PAUL J. FETHERSTON
TOWN MANAGER

TOWN OF NEWINGTON

131 CEDAR STREET
NEWINGTON, CONNECTICUT 06111

OFFICE OF THE TOWN MANAGER

Information Technology Policy
Effective Immediately
February 1, 2005

SUBJECT : Virtual Private Network (VPN) Policy

PURPOSE : To provide guidelines for Remote Access IPSec or L2TP Virtual Private Network (VPN) connections to the Town of Newington's (hereinafter Town) communication networks.

APPLICABILITY: This policy applies to all Town employees, contractors, consultants, temporaries, and other workers including all personnel affiliated with third parties utilizing VPNs to access the Town's communication networks. This policy applies to implementations of VPN that are directed through a VPN/IPSec Concentrator.

1.0 Policy

Authorized Town 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.

2.0 Additionally

2.1. It is the responsibility of employees with VPN privileges to ensure that unauthorized users are not allowed access to Town's communication networks.

2.2. 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.

2.3. When actively connected to the Town's communication networks, VPNs will force all traffic to and from the PC over the VPN tunnel: all other traffic will be dropped.

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

2.5. VPN gateways will be set up and managed by Information Systems and Technology.

2.6. All computers connected to Town's communication networks via VPN or any other technology must use approved/ up-to-date anti-virus software application and an approved firewall; this includes personal computers.

2.7. VPN users will be automatically disconnected from the Town's communication networks 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.

2.8. The VPN concentrator is limited to an absolute connection time of 24 hours.

2.9. Users of computers that are not Town owned equipment must configure the equipment to comply with Town's VPN, Acceptable Use Policy and/ or other policies effecting the Town's communication networks.

2.10. Only Information Systems and Technology-approved VPN clients may be used.

2.11. By using VPN technology with personal equipment, users must understand that their machines are a de facto extension of Town's communication networks, and as such are subject to the same rules and regulations that apply to Town's owned/operated equipment, i.e., their machines must be configured to comply with Information Systems and Technology Security Policies.

Phone: (860) 665-8510 Fax: (860) 665-8507
townmanager@ci.newington.ct.us
www.ci.newington.ct.us

3.0 Enforcement

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

4.0 Definitions

Term	Definition
IPSec Concentrator	A device in which VPN connections are terminated.
VPN	Virtual Private Network

_____
Paul J. Fetherston
Town Manager