STATE OF ALABAMA

Information Technology Standard

STANDARD 622S1-00: VIRTUAL PRIVATE NETWORKS

A Virtual Private Network (VPN) is a private data network that makes use of the public telecommunication infrastructure, maintaining privacy through the use of a tunneling protocol and security procedures. VPN is the preferred method for users to remotely access (from homes, hotels, off-site offices, etc.) State of Alabama information system resources.

OBJECTIVE:

Define requirements for secure remote access VPN connections into the State network.

SCOPE:

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

REQUIREMENTS:

Based on the recommendations of the National Institute of Standards and Technology (NIST) as set forth in Special Publication (SP) 800-77: Guide to IPsec VPNs, and SP 800-113: Guide to SSL VPNs, State of Alabama organizations that deploy and/or manage virtual private networks shall comply with the following requirements:

VPN MANAGEMENT

Requests for VPN connectivity require the written approval of the agency IT Manager.

VPN connections with business partners and other non-State entities require a written interconnection agreement defining the rules of behavior and security controls that must be maintained and the terms and conditions for sharing data and information resources.

Create and document an access control policy listing the resources that will be accessed through the VPN, the groups or users, the conditions under which the resources should be accessible by the groups, and how the VPN should be used to access the resources. Limit access to specific and necessary information resources.

VPN connections shall allow for monitoring.

To assist in troubleshooting and maintenance, VPN configuration information and technical controls shall be documented.

VPN access accounts shall be reviewed at least quarterly. Inactive accounts shall be disabled in accordance with access management requirements (State IT Policy 621: Network and System Access).

VPN access may be terminated at any time for reasons including, but not limited to, termination of service provider agreements, changes in or termination of employment, request by the system/data owner, non-compliance with security policies, or negative impact on overall network performance attributable to VPN communications.

VPN ADMINISTRATION

Authentication:

Enforce user authentication at the access point before granting VPN access to State network resources. VPN access and authentication shall comply with applicable network access policies and procedures (including password standards, log-in attempts, lock-out policy, etc).

Users will authenticate using their domain login when a trust relationship is established between the RADIUS server and the user's Domain Controller.

When a trust relationship cannot be established, create locally administered user accounts on either the RADIUS server or the VPN Concentrator.

Secure Host:

Systems and networks at the VPN endpoints must meet all the security policies and standards applicable to other State systems and networks.

All hosts, including publicly and privately owned personal computers and other remote access devices, connected to State networks via VPN must 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, and users may be denied VPN access if their host system presents an unacceptable risk to State networks.

Technical Controls:

VPN communications shall utilize encryption consistent with State encryption policy.

Terminate the VPN on or outside the firewall such that VPN traffic is visible to network intrusion detection/prevention systems.

Split tunneling is not permitted. All traffic to and from the VPN client shall be routed through the VPN tunnel; all other traffic shall be dropped.

Users connected via VPN shall not be allowed simultaneous access to the Internet.

Log VPN activity and establish log review procedures. At a minimum, VPN devices shall log all successful and failed login attempts.

Monitor VPN usage and test VPN security controls on a regular basis (at least quarterly) for security and performance.

Any unusual VPN event that may indicate unauthorized use of VPN services shall immediately be reported as a cyber security incident following applicable reporting procedures.

SUPPORTING DOCUMENTS:

- Information Technology Policy 622: Remote Access
- Information Technology Policy 621: Network and System Access
- Information Technology Policy 683: Encryption

By Authority of the Office of IT Planning, Standards, and Compliance

DOCUMENT HISTORY:

Version	Release Date	Comments
640-02S2	2/16/2007	Original document
640-02S2_A	2/13/2009	Added requirements for access control policy, documentation, session time-out, logging, and quarterly testing of security controls.
622S1-00	09/01/2011	New number and format