KAY IVEY
Governor

STATE OF ALABAMA

OFFICE OF INFORMATION TECHNOLOGY

JIM PURCELL
Acting Secretary

POLICY 636: Remote Access

VERSION NUMBER	Policy 636-01
VERSION DATE	September 25, 2018
POLICY TITLE	Remote Access
OBJECTIVE	Set forth responsibilities for authorizing, administering, and using remote access capabilities for individual access to state network resources.
AUTHORITY	The authority of the Office of Information Technology (OIT) to create and enforce policies relating to the management and operation of IT by state agencies, and exceptions to such authority, are derived from: *Articles 8 and 11 of Chapter 4 of Title 41, and Chapter 28 of Title 41, Code of Alabama 1975 (Acts 2013-68 and 2017-282).* Policies of the OIT are approved and signed by the Governor.
APPLICABILITY	The requirements and responsibilities defined in OIT policies apply to all departments, agencies, offices, boards, commissions, bureaus, and authorities (referred to generally as *agency* or *agencies*) and authorized individuals in the employment of the State of Alabama responsible for the management, operation, or use of state IT.
STATEMENT OF POLICY	The increasing mobility of state employees has made remote access to 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 owned information systems maintain acceptable levels of security and service.

It is the policy of the OIT that:

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

b) All hosts, including publicly and privately owned personal computers and other remote access devices, connecting remotely to state owned networks shall have up-to-date and properly configured anti-virus software and current operating system service pack and patch level.

c) The System Owner may deny remote access if an information system presents an unacceptable risk to state information system assets and networks.

d) Anonymous logon shall be prohibited for remote access of information systems or network resources (except for web servers or other systems where all regular users are anonymous).

e) State employees and authorized third parties (consultants, vendors, etc.) may utilize remote access capabilities only with written approval of the appropriate agency authority.

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

g) Locate 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.

h) Logon setting will enforce a limit of not more than 10 consecutive invalid access attempts by a user during a 15-minute period. The logon credentials shall automatically lock the account/node when the maximum number of unsuccessful attempts is exceeded.

i) Remote access security shall be strictly controlled. Where possible, control will be enforced via multi-factor authentication, one-time password authentication or public/private keys with strong pass-phrases.

j) Session time-outs shall be applied that terminates all sessions and requires re-authentication after no more than 15 minutes of inactivity (30 minutes for CICS).

OIT RESPONSIBILITIES

Establish usage restrictions and implementation guidance for each allowed remote access methodology.

Monitor remote connection traffic and points of entry into network to detect unauthorized access attempts and unusual or unauthorized conditions.

Configure network firewalls to alert network security personnel following indication of preconfigured compromise thresholds.

Employ automated tools to support real-time or near real-time monitoring and analysis of network traffic.

Monitor for unauthorized remote access connections to state information systems or network resources.

Implement encryption on remote connections in accordance with federal laws, state laws, policies, regulations, and standards to protect the confidentiality and integrity of remote access sessions.

AGENCY RESPONSIBILITIES

Agencies that manage their own network or systems shall also be responsible for items stated in the "OIT RESPONSIBILITIES" section above.

Configure information systems to route all remote access connections through designated state managed network access control points.

Document access request approval procedures including allowed methods of remote access to organizational information systems.

Authorize remote access to information systems prior to connection configuration and implementation. 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.

Enforce requirements for remote connections to organizational information systems.

Annually review remote access authorizations.

Terminate 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 or data owner, or negative impact on overall network performance attributable to remote access communications.

Authorize the execution of administrative (privileged) commands and access to security relevant information via remote access only when deemed necessary by agency executive management.

Document justification for elevated privileges of personnel utilizing remote access in agency information system security plan.

USER RESPONSIBILITIES

Users shall not divulge details or instructions regarding remote access procedures to access state information systems resources, including external network access points or website addresses

Users shall not circumvent remote access session time-out controls employing automated software mechanisms, or any other strategies, to prevent session time-outs.

SUPPORTING DOCUMENTS

The following documents support implementation of this policy:

- Standard 636S1: Virtual Private Network
- Standard 636S2: Dial-In Access

EFFECTIVE DATE

This policy shall be effective upon its approval by the Secretary of Information Technology and the Governor of Alabama as evidenced by the signatures of the Secretary and Governor being affixed hereto.

SUPERSEDES

This policy supersedes Policy 622: Remote Access.

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 policy to be adopted as of the date on which the Governor has approved and signed it.

_____

Jim Purcell
Acting Secretary of Information Technology

ORDERED

_____

Kay Ivey
Governor

This _____ day of _____, 2018.

DOCUMENT CHANGE HISTORY

Version	Version Date	Comments
636-01	09/25/2018	Initial version