I.T. VPN Remote Access Policy

Policy Number:
Owner Department: Information Technology
Effective Date: February 24, 2011
Approved By: President's Council

I. POLICY TITLE

I.T. VPN Remote Access Policy

II. POLICY STATEMENT

Remote access to electronic information of SCNM computer resources must be secure and prohibit unauthorized access by using virtual private network (VPN) or similarly securable connectivity protocols.

III. POLICY STATUS

Revised (to new format)

IV. HISTORY/BACKGROUND

N/A

V. DEFINITION(S)

Virtual Private Network: a mechanism for creating a private computer communications or providing a secure extension of a private network into an insecure network such as the Internet or corporate network.

Anti-Virus Definitions: a file regularly updated by anti-virus companies to combat virus attacks. These files are automatically applied to computers with active fee-based subscriptions and employ multiple methods of virus detection analysis including: signature-based, malicious activity, heuristic-based, file analysis, and file detection.

VI. PURPOSE

The purpose of this policy is to protect the electronic information from being compromised by unauthorized remote access connections.

VII. SCOPE/KEY STAKEHOLDERS

The scope of this policy is to define appropriate VPN access and its use by authorized personnel. Employees and authorized third parties (customers, vendors, etc.) may use VPN connectivity to gain access to the SCNM network resources from off-site locations.

I.T. VPN Remote Access Policy

Stakeholders are defined as staff and faculty permitted VPN access

VIII. POLICY ITEMS

A. Access is strictly controlled, using network and password authentication.
    a. Permission from the employee's Vice President is required for all VPN access.
    b. Access is reserved for:
        i. Employees that need 24 hour access to network resources.
        ii. Employees required to work from an external location
B. Employees with access privileges must ensure that the VPN connection to SCNM's network is not used by non-employees to gain access to any SCNM resources.
    a. An employee who is granted access privileges must remain constantly aware that VPN connections between their location and SCNM are literal extensions of SCNM's network, and that they provide a potential path to the College's most sensitive information.
    b. The employee and/or authorized third party individual must take every reasonable measure to protect SCNM's assets.
C. Only SCNM configured laptops are considered secure enough for connection to SCNM's network.
D. Users granted VPN access must comply with IT's accepted VPN access methods.
    a. VPN software is setup and configured by IT.
    b. Tampering or altering of the VPN client software will result in disciplinary action, up to and including revocation of VPN account privileges and disciplinary action up to and including employment termination.
    c. VPN client software will not be installed on non-SCNM computers (no personal home computing devices will be accepted).
E. Enforcement
    a. Connection activity may be monitored. Unauthorized moving of files across the VPN that contain sensitive or private patient or student information will result in revocation of account access privilege OR extended disciplinary actions when warranted. Violations of this policy may be subject to disciplinary action, up to and including termination of employment.

IX. RESPONSIBILITY FOR IMPLEMENTATION

Network Administrator

X. APPROVAL BODY

President's Council

XI. DATE POLICY APPROVED

February 23, 2011

I.T. VPN Remote Access Policy

XII. RELATED POLICIES

IT Acceptable Use Policy

XIII. RELATED DOCUMENTS

Form: User/Employee Agreement for VPN Access

XIV. DATE EFFECTIVE

February 24, 2011

XV. NEXT REVIEW DATE

As needed

XVI. VERSION CONTROL AND CHANGE HISTORY

Version Control	Approved By/Date	Date Effective	Amendment
1	President's Council/ February 23, 2011	February 24, 2011	
2			

XVII. POLICY OWNER

Information Technology Department

XVIII. POLICY AUTHOR/CONTACT

Stan Zalewski/Director IT