REMOTE ACCESS PROCEDURE

Related Board of Trustees Policy: BP 8.4
Approval: August 2012
Revision: August, 2015
NC Statewide Technology Standard(s): 20112

Purpose: Require users ensure security measures are followed when accessing Craven Information Technology Systems.

Authorized users of Craven computer systems are permitted to remotely connect to the network for the conduct of Craven-related business only through secure, authenticated, and carefully managed access methods.

Access to the Craven Network via external connections from local or remote locations including homes, hotel rooms, wireless devices and off-site offices are not automatically granted network or system access. Systems are available for on- or off-site remote access only after an explicit request is made by the user, the VPN Access Request Form completed, approved by the supervisor and the Vice President of Administrative Services, and a copy returned to the Network Administrator.

Opening uncontrolled or unsecured paths into any element of the Craven Network that requires security or to internal computer systems presents unacceptable risk to the College.

Approved Craven Community College employees and authorized third parties (customers, vendors, etc.) may utilize the benefits of a VPN, which is a "user managed" service. This means the user is responsible for selecting an Internet Service Provider (ISP), coordinating installation, installing any required software, and paying associated fees.

It is the responsibility of employees and permitted third parties with VPN privileges to ensure that unauthorized users are not allowed access to Craven Community College internal networks.

- VPN use is to be controlled using either a one-time password authentication, such as a token device, or a public/private key system with a strong passphrase.
- When actively connected to the corporate network, VPNs will force all internal network traffic to and from the PC over the VPN tunnel.
- VPN gateways will be set up and managed by Craven Community College.
- All computers connected to Craven Community College internal networks via VPN or any other technology must have an up-to-date antivirus application installed.
- VPN users will be automatically disconnected from Craven Community College's network after thirty (30) minutes of inactivity. The user must then logon again to reconnect to the network. Pings or other artificial network processes are not to be used to keep the connection open.
- The VPN connection is limited to an absolute continuous connection time of 24 hours.
- Users of computers that are not Craven Community College-owned equipment must configure the equipment to comply with Craven Community College's VPN and Network policies.
- Only Craven-approved VPN clients may be used.
- By using VPN technology with personal equipment, users must understand that their machines are a de facto extension of Craven Community College's network, and as such are subject to the same rules and regulations that apply to Craven Community College-owned equipment.
- Revocation/modification: Remote access will be revoked at any time for reasons including non-compliance with security policies, request by the user's supervisor or negative impact on overall network performance attributable to remote connections. Remote access privileges will be terminated upon an employee’s or

contractor's termination from service. Remote access privileges will be reviewed upon an employee's or contractor's change of assignments and in conjunction with regularly scheduled security assessments.

- Anonymous interaction: With the exception of web servers or other systems where all regular users are anonymous, users are prohibited from remotely logging into any Craven Community College system anonymously, such as by using "guest" user IDs.
- Audit: Audit logs of remote access activities shall be maintained for at least ninety (90) days by the Network Administrator.
- User rights are reviewed at six (6) month intervals by the Network Administrator.
- A checklist shall be completed for vendors requiring VPN access.

VPN Access Request Form

Requestor Information

Requestor's Name: _____ Department: _____
Date of Request: _____ E-mail: _____
Duration of Access: _____ Phone Number: _____
Justification for Access:

_____

_____

_____

Guidelines: Each VPN user is assigned their own group name and password. In all transactions VPN users shall **use their assigned group and individual VPN User Name and password**.

It is the responsibility of the requestor to ensure the computer connecting to the VPN has an active and running antivirus program installed. If you need help verifying that your computer meets these requirements, please contact the IT department by opening a Helpdesk ticket by emailing helpdesk@cravencc.edu or calling 252.638.1222.

Remember, each member of the Craven Community College VPN plays an important role in maintaining the security and confidentiality of Craven Community College's records. I certify that the computer I use to connect via VPN is running an antivirus program and I understand that the same Acceptable Use Policies apply to this service. I also understand that my login ID and password are to be used by me only and will not be shared with any other individual or party. I further understand that I am obligated to notify Craven Community College's Network Administrator in the event of any security incidents involving my equipment.

By signing this document, supervisor confirms that a criminal background check is conducted on every employee who will be requesting VPN access to Craven Community College's network.

By signing this document you're acknowledging that you have read and understand Craven Community College's Remote Access Procedures.

Requestor's Signature: _____ Date: _____
Requestor's Title: _____
Supervisor's Signature: _____ Date: _____
Supervisor's Title: _____
VP of Administrative
Services: _____ Date: _____

Return to the Table of Contents