Policy & Procedures

Remote Network Access

Issued by: Department of Information Technology

Effective: **February 26, 2003**

Applies to: All NJCU employees, contractors, consultants, and temporary hires that request and are granted remote network access.

Table of Contents

Introduction 1
Purpose 1
Definitions 1
Policy 2
Enforcement 2
Key Performance Indicators (KPIs) 3
Procedures 3
Guidelines 3
Contact 4
Related Documents 4

Introduction

Remote network access is provided for those faculty and staff who find themselves doing university business from a remote location, such as home or when traveling. Remote access to the NJCU data network is also provided to consultants and contractors as needed. While the connection is as secure as possible, remote access is inherently a security risk. Consequently, policy and procedures are required to minimize this risk.

Purpose

NJCU provides remote network access so that authorized personnel have access to network services from off campus. The policy, procedures, and guidelines provided in this document were developed to minimize risk associated with this activity. It is, therefore, very important that members of the university and contracted workers who are granted remote access privileges follow these regulations.

Definitions

Remote network access involves setting up *a virtual private network* (VPN) connection between the remote computer using VPN client software and a special gateway router that allows access to the university network over the Internet. This requires a high-speed connection to the Internet via an Internet Service Provider. Access is granted to users by login, using an account name and password combination. When actively connected to the NJCU network, all traffic to and from the remotely attached PC is through the VPN tunnel, including Internet browsing.

VPN client software provides an encrypted connection between an individual and a private network, so activity over this connection is secure and private. By utilizing the public Internet for data transport, VPN provides a low cost solution to remote access or connectivity. In effect, this allows members of the University community to access NJCU network recourses as if they were on campus.

Policy

Administrators, IT staff, faculty and authorized contractors are permitted remote network access through VPN client software with the approval of the requester's supervisor and/or the head of the Department of Information Technology (IT) or by contractual agreement. VPN is a "user managed" service. This means that the user is responsible for selecting an Internet Service Provider (ISP), coordinating installation, installing any required software, and paying associated connection fees.

Additionally,

- VPN access is provided through the Department of Information Technology. No other department may implement VPN services.
- Only the VPN client software distributed by IT may be used.
- VPN account names and passwords will be assigned by an IT network administrator or authorized delegate.
- It is the responsibility of employees and third parties with VPN privileges to ensure that unauthorized users are not allowed access the NJCU network.
- All network activity during a VPN session is subject to NJCU policies and may be monitored for compliance.
- Dual (split) tunneling is NOT permitted during VPN sessions to the NJCU network.
- All computers connected to the NJCU network via VPN or any other technology must use the most up-to-date anti-virus software that meets or exceeds the corporate standard. Proof of compliance is required prior to the assignment of a VPN account.
- VPN users will be automatically disconnected from the NJCU network after thirty 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 gateway is limited to an absolute connection time of 24 hours.
- Users of computers that are not NJCU-owned equipment must configure the equipment to comply with NJCU's VPN and Network policies.
- By using VPN technology with personal equipment, users must understand that their machines are a de facto extension of the NJCU network, and as such are subject to the same rules and regulations that apply to NJCU-owned equipment.

Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment. Consultants and contractors will be subject to legal action up to

and including the payment of fines and penalties that may be incurred, and immediate termination of all contractual agreements.

Key Performance Indicators (KPIs)

The following success of the policy will be assessed annually using the following quantifiable measures:

- No security issues over this connection
- No violations of policy

Procedures

The following procedures should be followed to acquire VPN access:

Employees

1. Employees must discuss the viability of remote access with their immediate supervisor.
2. If the supervisor approves, enter a request for VPN services via the Online Remote Access Request Form for Faculty and Staff.
3. Upon request, provide proof of anti-virus compliance to the IT network administrator.
4. The IT network administrator or delegate will provide the software and setup instructions.
5. Install the VPN software on the target computer as instructed.

Consultants and Contractors

1. Intention of use must be included with bid submissions and in final contracts.
2. The Online Remote Access Request Form for Consultant and Contractors must be completed for each individual who will be utilizing remote access.
3. Each individual must provide proof of anti-virus compliance to the IT network administrator.
4. The IT network administrator or delegate will provide the software and setup instructions.
5. Install the VPN software on the target computer as instructed.

Guidelines

The *minimum* hardware/software requirements for connectivity are:

- A computer capable of providing appropriate network connectivity
- Broadband connection to the Internet via a local Internet Service Provider (ISP)
- Internet interface device (provided by and connects to the ISP network)
- Ethernet network interface in computer (connects to ISP interface device)
- VPN Client Software (provided by IT) and installation instructions

Contact

This policy is managed by:

University Title: Associate VP for Information Technology
Location: Rossey Hall, Room 58
Telephone: (201) 200-3350
Facsimile: (201) 200-2332
Email: it@njcu.edu

Questions should be directed to the appropriate resource from the following list:

Issue	Contact
Connectivity & Technical Support	NJCU Help Desk, IT
Policy & Guidelines	Assist. Director, IT

Related Documents

- Responsible Use of Computing Resources
- Peer-to-Peer Networking Policy
- Email Security Policy
- Network Storage Policy

Forms

- Remote Access Request Form for Faculty & Staff
- Remote Access Request Form for Consultants & Contractors

All documents and forms are available from the IT website, Documents and Support pages.