ADMINISTRATIVE POLICY

Remote Access

POLICY STATEMENT

Nevada State College's (NSC) electronic resources must be protected from unauthorized use and/or malicious attack that could result in loss of information, damage to critical applications, and damage to its public image. Therefore, all remote access to technology resources at Nevada State College must employ college approved connection methods.

REASON FOR POLICY

The purpose of this policy is to define standards and procedures for connecting securely to Nevada State College's internal network from external hosts via remote access technology.

PROCEDURES

It is the responsibility of any employee of Nevada State College with remote access privileges to ensure that their remote access connection remains as secure as his or her network access within the office. It is imperative that any remote access connection used to conduct NSC business be utilized appropriately, responsibly, and ethically. Therefore, the following rules shall be observed and any violations may result in having remote access revoked.

1. General access to the Internet by residential remote users through NSC's network is permitted. However, both the employee and his/her family members using the Internet for recreational purposes through company networks are not to violate any of NSC's acceptable use policies.

2. Employees will use secure remote access procedures. This will be enforced through password protection, data encryption, and the use of secure remote access systems. Employees agree to never disclose passwords to these systems to anyone, particularly to family members if business work is conducted from home.

3. All remote computer equipment and devices used for business interests, whether personal or institution-owned, must display reasonable physical security measures. Computers shall have appropriate antivirus or security software installed.

4. No employee is to use Internet access through company networks via remote connection for the purpose of illegal transactions, harassment, competitor interests, or obscene behavior, in accordance with other existing policies.

5. If a personally-owned or institutionally-owned computer or related equipment used for remote access is damaged, lost, or stolen, the authorized user will be responsible for notifying Information & Technology Services immediately.

6. The remote access user also agrees to immediately report to their manager and Information & Technology Services any incident or suspected incidents of unauthorized access and/or disclosure of college resources, databases, networks, etc.

7. The remote access user also agrees to and accepts that his or her access and/or connection to NSC's networks may be monitored to record dates, times, duration of access, etc., in order to identify unusual usage patterns or other suspicious activity. As with on campus computers, this is done in order to identify accounts/computers that may have been compromised by external parties.

CONTACTS

SUBJECT	CONTACT	PHONE	EMAIL
Primary Contact(s)	Brian Chongtai	702-992-2410	brian.chongtai@nsc.edu

DEFINITIONS

Electronic Resources - Student data, computer systems, networks, databases, etc.

RELATED INFORMATION

HISTORY

Revised 3/19/18