

Third (3rd) Party Network Access Request Form

Instructions: Read these policies and terms carefully. Sign and complete the section on page 3 indicating your agreement. Please note that both the end-user and the responsible R-CCC unit/department must agree to these terms and conditions.

Third Party Network Access Request

Service

This document outlines a service for accessing Roanoke-Chowan Community College's network by means of a direct R-CCC network connection, or Virtual Private Network (VPN) connection, within the Remote Access Policy of the College. The Remote Access Policy states: Remote access to the College will be appropriately provisioned and/or controlled to ensure required security.

Definitions

Virtual Private Network (VPN): A VPN creates a secure connection, called a tunnel between a client computer and a VPN server. This connection is usually made over the Internet and, in that case, has the effect of extending R-CCC's remote users. Once connected, a user may access files and/or applications stored on central servers just as the user's machine was connected directly to R-CCC. If a VPN is used on campus, the effect is to create an encrypted connection across R-CCC network.

Third (3rd) Party: Refers to an affiliate or individual/entity from a vendor/agency requesting data/services access.

Service Terms and Conditions

Approved 3rd Parties may connect to R-CCC either directly from an on-campus computer or remotely via VPN. Approvals must be obtained from the appropriate management at the Director level and above. The College IT Department must approve direct network access of 3rd Parties. 3rd Party Network Access Request forms can be found on the R-CCC website. Requestors must have a demonstrated academic or business need to connect securely and/or to appear as a part of R-CCC Network. Use of this service in the performance of activities unrelated to the mission of the College is strictly prohibited.

VPN is a user-managed service, which means that off-campus users of this technology are responsible for selecting an Internet Service Provider (ISP), coordinating installation with their ISP of any required software, and paying associated fees.

Additionally,

1. It is the responsibility of those with VPN privileges to prevent unauthorized access to R-CCC's network from their VPN connected computer.
2. Users will be authenticated through their R-CCC ID and password.

3. All computers connected to R-CCC's network **must:**
 - a. Use the most current anti-virus protection
 - b. Keep computers updated with the latest critical operating systems patches
 - c. Use compatible firewall protection. More information regarding Cisco compatible firewalls are also listed on this site.
 - d. Not bridge R-CCC to another network using this VPN connection.
4. When remotely connected to R-CCC via VPN, off-campus users agree that they are subject to the same College rules and regulations that apply to on-campus usage. In particular, users must adhere to R-CCC's Information Technology Policies including its Acceptable Use Policies (AUP) see Appendix 1.
5. VPN users will be disconnected from R-CCC after 15 minutes of inactivity. Pings or other artificial means used to bypass this time limit are strictly prohibited.
6. VPN absolute connection times are limited to 8 hours.
7. All requestors must read and agree to these terms and condition before a connection is granted.
8. Data collected, stored, backed up, processed or accessed using this service must be protected according to College policies and procedures.
9. **Confidential college data should not be stored on privately owned systems.**
10. Proper data removal/destruction procedure must be followed for off-campus systems at the end of employment, any contractual arrangement, or cessation of the of the individuals VPN service.
11. Vendors require access to R-CCC's network via firewall access control must adhere to R-CCC's network and data access procedures.
12. IT Dept. may annually review VPN requests for validation and audit purposes.

Enforcement

All individuals granted access to R-CCC's network or VPN service must adhere to the service terms and conditions. If these terms and conditions are violated, R-CCC's network access will be revoked. Violations will also be reported to the users' management, which may lead to the termination of 3rd party services or legal action.

**Third (3rd) Party Network Access
Request Form – Continued**

Data Access Agreement

1. I understand and accept that being granted access to the Roanoke-Chowan Community College's (from now on referred to as R-CCC) network and information systems involves my assuming considerable responsibility for maintaining the integrity and security of R-CCC data. I am responsible for the privacy and confidentiality of any R-CCC data to which I have access. Such data may include but is not limited to the student, financial, medical, and personnel records.
2. I will comply with all related R-CCC policies, including its Acceptable Use Policy. I will comply with all the applicable federal and state laws, including but not limited to FERPA, HIPAA, ECPA, USA Patriot Act, TEACH Act, GLBA and SEVIS.
3. I will not share any R-CCC data with any third party without the express authorization from the Data Steward/Information Owner and R-CCC's IT Department or the Chief Information Officer. I understand that providing unauthorized access to R-CCC's data or information is in violation of applicable state and federal laws, as well as R-CCC's Information Technology Policies.
4. I agree to keep all R-CCC data that I collect, store, back-up, process or otherwise access secure by following accepted practice for secure use. For example, proper utilization of screen blanking, idle system timeouts, password standards, data encryption, anti-virus software, secure document storage and the shredding printed outputs, etc.
5. I agree to return or destroy all R-CCC data in my possession upon the cessation of access to R-CCC systems. I agree to immediately notify R-CCC if my stewardship of R-CCC data or my system access has been, or might have been compromised. In case of reasonable suspicion or actual threat, I will immediately contact the R-CCC Chief Information Officer at 252-862-1302.
6. For remote access, I agree to sign and be bound by the terms and conditions of R-CCC's Virtual Private Network Service. (To be attached to this agreement)
7. I understand the term of access granted will be limited to the dates indicated in the access request form and is not to exceed 180 days. Long term access, beyond a 180 day term, may be requested by R-CCC's sponsoring division/unit but must be fully documented, justified and submitted to the IT Security Office for review.

I understand that violating these terms and conditions may result in my access being revoked with notice and could include additional legal action.

**Third (3rd) Party Network Access
Request Form Continued**

3rd Party Network Access & VPN Request Form

| | |
|--|---|
| Instructions | <ul style="list-style-type: none"> • Read the Service Terms and conditions. • Complete the 3rd Party Data Section. • Have your sponsoring department/unit complete the R-CCC Sponsor Authorization section. • Sign and date the form. • Deliver signed request form to the R-CCC IT Department. • IT Department will initiate the account creation process and will review for approval. • Network access will not be granted until approvals are obtained. • Please allow for up to 5 business days for processing each request. |
| 3rd Party Data (Requestor to Complete) | <p align="center">Required Required</p> <p>3rd Party Data: Please Print Access Start Date _____ Access Expiration Date _____ (if applicable)</p> <p>LAST NAME: _____ FIRST NAME: _____ COMPANY: _____ ADDRESS _____ PHONE _____</p> <p>EMAIL: _____ VPN ACCESS REQUIRED? (Circle one) YES / NO</p> <p>LAST NAME: _____ FIRST NAME: _____ TITLE: _____ CAMPUS: _____</p> <p>EMAIL: _____ VPN ACCESS REQUIRED? (Circle one) YES / NO</p> <p>I have read the service terms and conditions and agree to abide by the policies outlined therein.</p> <p>SIGNATURE: _____ DATE: _____ SIGNATURE: _____ DATE: _____</p> |
| R-CCC Sponsor Authorization | <p>Sponsoring Department/Unit Authorization: Please Print</p> <p>LAST NAME: _____ FIRST NAME: _____</p> <p>DEPARTMENT/UNIT: _____ CAMPUS _____</p> <p>I approve the access requested for the above 3rd Party. When the 3rd Party leaves the college, I will notify OIT to terminate network access.</p> <p>APPROVAL SIGNATURE: _____ DATE: _____</p> |

| | |
|---|--|
| IT Security (Official Use Only) | <p>REVIEWED BY: _____ DATE: _____</p> <p>REVIEWED BY: _____ DATE: _____</p> <p>IMPLEMENTATION DATE: _____</p> <p>SCHEDULED FOR REVIEW DATE: _____</p> |
| Administration/ Department Head Signatures | <p>Dean/IT Director: _____ Date: _____</p> <p>President's Signature: _____ Date: _____</p> |