STATE OF ALABAMA

INFORMATION TECHNOLOGY STANDARD

Standard 639S1: External System Connections		
Document/Version: 639S1-01	Version Date: 03/17/2021 (draft)	Effective Date: TBD

OBJECTIVE

Define the requirements for planning, establishing, maintaining, and terminating interconnections between Information Technology (IT) systems that are owned and operated by different organizations to accomplish a stated business goal while maintaining integrity of the State enterprise network and IT assets. These requirements are based on recommendations published in the National Institute of Standards and Technology (NIST) Special Publication 800-47: Security Guide for Interconnecting Information Technology Systems.

REQUIREMENTS

Establishing interconnections between IT systems can expose organizations at each end of the connection to greater risk of a cybersecurity incident. Security and system controls not properly implemented could compromise the connected systems and the data that they store, process, or transmit. Similarly, if one of the connected systems is compromised, the interconnection could be used as a conduit to compromise the other system and its data.

1. PLANNING THE INTERCONNECTION

1.1. Establish a planning team composed of individuals from managerial and technical staff members to develop the interconnection plan. Agency management must ensure sufficient resources are available to the planning team to coordinate all aspects of the planning process.

1.2. Participating agencies must examine all relevant technical, security, and administrative issues, and form an agreement governing the management, operation, and use of the interconnection.

1.3. Organizations shall work together to define the objective of the interconnection, determine how it will support their respective mission requirements, and identify potential costs and associated risks.

1.4. Examine privacy issues related to data that will be exchanged or passed over the interconnection and determine whether such use is restricted under current statutes, regulations, or policies.

DRAFT

1.5. Each organization has primary responsibility for ensuring the security of its respective systems and data.

2. ESTABLISHING THE INTERCONNECTION

2.1. To centralize all aspects of the interconnection effort in one document, and to clarify how technical requirements will be implemented, develop a system interconnection implementation plan. At a minimum, the implementation plan shall:

2.1.1. Describe the IT systems that will be connected.

2.1.2. Identify the sensitivity level of data that will be made available, exchanged, or passed across the interconnection.

2.1.3. Identify personnel who will establish and maintain the interconnection and specify their responsibilities.

2.1.4. Identify implementation tasks and procedures.

2.1.5. Identify and describe security controls that will be used to protect the confidentiality, integrity, and availability of the connected systems and data.

2.1.6. Provide test procedures and measurement criteria to ensure that the interconnection operates properly and securely.

2.1.7. Specify training requirements for users.

2.2. Execute Implementation Plan (Security Controls):

2.2.1. Host servers in a separately protected zone.

2.2.2. One or both organizations shall utilize an intrusion detection or prevention system to detect undesirable or malicious activity that could affect the interconnection or data that pass over it.

2.2.3. Install or configure audit/logging mechanisms to record activities occurring across the interconnection, including application processes and user activities.

2.2.4. Implement strong mechanisms to identify and authenticate users to ensure that they are authorized to access the interconnection.

2.2.5. Use access control lists (ACL) and access rules to specify the access privileges of authorized personnel, including the level of access and the types of transactions and functions that are permitted (e.g., read, write, execute, delete, create, and search).

DRAFT

2.2.6. Configure access rules to grant appropriate access privileges to authorized personnel, based on their roles or job functions. Ensure only system administrators have access to the controls.

2.2.7. Install, and keep current, antivirus software on all servers and computer workstations linked to the interconnection.

2.2.8. Configure devices to apply the appropriate level of encryption required for data that pass over the interconnection.

2.2.9. Test the interconnection to ensure equipment operates properly and there are no obvious ways for unauthorized users to circumvent or defeat security controls.

2.2.10. Test security controls under realistic conditions, and if possible, conduct testing in an isolated, non-operational environment to avoid affecting the IT systems.

2.2.11. Document the testing results and compare them with a set of predetermined operational and security standards approved by both organizations. Determine whether the results meet a mutually agreed level of acceptable risk.

2.2.12. Conduct security training and awareness for all authorized personnel who will be involved in managing, using, and/or operating the interconnection.

3. MAINTAINING THE INTERCONNECTION

3.1. Actively maintain the interconnection after it is established to ensure that it operates properly and securely. Activities for maintaining the interconnection include:

3.1.1. Maintain clear lines of communication.

3.1.2. Maintain equipment.

3.1.3. Manage user profiles.

3.1.4. Conduct security reviews.

3.1.5. Analyze audit logs.

3.1.6. Report and respond to security incidents.

3.1.7. Coordinate contingency planning activities.

3.1.8. Perform change management.

3.2. Update system security plans or other relevant documentation at least annually or whenever there is a significant change to the IT systems or to the interconnection.

DRAFT

4. DISCONNECTING THE INTERCONNECTION

4.1. Termination should be conducted in a planned manner to avoid disrupting the other party's system; however, in response to an emergency one or both organizations may decide to terminate the interconnection immediately.

4.2. Planned Disconnect:

4.2.1. The schedule for terminating the interconnection should permit a reasonable period for internal business planning so both sides can make appropriate preparations, including notifying affected users and identifying alternative resources for continuing operations.

4.2.2. Managerial and technical staff from both organizations shall coordinate the logistics of the disconnection and the disposition of shared data, including purging and overwriting sensitive data or sanitizing media for reuse or disposal.

4.2.3. Following the disconnection, each organization shall update its system security plan and related documents to reflect the changed security environment in which the respective systems operate.

4.3. Emergency Disconnect:

4.3.1. If either organization detects an attack, intrusion attempt, or other contingency that exploits or jeopardizes the connected systems or their data, it might be necessary to abruptly terminate the interconnection.

4.3.2. All parties should work together to isolate and investigate the incident, including conducting a damage assessment and reviewing audit logs and security controls, in accordance with incident response procedures.

4.3.3. If the incident was an attack or an intrusion attempt, law enforcement authorities should be notified, and all attempts should be made to preserve evidence.

SUPPORTING DOCUMENTS

This document is governed by:

- Policy 639: External Information Systems

DRAFT

Additional supporting documents:

The following special publications (SP) of the National Institute of Standards and Technology (NIST) support this standard and may aid in its implementation:

- NIST SP 800-47: Security Guide for Interconnecting Information Technology Systems
- NIST SP 800-53, Revision 5: Security and Privacy Controls for Information Systems and Organizations

DOCUMENT CHANGE HISTORY

Version	Version Date	Comments
639S1-01	03/17/2021	Initial version; DRAFT

DRAFT