# STATE OF ALABAMA

## OFFICE OF INFORMATION TECHNOLOGY

KAY IVEY
Governor

MARTY REDDEN
Acting Secretary

# POLICY 639: External Information Systems

VERSION NUMBER

Policy 639-01

VERSION DATE

August 1, 2019

POLICY TITLE

External Information Systems

OBJECTIVE

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

AUTHORITY

The authority of the Office of Information Technology (OIT) to create and enforce policies relating to the management and operation of information technology (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 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

Connections between state-owned information systems and external (non-state) information systems 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 policies of the external system are unknown) is inherently risky. External information system connections are generally allowed only by exception.

It is the policy of OIT that:

a) Agencies shall document information system connection agreements or service level agreements (SLAs) with the organizational entity hosting the external information system.

b) Agencies shall document the implementation of required security controls on the external system connections (i.e., by third-party, independent assessments, attestations, or other means, depending on the confidence level required by agencies).

c) Agencies shall establish restrictions on the use of agency controlled portable storage devices being connected to external information systems. [AC-20 (CE2)]

d) Agencies shall restrict the use of non-agency owned computer systems or devices to process, store, or transmit agency data without a signed SLA detailing security control requirements.

e) Agencies shall restrict the use of privately-owned computer systems to process, store, or transmit agency data without prior agency management approval.

f) Organizations shall constrain system connectivity to external domains by employing a deny-all, allow by exception policy. Organizations shall determine what exceptions, if any, are acceptable. [CA-3 (CE5)]

g) Configure information systems to provide only essential capabilities, and prohibit or restrict the use of functions, ports, protocols, or services that are not necessary to support essential functionality. [CM-7]

## OIT RESPONSIBILITIES

OIT shall:

O.1 Assist agencies with identifying applicable security controls and connection requirements to ensure external connections meet state cybersecurity standards prior to implementation.

O.2 Review all new external connection requests to ensure access matches the necessary security controls to maintain integrity of the enterprise network and information systems.

O.3 Conduct semi-annual vulnerability assessments of external connections to determine the risk to the state-owned enterprise network and IT assets.

## AGENCY RESPONSIBILITIES

Agencies shall:

A.1 Ensure that all connections with external networks, systems, or applications have documented SLAs addressing acceptable security controls and procedures.

A.2 Ensure external connections are continuously monitored (in accordance with applicable standards) for security, performance, and continued business need.

A.3 Conduct semi-annual assessments of external connections to ensure they are terminated when no longer required or as security or performance issues require.

A.4 Establish SLAs with outside entities for external connections from the information system to other information systems outlining what type services or applications will be available.

A.5 Maintain documentation for each external connection describing the interface characteristics, security requirements, and the nature of the information communicated.

A.6 Review annually and update external connection SLAs.

A.7 Configure information systems that utilize external connections to provide only essential functions needed to conduct agency business. [CM-7]

A.8 Identify information system functions, ports, protocols and services to be restricted when establishing external connections. [CM-7]

## 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

## 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 legacy Policy 641: External Connections.

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.

________________________________________
Marty Redden
*Acting Secretary of Information Technology*

ORDERED

________________________________________
Kay Ivey
*Governor*

This ______ day of _______________, 2019.

DOCUMENT CHANGE HISTORY

| Version | Version Date | Comments |
|---|---|---|
| 639-01 | 08/01/2019 | Initial version; DRAFT |
| | | |
| | | |