Policy: Virtual Private Network (VPN)

Issuing Dept: Information Technology

Effective Date: 1-1-2014

Approved By:

1/8/14

John M. Lewis, Jr.
Chief Executive Officer

SCOPE

This Policy applies to all Central Florida Regional Transportation Authority contractors, consultants, and other workers including all personnel affiliated with third parties utilizing VPNs to access the Central Florida Regional Transportation Authority network. This Policy applies to implementations of all VPN that are directed through any type VPN Concentrator or software.

POLICY

Approved Central Florida Regional Transportation Authority authorized third parties (contractors, consultants, vendors, etc.) will utilize the VPN to remotely support the applications for which they are responsible. The third party utilizing the VPN is responsible for selecting an Internet Service Provider (ISP), coordinating installation, installing any required software, and paying associated fees to connect to LYNX' VPN solution.

Additionally,
1. A Signed copy of this policy must be returned to Central Florida Regional Transportation Authority's Information Technology Department before access is granted.

2. It is the responsibility of entity with VPN privileges to ensure that unauthorized users are not allowed access to Central Florida Regional Transportation Authority internal networks via their VPN.

3. VPN use is to be controlled using password authentication. When actively connected to the administrative network, VPNs will force all traffic to and from the PC over the VPN tunnel: all other traffic will be dropped.

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

5. VPN gateways will be set up and managed by the Central Florida Regional Transportation Authority Information Technology Department.

6. All computers connected to Central Florida Regional Transportation Authority internal networks via VPN or any other technology must use the most up-to-date anti-virus software that is the administrative standard. Information on this software can be obtained from Central Florida Regional Transportation Authority Technical Support (phone: 407-254-6035, email: helpdesk@golynx.com); this includes personal computers.

7. All computers connected to Central Florida Regional Transportation Authority internal networks via VPN must have the latest operating system security patches applied. Information on these patches can be obtained from Central Florida Regional Transportation Authority Technical Support or manufacture of the software.

8. Users of computers that are not Central Florida Regional Transportation Authority-owned equipment must configure the equipment to comply with Central Florida Regional Transportation Authority's VPN and Network policies.

9. Only Central Florida Regional Transportation Authority Information Technology's approved VPN clients may be used.

10. By using VPN technology with personal equipment, users must understand that their machines are a de facto extension of Central Florida Regional Transportation Authority's network, and as such are subject to the same rules and regulations that apply to Central Florida Regional Transportation Authority-owned equipment, i.e., their machines must be configured to comply with all Central Florida Regional Transportation Authority Security Policies.

11. Peer-to-peer software is not allowed over VPN.

12. Computer with multiple user accounts (ie true multiuser hosts) are not allowed to create VPN connections to the trusted network for the entire host and its users. Note: At this time we know of no way to allow single user VPN connections on multiuser computers.

13. Third parties (contractors, consultants, vendors, etc.) are restricted to only accessing the systems that are in their scope of responsibility.

Enforcement

Anyone found to have violated this Policy may have their network access privileges temporarily or permanently revoked.

Florida has very broad public records laws. All users are required to abide by the Florida Sunshine laws.

While connected any disruption to service must be reported immediately to the point of contact on file. Notification of any possible service effecting conditions must be reported immediately, these include but not limited to viruses and malware, found on computer/s or networks used to connect to LYNX' network.

PROCEDURES AND RESPONSIBILITIES

Information Technology Department is responsible for setting up the VPN on LYNX' network, collecting the signed copy of this policy, and for monitoring the use of the VPN system.

REPLACES: This is the first formal policy for allowing contractors the use of VPN technology for the purpose of monitoring, repairing, supporting software or other technology remotely.

Company:_____

Contractor Signature:_____

Title:_____

Date:_____

Agency Signature: _____

Title:_____

Date:_____