



STATE OF ALABAMA

INFORMATION TECHNOLOGY STANDARD



Standard 636S2: Dial-In Access and Modem Use

Document/Version: 636S2-01

Version Date: 03/15/2021 (draft)

Effective Date: TBD

OBJECTIVE

Protect the state's electronic information resources from inadvertent compromise by authorized personnel using a dial-in connection by highlighting the risks associated with modem access, prohibiting modem use except where required, and ensuring modems have been configured securely and are monitored effectively.

REQUIREMENTS

Dial-in access poses a considerable number of risks. A modem connection can bypass access controls the firewall provides, and expose the network to vulnerabilities the firewall was designed to protect against. State employees granted dial-in access privileges must remain constantly aware that dial-in connections between their location and the state are literal extensions of the state network and that they provide a potential path to the state's most sensitive information.

1. DIAL-IN ACCESS

- 1.1. State employees and authorized third parties (customers, vendors, etc.) may, with the IT Manager's or Director's written approval, use dial-in connections to gain access to the state network when no other viable option exists.
- 1.2. Dial-in accounts are considered "as needed" accounts. If a dial-in account is not used for a period of six months the account must be disabled. If dial-in access is subsequently required, the individual must request a new account. Along with justification as to why the user's dial-access was inactive for six months.
- 1.3. Dialing directly into or out of a system that is simultaneously connected to the state's network infrastructure is prohibited, except as required for remote maintenance. Remote maintenance connections must comply with all applicable state standards.
- 1.4. Dial-in access requires strong authentication consistent with identification and authentication policy and with remote access requirements.
- 1.5. 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.

- 1.6. It is the responsibility of employees with dial-in access privileges to ensure dial-in connections are not used by non-employees to gain access to state information system resources.
- 1.7. Account activity must be monitored and audited to ensure that malicious activity is not occurring.
2. MODEM USE
 - 2.1. The use of modems is generally prohibited except as described in this and other applicable policies and standards.
 - 2.2. Modems must not be part of the standard desktop computer hardware configuration.
 - 2.3. Modems must not utilize auto-answer mode such that they are able to receive incoming dial-up calls.
3. FAX AND MULTI-FUNCTION DEVICE MODEMS
 - 3.1. Fax machines and multi-function (fax/printer/copier) devices connected to the state network must have modems disabled (if so equipped) or configured such that they do not accept incoming calls.
 - 3.2. Fax or multi-function devices for which in-bound modem (dial-in) access is required shall not be connected to the state network.
4. EXEMPTION: Agencies requesting exemption from these requirements must include a migration plan addressing alternative to modem use and stating when compliance will be attained.

SUPPORTING DOCUMENTS

This document is governed by:

- [Policy 636: Remote Access](#)

Additional supporting documents:

- [Policy 630: Identification and Authentication](#)

DOCUMENT CHANGE HISTORY

Version	Version Date	Comments
636S2-01	03/15/2021	Initial version