doit

STATE OF MARYLAND
DEPARTMENT OF INFORMATION TECHNOLOGY

Remote Access Policy

1.0 Purpose

The purpose of this policy is to define requirements for connecting to DoIT's network (or any network managed by DoIT) from an outside entity. These requirements are designed to minimize the potential exposure to DoIT from damages which may result from unauthorized use of DoIT resources. Damages include the loss of sensitive or confidential information, damage to public image and damage to critical DoIT internal systems.

2.0 Scope

This policy applies to all DoIT employees, contractors, vendors and agents with a DoIT-owned or personally-owned computer used to connect to the DoIT network. This policy applies to remote access connections used to perform work on behalf of DoIT 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, WiFi and cable modems.

3.0 Policy

3.1 General

1. Storage of confidential information on any non-state owned device is prohibited. Confidential information may not be stored on any state owned portable device without prior written approval from agency Secretary (or delegated authority). Approved storage on any portable device must be encrypted.
2. It is the responsibility of DoIT employees and contractors with remote access privileges to DoIT's corporate network to ensure that their remote access connection is given the same consideration as the user's on-site connection to DoIT.
3. All remote access users are expected comply with DoIT policies, may not perform illegal activities, and may not use the access for outside business interests.

3.2 Requirements

1. Remote access must be strictly controlled by the use of unique user credentials. For information on creating a strong password please review DoIT's Password Policy & Guidelines.
2. Remote access passwords are to be used only by the individual to whom they were assigned and may not to be shared.

3. All remote access connections that utilize a shared infrastructure, such as the Internet, must utilize some form of encryption. For information on acceptable encryption technologies please review DoIT’s Acceptable Encryption Policy.
4. Reconfiguration of a home user's equipment for the purpose of split-tunneling or dual homing is not permitted at any time.
5. All hosts that are connected to DoIT internal networks via remote access technologies must have up-to-date anti-virus software implemented.
6. All hosts that are connected to DoIT internal networks via remote access technologies must have current operating system security patches installed.
7. Personal equipment that is used to connect to DoIT’s networks must meet the requirements of DoIT-owned equipment for remote access.
8. Organizations or individuals who wish to implement non-standard Remote Access solutions to the DoIT production network must obtain prior approval from DoIT.

4.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment. Deliberate, unauthorized disclosure of confidential information may result in civil and/or criminal penalties.

5.0 Definitions

Term	Definition
Cable Modem	Cable companies provide Internet access over Cable TV coaxial cable. A cable modem accepts this coaxial cable and can receive data from the Internet.
Dial-in Modem	A peripheral device that connects computers to each other for sending communications via the telephone lines.
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).
DSL	Digital Subscriber Line (DSL) is a form of high-speed Internet access competing with cable modems.
Remote Access	Any access to DoIT’s corporate network through a non-DoIT controlled network, device, or medium.
Split-tunneling	Simultaneous direct access to a non-DoIT network (such as the Internet, or a home network) from a remote device (PC, PDA, WAP phone, etc.) while connected into DoIT’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.
Wi-Fi	Wireless networking technology that uses radio waves to provide wireless high-speed Internet and network connections. A Wi-Fi enabled device such as a PC, mobile phone, or PDA can connect to the Internet when within range of a wireless network.

6.0 Revision History