STATE OF ALABAMA

Information Technology Policy

POLICY 622-00: REMOTE ACCESS

The increasing mobility of State employees has made remote access to State network resources vital to conducting State business. State employees, contractors, vendors and business partners with remote access privileges to the State network need to ensure that remote access connections are given the same consideration as on-site connections with respect to acceptable use, anti-virus, and other security measures. Agency IT personnel need to ensure that remote access technologies are deployed in a manner that ensures State systems maintain acceptable levels of security and service.

OBJECTIVE:

Set forth responsibilities for authorizing, administering, and using remote access capabilities for individual access to State network resources.

SCOPE:

This policy applies to all Executive Branch agencies, boards, and commissions except those exempt under The Code of Alabama 1975 (Title 41 Chapter 4 Article 11).

RESPONSIBILITIES:

Agency Management, Information Technology Organization:

Document allowed methods of remote access to organizational information systems. Establish usage restrictions and implementation guidance for each allowed remote access method.

Monitor for unauthorized remote access to the information system. Monitor remote access systems and points of entry to the trusted network to detect unauthorized access attempts and other security weaknesses.

Authorize remote access to the information system prior to connection. Access to State network resources from remote locations (including but not limited to homes, hotel rooms, wireless devices and off-site offices) is not automatically granted to users in conjunction with network or system access. State employees and authorized third parties (consultants, vendors, etc.) may utilize remote access capabilities only with written approval of the appropriate authority. Document access request-approval procedures.

Enforce requirements for remote connections to organizational information systems.

Review remote access authorizations at least annually.

ADDITIONAL REQUIREMENTS:

The preferred method of remote access to State network resources is through a centrally managed Virtual Private Network (VPN) connection that provides encryption and secure authentication in accordance with State VPN standards.

Do not divulge details or instructions regarding remote access, including external network access points or dial-up numbers except to those requesters that have been verified as authorized to connect to the State network as an external user.

All hosts, including publicly and privately owned personal computers and other remote access devices, connecting remotely to State networks shall have up-to-date and properly configured anti-virus software and current operating system service pack and patch level. Hosts may be scanned to ensure compliance with State standards. Users may be denied remote access if their host system presents an unacceptable risk to State networks.

Place dial-in users under the same access policy as those connecting via VPN by placing the remote access server either in the DMZ or within a screened subnet where the VPN gateway resides.

Routers for dedicated ISDN lines configured for access to the State network must meet minimum authentication requirements of CHAP (Challenge Handshake Authentication Protocol).

Dual-homing is not permitted.

Secure remote access shall be strictly controlled. Where possible, control will be enforced via one-time password authentication or public/private keys with strong pass-phrases.

With the exception of web servers or other systems where all regular users are anonymous, users are prohibited from remotely logging into any State system or network anonymously (for example, by using “guest” user IDs).

Terminate remote access accounts in accordance with State network and system access policy and standards.

Revoke remote access authorization when necessary for reasons including, but not limited to, changes in employment, contract termination, non-compliance with security policies, request by the system/data owner, or negative impact on overall network performance attributable to remote access communications.

Enforce a limit of not more than 10 consecutive invalid access attempts by a user during a 15-minute time period. The information system shall automatically lock the account/node when the maximum number of unsuccessful attempts is exceeded. Due to the potential for denial of service, automatic lockouts may be automatically released after 15 minutes.

Apply a session time-out that terminates all sessions and requires re-authentication after no more than 15 minutes of inactivity (30 minutes for CICS). Users shall not circumvent this control by deploying automated software mechanisms, or any other strategies, to prevent session time-outs.

SUPPORTING DOCUMENTS:

- Information Technology Policy 621: Network and Systems Access
- Information Technology Standard 622S1: Virtual Private Networks
- Information Technology Standard 622S2: Dial-In Access/Modem Use

By Authority of Director, Information Services Division, Department of Finance

DOCUMENT HISTORY:

Version	Release Date	Comments
622-00	09/01/2011	Replaces Policy 640-02 and Standard 640-02S1 (both are hereby rescinded)