Cyber Tree Systems
A Business IT Solution Company

POLICY NAME	**Remote Access**		
DATE OF LAST REVISION:	9/4/2003	**VERSION NO.**	1.43
ADMINISTRATOR RESPONSIBLE	Kevin McKnight		

Purpose

The purpose of this policy is to define standards for connecting to CTS's network from any host. These standards are designed to minimize the potential exposure to CTS from damage which may result from unauthorized use of CTS resources. Damages include the loss of sensitive or company confidential data, intellectual property, damage to public image, damage to critical CTS internal systems, etc.

Scope

This policy applies to all CTS employees, contractors, vendors, and agents with a CTS owned or personally owned computer or workstation used to connect to the CTS network. This policy applies to remote access connections used to do work on behalf of CTS, including reading or sending email and viewing intranet web resources.

Remote access implementations that are covered by this policy include, but are not limited to, dial-in modems, frame relay, ISDN, DSL, VPN, SSH, and cable modems, etc.

Policy Statement

- General Guidelines

  It is the responsibility of CTS employees, contractors, vendors, and agents with remote access privileges to CTS's corporate network to ensure that their remote access connection is given the same consideration as the user's on-site connection to CTS.

  General access to the Internet for recreational use by immediate household members through the CTS Network on personal computers is permitted for employees that have flat-rate services. The CTS employee is responsible for ensuring the family member does not violate any CTS policies, does not perform illegal activities, and does not use the access for outside business interests. The CTS employee bears responsibility for the consequences should the access be misused. Please review the following policies for details of protecting information when accessing the corporate network via remote access methods, and acceptable use of:

  CTS's network:

  - Acceptable Encryption Policy
  - Virtual Private Network (VPN) Policy
  - Wireless Communications Policy

        - • Acceptable Use Policy

        - • Cloud Services Policy

    For additional information regarding CTS's remote access connection options, including how to order or disconnect service, cost comparisons, troubleshooting, etc., go to the Remote Access Services website.

- Specific Requirements
    - Secure remote access must be strictly controlled. Control will be enforced via one-time password authentication or public/private keys with strong passphrases. For information on creating a strong passphrase, see the Password Policy.

    - At no time should any CTS employee provide their login or email password to anyone, not even family members.

    - CTS employees and contractors with remote access privileges must ensure that their CTS-owned or personal computer or workstation, which is remotely connected to CTS's corporate network, is not connected to any other network at the same time, except for personal networks that are under the complete control of the user.

    - CTS employees and contractors with remote access privileges to CTS's corporate network must not use non-CTS email accounts (i.e., Hotmail, Yahoo, AOL), or other external resources to conduct CTS business, thereby ensuring that official business is never confused with personal business.

    - Routers for dedicated ISDN lines configured for access to the CTS network must meet minimum authentication requirements of CHAP.

    - Reconfiguration of a home user's equipment for the purpose of split-tunneling or dual-homing is not permitted at any time.

    - Frame Relay must meet minimum authentication requirements of DLCI standards.

    - Non-standard hardware configurations must be approved by Remote Access Services, and InfoSec must approve security configurations for access to hardware.

    - All hosts that are connected to CTS internal networks via remote access technologies must use the most up-to-date anti-virus software (place URL to corporate software site here); this includes personal computers. Third party connections must comply with requirements as stated in the Third-Party Agreement.

    - Personal equipment that is used to connect to CTS's networks must meet the requirements of CTS-owned equipment for remote access.

    - Organizations or individuals who wish to implement non-standard Remote Access solutions to the CTS production network must obtain prior approval from Remote Access Services and InfoSec.

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
Cable Mode	Cable companies such as AT&T Broadband provide Internet access over Cable TV coaxial cable. A cable modem accepts this coaxial cable and can receive data from the Internet at over 1.5 Mbps. Cable is currently available only in certain communities.
CHAP	Challenge Handshake Authentication Protocol (CHAP) is an authentication method that uses a one-way hashing function. DLCI Data Link Connection Identifier (DLCI) is a unique number assigned to a Permanent Virtual Circuit (PVC) endpoint in a frame relay network. DLCI identifies a particular PVC endpoint within a user's access channel in a frame relay network and has local significance only to that channel.
Dial-in Modem	A peripheral device that connects computers to each other for sending communications via the telephone lines. The modem modulates the digital data of computers into analog signals to send over the telephone lines, then demodulates back into digital signals to be read by the computer on the other end; thus, the name "modem" for modulator/demodulator.
Dual Homing	Having concurrent connectivity to more than one network from a computer or network device. Examples include Being logged into the corporate network via a local Ethernet connection, and dialing into AOL or other Internet service provider (ISP). Being on a CTS provided Remote Access home network, and connecting to another network, such as a spouse's remote access. Configuring an ISDN router to dial into CTS and an ISP, depending on packet destination.
DSL	Digital Subscriber Line (DSL) is a form of high-speed Internet access competing with cable modems. DSL works over standard phone lines and supports data speeds of over 2 Mbps downstream (to the user) and slower speeds upstream (to the Internet).
Frame Relay	A method of communication that incrementally can go from the speed of an ISDN to the speed of a T1 line. Frame Relay has a flat rate billing charge instead of a per time usage. Frame Relay connects via the telephone company's network.
ISDN	There are two flavors of Integrated Services Digital Network or ISDN: BRI and PRI. BRI is used for home office/remote access. BRI has two "Bearer" channels at 64kbit (aggregate 128kb) and 1 D channel for signaling info.
Remote Access	Any access to CTS's corporate network through a non-CTS controlled network, device, or medium.
Split-tunneling	Simultaneous direct access to a non-CTS network (such as the Internet, or a home network) from a remote device (PC, PDA, WAP phone, etc.) while connected into CTS's corporate network via a VPN tunnel. VPN Virtual Private Network (VPN) is a method for accessing a remote network via "tunneling" through the Internet.

Revision History

Revisions made 9/4/2023