Information Services & Technology
Virtual Private Network (VPN) Policy

I. PURPOSE

The purpose of this policy is to provide guidelines for Remote Access IPSec or L2TP Virtual Private Network (VPN) connections to the UMDNJ network.

II. APPLICABILITY

This policy applies to all UMDNJ employees, contractors, consultants, temporaries, and other workers including all personnel affiliated with third parties utilizing VPNS to access the UMDNJ network. This policy applies to implementations of VPN that are directed through an IPSec Concentrator.

III. ACCOUNTABILITY

Under the President, the Senior Vice Presidents shall insure compliance with this policy. The Vice President for Information Systems and Technology (IST), the President/CEOs of the Healthcare Units, Deans and Vice Presidents shall implement this policy by means of system specific procedures, guidelines and standards.

IV. DEFINITIONS

IPSec Concentrator - A device in which VPN connections are terminated.
VPN - Virtual Private Networks offer secure communications between network applications using a public or unsecured medium such as the Internet through the use of various technologies offering secure user authentication, data integrity, data confidentiality and access control.

V. POLICY

Approved UMDNJ employees and authorized third parties (customers, vendors, etc.) may utilize the benefits of VPNS, which are 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 fees. Further details may be found in the Remote Access Policy.

Additionally,

A. It is the responsibility of employees with VPN privileges to ensure that unauthorized users are not allowed access to UMDNJ internal networks.

B. VPN use is to be controlled using either a one-time password authentication such as a token device or a public/private key system with a strong pass phrase.

C. When actively connected to the UMDNJ network, VPNS will force all traffic to and from the device over the VPN tunnel; all other traffic will be dropped.

D. Dual (split) tunneling is NOT permitted; only one network connection is allowed.

E. VPN gateways will be set up and managed by UMDNJ network operational groups.

F. All computers connected to UMDNJ internal networks via VPN or any other technology must use the most up-to-date anti-virus software that is the University standard. This includes personal computers.
G. VPN users will be automatically disconnected from UMDNJ's 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.

H. The VPN concentrator is limited to an absolute connection time of 24 hours. Under IS&T Security Team approval, connection time can be adjusted based on business needs and/or technical specifications.

I. Users of computers that are not UMDNJ-owned equipment must configure the equipment to comply with UMDNJ's VPN and Network policies.

J. Only IS&T Security-approved VPN clients may be used.

K. By using VPN technology with personal equipment, users must understand that their machines are a de facto extension of UMDNJ's network, and as such are subject to the same rules and regulations that apply to UMDNJ-owned equipment, i.e., their machines must be configured to comply with IS&T Security's Security Policies.

VI. NONCOMPLIANCE AND SANCTIONS

Any person found to have violated this policy may be subject to denial or removal of access privileges to the University network; disciplinary action, under applicable University policies and procedures up to and including termination; civil litigation; and/or criminal prosecution under applicable state and federal statutes.