Northeastern Illinois University

NEIU POLICY

Volume I1: Information Technology	**I1.01.4** **Remote Network Connection**	**Responsible Office:** University Technology Services
Chapter 01: Acceptable Use	**Effective Date:** 02/29/2012	**Responsible Officer:** Executive Director

POLICY STATEMENT

Northeastern Illinois University (NEIU) will provide employees, based upon need, remote, secured and confidential access to specific NEIU administrative or academic applications.

PURPOSE OF THE POLICY

This policy describes procedures to obtain access and terms of use for secure remote access to University applications.

WHO IS AFFECTED BY THIS POLICY

The policy affects all employees of the University who are required to access NEIU confidential, secure applications from off campus.

DEFINITIONS

Virtual Private Network: A virtual private network (VPN) is a computer network that is layered on top of an underlying computer network. The private nature of a VPN means that the data travelling over the VPN is not generally visible, or is encapsulated, from the underlying network traffic. Similarly, the traffic within the VPN appears to the underlying network as just another traffic stream to be passed.

PROCEDURES

A NEIU employee required to be away from the University for a period of time or who is required to work from home may apply for remote access to confidential University applications through the virtual private network (VPN). Remote secure access is available wherever the internet is available.

Requests for access to the VPN for an employee must be made by the department head in writing to University Technology Services (UTS) – Service Delivery department. The request must include the following:

- The identity of the employee who is to be using the VPN including their employee ID, Department and Job Title.
- Explanation of the underlying reason for and intended use of the VPN and job functions that require access.
- The period of time the remote access is needed.

The employee with access to the VPN is responsible for all work completed while using it and is responsible for the confidentiality of all information used in conjunction with that work.

In the event that the remote secured access is no longer required the department must immediately contact University Technology Services – Service Delivery to disable the VPN access. When an employee who has access terminates his/her employment with the University the VPN access will be disabled.

NEIU reserves the right to check for security threats prior to allowing access to VPN and reserves the right to deny access based on identified threats.

HISTORY

N/A

RELATED POLICIES, DOCUMENTS, AND LINKS

- Family Educational Rights and Privacy Act (FERPA)
- I1.2.5 – PCI and PII Data Storage and Handling
- Health Insurance Portability and Accountability Act (HIPAA)

CONTACT INFORMATION

Please direct questions or concerns about this policy to:

Contact	Phone	E-Mail
Executive Director, University Technology Services	(773) 442-4374	k-tracy@neiu.edu
Director, UTS -Service Delivery	(773) 442-4357	t-black@neiu.edu

DISCLAIMER

The University reserves the right to modify or amend sections of this policy at any time at its sole discretion. This policy remains in effect until such time as the Responsible Officer calls for review. Requests for exception to any portion of this policy, but not to the policy statement, must be presented in writing to the Responsible Officer.