

# Remote Access Policy

## 1.0 Purpose

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

## 2.0 Scope

This policy applies to all Tennessee Bureau of Investigation employees, contractors, vendors and agents with a TBI-owned or personally owned computer or workstation used to connect to the Tennessee Bureau of Investigation network. This policy applies to remote access connections used to do work on behalf of TBI, 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.

## 3.0 Policy

### 3.1 General

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

### 3.2 Requirements

1. Secure remote access must be strictly controlled. Control will be enforced via certificate and strong password authentication or public/private keys with strong passwords. For information on creating a strong password see the Password Policy.
2. At no time should anyone with access to TBI resources provide his or her login or email password to anyone, not even family members.
3. TBI employees and contractors with remote access privileges must ensure that their TBI-owned or personal computer or workstation, which is remotely connected to the TBI network, is not connected to any other network at the same time, with the exception of networks that are under the complete control of the user.
4. Tennessee Bureau of Investigation employees and contractors with remote access privileges to TBI's network must not use non-TBI email accounts (i.e., Hotmail, Yahoo, AOL), or other external resources to conduct official TBI business, thereby ensuring that official business is never confused with personal business.
5. Reconfiguration of a home user's equipment for the purpose of split-tunneling or dual homing is not permitted at any time.
6. Non-standard hardware configurations must be approved by the Technical Support Services Unit.
7. All hosts that are connected to TBI networks via remote access technologies must use the most up-to-date anti-virus software (ie. [www.symantec.com](http://www.symantec.com)) this includes personal computers.
8. Personal equipment that is used to connect to TBI's networks must meet the requirements of TBI-owned equipment for remote access.
9. Organizations or individuals who wish to implement non-standard Remote Access solutions to the Tennessee Bureau of Investigation production network must obtain prior approval from the Technical Support Services Unit.

## 4.0 Enforcement

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

## 5.0 Definitions

Term	Definition
------	------------

Cable Modem	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 is an authentication method that uses a one-way hashing function. DLCIData Link Connection Identifier ( DLCI) is a unique number assigned to a Permanent Virtual Circuit (PVC) end point 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 Tennessee Bureau of Investigation-provided Remote Access home network, and connecting to another network, such as a spouse's remote access. Configuring an ISDN router to dial into Tennessee Bureau of Investigation 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 Tennessee Bureau of Investigation's corporate network through a non-Tennessee Bureau of Investigation controlled network, device, or medium.
Split-tunneling	Simultaneous direct access to a non-Tennessee Bureau of Investigation network (such as the Internet, or a home network) from a remote device (PC, PDA, WAP phone, etc.) while connected into Tennessee Bureau of Investigation'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.

## 6.0 Revision History

THIS AGREEMENT will become effective on \_\_\_\_\_

IN WITNESS WHEREOF, the parties hereto caused this Agreement to be executed by the proper

officers and officials.

---

Mark R. Gwyn, Director

---

Date

---

Agency Representative

---

Date