08-07-00 Remote Network Access Policy

PURPOSE

The purpose of this policy is to establish the rules governing connection to the college campus network via Virtual Private Network technology.

DEFINITIONS

Information interception, data loss, and identity theft are serious and growing concerns. One instance of a security breach can cost millions of dollars to the college, a great deal of financial and legal problems for students or employees, and a loss of trust from the community. The NSCC network is monitored by TSD staff members, and a number of protections are in place to prevent security breaches. Off-campus systems do not offer this level of protection. Therefore, in order to safeguard sensitive information and identity information stored within the NSCC network the following must be observed.

POLICY

1. All remote access connections must be accomplished through the application of Virtual Private Network (VPN) software.
2. Internet Native Banner (INB) and Banner Admin Pages are to be accessed exclusively through VPN.
3. A signed Remote Network Access Security Authorization form approved by the direct supervisor, the Vice President to which the user’s division reports, and the Chief Information Officer or designee is required before off-site access is permitted.
4. This policy must be agreed to and observed by the user.
5. Employees approved for off-campus access must download the VPN client from https://vpn.nscc.edu. Instructions for downloading, installation and connecting are included.
6. While the software has been tested by TSD, we cannot guarantee that it will be compatible with all PC configurations. NSCC is not responsible for personal equipment, data or application loss, or damage. Personal data should be backed-up and application media readily available prior to installing the VPN client in the event that a reinstall becomes necessary.
7. Internet access is required but is not provided by the college; high speed Internet access is recommended.
8. NSCC Technology Services will add the employee’s identification information to the RADIUS

(Remote Authentication Dial In User Service) server, which will authenticate that the employee has been given remote access permission when that employee attempts to connect from off-campus. The TSD staff member who adds this information must sign the authorization form and the Chief Information Officer or designee must approve it.

9. Users are responsible for maintaining anti-virus software and updated operating system (i.e. – Windows, Linux, Mac) software on non-NSCC computers.
10. NSCC-owned mobile devices will be encrypted and must be returned to TSD at each renewal to ensure that software has current patch maintenance.
11. Access is granted for a 6-month period and must be renewed by the employee on a new Remote Network Access Security Authorization form with the required authorizations.
12. Supervisors are responsible for notifying TSD in a timely manner of any changes in employment status that necessitate changes to the employee's Banner access. Notification is to be made on the Separation TFSA Form. When this notification is received the authentication information will be disabled on the RADIUS server.
13. College data, including Personally Identifiable Information (PII), will never be stored on the home computer unless it is an encrypted NSCC-owned device.
14. VPN connections are never left unattended when not in use.
15. The PC will not be made available for use by individuals who may knowingly load software from untrustworthy websites or email.
16. Monitor placement is such that the screen cannot be viewed through an outside window or by individuals other than the employee who may be in the room where the computer is located.
17. TSD will provide a purchase consult and/or a quote to the department for computer/laptop purchases as well as assistance with loading and troubleshooting VPN connection issues.
18. In instances where NSCC owned computing equipment is approved for off-site use, equipment loan forms must be properly filed with the Property Manager office, and the equipment must be returned to TSD for any repairs that may become necessary, as well as for maintenance software patches and updates.
19. In accordance with TBR and State regulations, the college is not permitted to provide technical support for items that the employee may use personally.
    A. In-home service, other than phone support, is not permitted.
    B. It is the responsibility of the individual to make all financial and technical support arrangements that will enable them to work from home or other off-network locations.
    C. TSD is not permitted to provide or support personal items, such as computer hardware, routers, printers, software (other than VPN), backup services, installation, and internet connections.

CHANGE LOG

Date	Change	By
5/11/2018	Revised to encompass all use of remote access	PAK
3/15/2021	Modified for new policy format	PAK
3/15/2021	Changed all instances of CSD to TSD	PAK
10/26/2023	Changed title from Director of Technology Services to Chief Information Officer or designee	BR
10/26/2023	Removed outdated sample VPN form	JMS

Approved by President's Cabinet 6/14/21; updated 12/11/23