3357:14-3-16-282 Remote use of North Central State College Resources

(A) The purpose of the Remote Site Security Standards is to provide the data protection security necessary to comply with the College’s Remote Site (Telecommuting) Policy. These standards are mandatory requirements and establish an effective baseline of appropriate system, administrative, and physical controls to safely and effectively secure a remote working environment. Specific information security guidelines are available to provide guidance on how to comply with these standards.

(B) These standards apply to all College employees, or contractors with the College who have been provided with College owned equipment or utilizing personally-owned computer, or other equipment to connect to College network from a remote location. Remote access implementations that are covered by this policy include, but are not limited to DSL, Cable, VPN, SSL.

(C) One of the most important aspects of information security is protecting critical information. Confidentiality, integrity and availability are the three predominant principles of information protection. Compromising these principles leaves systems and critical information in jeopardy. Establishing remote site access creates the potential for security risks and threats that could result in damage to the integrity of the College, cause financial loss to the College, and/or personal hardship to individuals. Threats are the accidental or adversarial attacks against the College, while risks are the realization of the threat based on its potential loss. Below are some of the security threats that should be considered when determining whether remote site access is feasible in your department.

(1) The networks utilized are not controlled by College and may be more open. Physical loss of data residing on equipment used for remote site access

(2) Access to data by those unaffiliated with the College, including family members, on shared devices in a household

(3) Disgruntled users or employees who abuse the privilege of remote site access to acquire or steal College data

(4) Intercepted or stolen data transmitted over an insecure network

(5) Home devices may be subject to E-Discovery requests

(D) Standards for Operating from a Remote Environment

(1) Operating Environment

(a) All employee computers connected to the College’s network via remote site access technologies must use current/up to date anti-virus software to ensure that their computer is protected from hackers and malware. All employee computers connected to the College network via remote site access technologies should employ a software or hardware based firewall.

(b) All equipment should utilize operating systems and software that are currently supported by a legitimate vendor (i.e., Microsoft, Apple, Adobe, etc.).

(c) All employee computers connected to the College network must automatically or manually apply all necessary Operating System (OS) and application security updates or “patches” and keep the equipment up to date.

(d) As a rule, users may not store any College restricted data on their personally owned devices. Restricted data includes data that the College is required to protect under regulatory or legal requirements. Examples include student or employee identifiable information (i.e., name, SSN, birth date, home address, etc.), medical records, legal records, student records, police records, and credit card information. Restricted data needs to be protected at the same level as required on campus.

(e) The wireless (wi-fi) preferences/settings for your computer and portable devices must not be set up to auto-connect to any wireless network they detect. Auto-connecting to unknown networks could put your computer and data at risk.

(f) The employee is responsible for ensuring that family members do not violate any College policies, do not perform illegal activities, and do not use the access for outside business interest. The employee bears responsibility for the consequences should the access be misused.

(g) A minimum internet bandwidth requirement for remote access is 20MB. The equipment and service required to achieve this recommendation are the responsibility of the employee.

(h) Secure remote access must be strictly controlled. Control will be enforced via multi factor authentication or public/private keys with strong pass-phrases.

(i) Employees and contractors with remote access privileges must ensure that their College owned or personal computer, which is remotely connected to NCSC's corporate network, is not connected to any other network at the same time, with the exception of personal networks that are under the complete control of the user.

(j) Reconfiguration of a home user's equipment for the purpose of accessing the public internet at the same time while accessing NCSC secured resources via a VPN connection **(split tunneling)** is not permitted at any time.

(k) Organizations or individuals who wish to implement non-standard remote access solutions to the College’s network must have approval from NCSC’s IT department.

(2) Home Wireless Networks

(a) Home wireless networks are easy to set up and are often times provided by Internet Service providers. While they are extremely convenient to use, an insecure wireless environment opens up several risks that need to be addressed.

(i) A person that is in close proximity to your home can use your Internet connection.

(ii) A person that is in close proximity to your home may be able to access your computer.

(iii) Information sent over the wireless connection can be stolen.

(b) In order to help mitigate the risks associated with home wireless networks used for remote site access, the following wireless home networking configurations must be implemented.

(i) Wi-Fi Protected Access (WPA) encryption should be enabled

(ii) The default Service Set Identifier (SSID) or the name of the Wi-Fi connection for your wireless router should be changed.

(iii) The default Administrator Passwords and Usernames for your wireless router should be changed.

(iv) Media Access Controls (MAC) filtering should be utilized

(E) Physical Security

(1) Hardware, software and data destruction of restricted materials must be done securely and disposed of at the termination of business need, and in conjunction with the College data disposal policy. Remote working arrangements should be equipped to facilitate this activity (shredder).

(2) Files must be backed up and tested on a regular schedule, and stored in a secured location.

(3) Employees and units are responsible for security breaches involving NPPI (non-public personal information). The measures described will help reduce the number of security breaches and limit the cost, time, and negative publicity associated with such breaches.

(F) Definitions

(1) Encryption: The process of converting information using an algorithm to make it unreadable to anyone except those possessing special knowledge, referred to as a key.

(2) MAC: Refers to Media Access Control. A PC network card or device has a unique identifier called the MAC address that is used for identification purposes.

(3) Patch: A patch is a piece of software designed to fix problems or update a computer application or operating system. Intruders often seek methods to take advantage of vulnerabilities resulting from these problems to penetrate systems.

(4) SSID: Refers to Service Set Identifier, and is the name that identifies a particular wireless Local Area Network (LAN).

(5) WPA: Wi-Fi Protected Access is a certification created by the Wi-Fi Alliance to indicate compliance with security protocol. Most newer Wi-Fi certified devices support the security protocols, out-of-the-box, as compliance with this protocol has been required for a Wi-Fi certification since September 2003.

(6) VPN Split Tunneling: Virtual private network (VPN) split tunneling lets you route some of your application or device traffic through an encrypted VPN, while other applications or devices have direct access to the internet. While split tunneling offers obvious benefits, risks abound as well. Additionally, if an end-user has an insecure network, they risk the corporate systems as well. Specifically, if a hacker compromised an employee's home network through the split tunnel, they could potentially penetrate the corporate system as well.

Effective: March 23, 2021
Next Review: March 1, 2026
Review Dates: 9/1/15, 3/23/21