in place. (IE: Current Anti-Virus and all major Operating System updates have been installed).
- Users must use multifactor authentication to connect remotely.
- Users must ensure their device they use to remotely connect is protected by a password that at a minimum meets RSU's password requirements.

- Users with remote access privileges shall ensure that their remote access connection is used explicitly for work business and used in a manner consistent with RSU's Computer Use Policy.
- Users must ensure that their devices are not shared with others while connected to RSU's network.
- The list of users with remote access will be reviewed by the Vice Presidents and Deans on a quarterly basis to ensure that such access is needed.

## 5. Compliance

---

This policy shall take effect upon publication. Compliance is expected with all enterprise policies and standards. Policies and standards may be amended at any time; compliance with amended policies and standards is expected.

Employees and contractors found to be in violation of this policy may have their remote access revoked and possibly face additional disciplinary action as appropriate.

## 6. Definitions of Key Terms

---

<b>Term</b>	<b>Definition</b>
-------------	-------------------

IT	Information Technology
----	------------------------

## 7. Contact Information

---

Submit all inquiries and requests for future enhancements to the policy owner at:

breeves@rsu.edu

## 8. Revision History

---

This standard shall be subject to periodic review to ensure relevancy.

<b>Timestamp</b>	<b>Reviewer</b>	<b>Comments</b>
------------------	-----------------	-----------------

TODO	Quince Fennell	Initial Conversion from CIS Source
------	----------------	------------------------------------