



STATE OF ALABAMA

INFORMATION TECHNOLOGY POLICY



Policy 636: Remote Access

Document/Version: 636-01

Version Date: 03/15/2021 (draft)

Effective Date: TBD

OBJECTIVE

The objective of this policy is to define responsibilities for authorizing, administering, and using remote access capabilities for individual access to state network resources.

AUDIENCE

Information technology professionals responsible for authorizing and administering remote access to state network resources.

DEFINITION

Remote access is defined as any access to an agency information system by a user communicating through an external network (for example, the Internet).

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, malware protection, and other security measures.

It is the policy of OIT that:

- a) State employees and authorized third parties (consultants, vendors, etc.) may utilize remote access capabilities only with the authorization of the appropriate agency authority.
- b) Multifactor authentication shall be required for remote access to systems that receive, process, store, or transmit sensitive or confidential information (e.g., FTI or PII), for access by privileged users performing privileged functions, or as required by Policy 630: Identification & Authentication.
- c) Remote execution of privileged commands or remote access to security-relevant information or devices shall be authorized only for compelling operational need. [AC-17 (CE4 (a))]
- d) The preferred method of remote access to state information systems is through a centrally managed Virtual Private Network (VPN) connection that provides encryption and secure authentication in accordance with state VPN standards.

- e) If sensitive or confidential information is transmitted over the remote connection, implement cryptographic mechanisms to protect the confidentiality and integrity of the data. [AC-17 (CE2)]
- f) 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.

OIT RESPONSIBILITIES

OIT (and other agencies managing their own network or remote access points) shall:

- O.1 Establish and document usage restrictions, configuration and connection requirements, and implementation guidance for each type of remote access allowed. [AC-17a.]
- O.2 Monitor remote traffic connections and points of entry into the network to detect unauthorized access attempts and unusual or unauthorized conditions. [AC-17 (CE1)]
- O.3 Ensure that remote access technologies are deployed in a manner that ensures state information systems maintain acceptable levels of security, service, and risk.

AGENCY RESPONSIBILITIES

Agency IT personnel and information system owners shall:

- A.1 Document allowed methods of remote access to agency information systems and remote access request approval procedures.
- A.2 Authorize remote access to the information system prior to allowing remote connections. [AC-17b.]
- A.3 Configure information systems to route all remote access connections through designated state-managed network access control points. [AC-17 (CE3)]
- A.4 Authorize the execution of administrative (privileged) commands and access to security relevant information via remote access. [AC-17 (CE4 (a))]
- A.5 Document justification for elevated privileges in the information system security plan. [AC-17 (CE4 (b))]
- A.6 Review remote access authorizations at a minimum of semi-annually (treat as privileged accounts). [AC-2j.]

USER RESPONSIBILITIES

- U.1 Users shall protect from unauthorized use or disclosure information about remote access procedures or mechanisms used to access state information systems including network access points and website addresses. [AC-17 (CE6)]
- U.2 Users shall not circumvent remote access session time-out controls by employing automated software mechanisms or any other strategy to prevent session time-out.

SUPPORTING DOCUMENTS

The following documents support implementation of this policy:

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

AUTHORITY AND APPLICABILITY

This policy is promulgated under the authority granted OIT as described in Policy 101: IT Governance. Unless granted exemption by law or by procedure of Policy 101, the requirements and responsibilities defined in OIT policies apply to all Executive Branch departments, agencies, offices, boards, commissions, bureaus, and authorities and authorized individuals in the employment of or under contract with the State of Alabama and responsible for the management, operation, or use of State IT resources.

DOCUMENT CHANGE HISTORY

Version	Version Date	Comments
636-01	03/15/2021	Initial version