Cyber Tree Systems
A Business IT Solution Company

POLICY NAME	**Virtual Private Network (VPN) Policy**		
DATE OF LAST REVISION:	10/2/2003	**VERSION NO.**	1.43
ADMINISTRATOR RESPONSIBLE	Kevin McKnight		

Purpose

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

Scope

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

Policy Statement

Approved CTS 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,

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

- VPN use is to be controlled using either a onetime password authentication such as a token device or a public/private key system with a strong passphrase.

- When actively connected to the corporate network, VPNs will force all traffic to and from the PC over the VPN tunnel: all other traffic will be dropped.

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

- VPN gateways will be set up and managed by CTS network operational groups.

- All computers connected to CTS internal networks via VPN, or any other technology must use the most up-to-date anti-virus software that is the corporate standard (provide URL to this software); this includes personal computers.

- VPN users will be automatically disconnected from CTS's network after thirty minutes of inactivity. The user must then log on again to reconnect to the network. Pings or other artificial network processes are not to be used to keep the connection open.

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

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

- Only InfoSec-approved VPN clients may be used.

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

Responsibilities and Ownership

When users are trying to access the CTS network, they will have to go through multi-factor authentication. This will send an alert to both the user and the administrator. By enforcing this kind of authentication, the network system will be monitored more effectively and prevent unauthorized access.

VPN Configuration and Requirement

Configuration for VPN can be the creation of digital certificates and key for identification and authentication purposes. This promotes a higher level of security.

Enforcement

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

Terms and Definitions

Define any acronyms, jargon, or terms that might have multiple meanings.

TERM	DEFINITION
IPSec Concentrator	A device in which VPN connections are terminated.
Virtual Private Network	A VPN is an encrypted connection over the Internet from a device to a network.

Revision History

Revisions made 9/4/2023
Revisions made 10/2/2023