



STATE OF ALABAMA

INFORMATION TECHNOLOGY POLICY



Policy 639: External Information Systems		
Document/Version: 639-01	Version Date: 03/17/2021 (draft)	Effective Date: TBD

OBJECTIVE Ensure connections to information systems external to state network systems are documented and properly secured.

AUDIENCE Information technology professionals responsible for authorizing, initiating, or maintaining connections between state-owned information systems and external (non-state) information systems.

STATEMENT OF POLICY Connections between state-owned information systems and external (non-state) information systems, including personally-owned devices, are often necessary for agencies to conduct government business; however, connecting a state information system to any unknown, un-trusted information system (where the security posture of the external system are unknown) is inherently risky.

It is the policy of OIT that:

- a) Processing, storing, or transmitting state data on non-state-owned computer systems or devices shall generally only be allowed by exception and shall require a signed agreement between the state entity and the non-state entity detailing the business need and security and privacy requirements.
- b) When connecting to external systems, configure state-owned information systems to provide only the essential functions needed to conduct agency business. [CM-7]
- c) System connectivity to external systems shall be constrained by employing a deny-all, allow by exception policy. System hosts shall determine what exceptions, if any, are acceptable. [CA-3 (CE5)]

OIT RESPONSIBILITIES OIT shall:
 O.1 Configure host information systems to provide only essential capabilities, and prohibit or restrict the use of functions, ports,

protocols, and services that are not necessary to support essential functionality. [CM-7]

- O.2 Review external connection requests to ensure access matches the necessary security controls to maintain integrity of the host network and information systems.
- O.3 Assist agencies with identifying applicable security controls and connection requirements to ensure external connections meet state cybersecurity standards prior to implementation.
- O.4 Continuously monitor external connections to the host enterprise network for security or performance issues.
- O.5 Conduct annual vulnerability assessments of external connections to monitor the risk to the state enterprise network and IT assets.

AGENCY RESPONSIBILITIES

Agencies shall:

- A.1 Establish and maintain documentation for each external connection describing the:
 - A.1.1 System interface characteristics,
 - A.1.2 Security and privacy requirements,
 - A.1.3 Sensitivity of the information communicated, and
 - A.1.4 Services and applications required.
- A.2 Restrict or prohibit the use of privately-owned computer systems to process, store, or transmit agency data in accordance with agency policy and/or federal directive.
- A.3 Establish restrictions on the use of portable storage devices connected to external information systems. [AC-20 (CE2)]
- A.4 Conduct semi-annual review of external connections and ensure they are closed when no longer required.

SUPPORTING DOCUMENTS

The following documents support this policy:

- [Standard 639S1: External System Connections](#)

The following special publication (SP) of the National Institute of Standards and Technology (NIST) supports this policy and may aid in its implementation:

- NIST SP 800-47: Security Guide for Interconnecting Information Technology Systems

**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
639-01	03/17/2021	Initial version; DRAFT