



STATE OF ALABAMA

OFFICE OF INFORMATION TECHNOLOGY



STANDARD 636S1: Virtual Private Network

VERSION NUMBER	Standard 636S1-01
VERSION DATE	July 30, 2019
STANDARD TITLE	Virtual Private Network (VPN)
GOVERNING POLICY	This standard is governed by Policy 636: Remote Access, regardless of revision.
OBJECTIVE	Establish and document usage restrictions, configuration and connection requirements, and implementation guidance for remote access into state IT resources utilizing VPN. [AC-17a.]
REQUIREMENTS	<p>State of Alabama organizations that deploy or manage VPN must comply with the following requirements:</p> <ol style="list-style-type: none">1. VPN MANAGEMENT<ol style="list-style-type: none">1.1. Requests for VPN connectivity require the written approval of the agency IT Manager.1.2. VPN connections with business partners and other non-state entities require a written interconnection agreement defining the rules of behavior, maintenance of security controls, terms and conditions for sharing data and information resources between parties.1.3. 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.1.4. VPN connections must be configured to allow a network administrator to monitor and control connections at the network boundary.1.5. To assist in troubleshooting and maintenance, VPN configuration information and technical controls must be documented.

- 1.6. VPN access accounts shall be reviewed quarterly. Inactive accounts shall be disabled after no more than 120 days of inactivity.
- 1.7. 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 or data owner, non-compliance with security policies, or negative impact on overall network performance attributable to VPN communications.
- 1.8. Log VPN activity and establish log review procedures. At a minimum, VPN devices must log all successful and failed login attempts. Review activity logs monthly.
- 1.9. Monitor VPN usage and test VPN security controls on a regular basis (quarterly) for security and performance.

2. AUTHENTICATION

- 2.1. Enforce user authentication at the access point before granting VPN access to state network resources. VPN access and authentication must comply with applicable network access policies and procedures (including password standards, log-in attempts, lock-out policy, etc.).
- 2.2. Users will authenticate using their domain login when a trust relationship is established between the RADIUS server and the user's Domain Controller.
- 2.3. When a trust relationship cannot be established, create locally administered user accounts on either the RADIUS server or the VPN Concentrator.

3. SECURE HOST

- 3.1. Systems and networks at the VPN endpoints must meet all the security policies and standards applicable to other state systems and networks.
- 3.2. 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.
- 3.3. 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.

4. TECHNICAL CONTROLS

- 4.1. VPN connections must be encrypted using Federal Information Processing Standard (FIPS) 140-2 validated cryptographic modules.
- 4.2. Terminate the VPN on or outside the firewall such that VPN traffic is visible to network intrusion detection or prevention systems.
- 4.3. Split tunneling is not permitted. All traffic to and from the VPN client, including public network and Internet traffic, shall be routed through the VPN tunnel; all other traffic shall be dropped.
- 4.4. Any unusual VPN event that may indicate unauthorized use of VPN services must be reported immediately as a cyber security incident following applicable reporting procedures.

SUPPORTING DOCUMENTS

The following documents support this standard:

- [Policy 636: Remote Access](#)

The following special publications (SP) of the National Institute of Standards and Technology (NIST) support this standard and may aid in its implementation:

- NIST SP 800-77: Guide to IPsec VPNs
- NIST SP 800-113: Guide to SSL VPNs

EFFECTIVE DATE

This standard is effective upon its approval by the Secretary of Information Technology, as evidenced by the signature of the Secretary being affixed hereto.

SUPERSEDES

This standard supersedes legacy Standard 622S1: Virtual Private Networks.

The undersigned, as Acting Secretary of Information Technology of the State of Alabama, exercising the power vested in that Office by the laws of this state, declares this standard to be adopted as of the _____ day of _____, 2019.

Marty Redden
Acting Secretary of Information Technology

DOCUMENT CHANGE HISTORY

Version	Version Date	Comments
636S1-01	07/30/2019	Initial version

DRAFT