GOVERNANCE

This document is governed by the IT Governance policy which provides the following requirements:

a. Roles and Responsibilities
b. Policy Control Application
c. Policy Compliance Requirements
d. Policy Exceptions and Exemptions
e. Policy Reviews and Updates

SCOPE

This policy covers all State information and systems used, managed, or operated by a contractor, agency, or other organization on behalf of the State. This policy applies to all State employees, contractors, and all other users of State information and systems supporting the operation and assets of the State.

All information assets that process, store, receive, transmit or otherwise impact the confidentiality, integrity, and accessibility of State data must meet the required security controls defined in this policy and based on the National Institute of Standards and Technology (NIST) SP 800-53 r5, Security and Privacy Controls.

APPLICABILITY

This document addresses the requirements set forth by the State to implement the family of System and Communications Protection security controls at the organization, process and/or system level for all information assets / State data and provides requirements for the identification and authentication process to assure information systems are designed and configured using controls sufficient to safeguard the State's systems and data.

SC-1 POLICY AND PROCEDURES

The State has adopted the security principles established in NIST SP 800-53 r5, "System and Communications Protection" control guidelines as the official policy for this security domain. The "SC" designator identified in each control represents the NIST-specified identifier for the System and Communications Protection control family. A designator followed by a number in parenthesis indicates a control enhancement that provides statements of security and privacy capability that augment a base control. Only those control enhancements associated with the moderate level controls are listed. Should an executive-branch agency be required to address other control enhancements for a control item, the organization will be responsible for writing an additional policy to meet that requirement.

The following subsections outline the minimum requirements State and executive-branch agencies shall implement and maintain for policy compliance.

This policy and associated procedures shall be reviewed and updated at least every three (3) years, or when State-defined events require more frequent review.

SC-2 SEPARATION OF SYSTEM AND USER FUNCTIONALITY

User functionality (including user interface services) shall be separated from information system management functionality in application components.

a. For the Application and Database secure zones, an approved firewall or other network segmentation mechanism, for example micro segmentation or virtual local area networks (VLANs), is required to segregate application servers and database servers.
b. Information systems shall not present information system management-related functionality at an interface for non-privileged users.

SC-4 INFORMATION IN SHARED SYSTEM RESOURCES

Information systems shall prevent unauthorized and unintended information transfer via shared system resources.

a. Information, including encrypted representations of information, produced by the actions of prior users/roles or processes acting on their behalf, shall not be available for object reuse nor shall residual information be available to any current users/roles or processes with access to shared system resources (e.g., registers, main memory, hard disks) after those resources are released back to information systems.
b. Information systems shall prevent unauthorized information transfer via shared resources when system processing explicitly switches between different information classification levels or security categories.

SC-5 DENIAL-OF-SERVICE PROTECTION

The effects of denial of service (DoS) attacks shall be limited by appropriately securing all potential target hosts for a common DoS or a distributed denial of service (DDoS) attack. The following controls shall be implemented:

a. Denying all inbound traffic by default limits the channels of network attacks;
b. Periodically scanning network and devices for bots (software robots) and Trojan horse programs;
c. Deploying authentication mechanisms wherever technically configurable;
d. Designing and implementing networks for maximum resiliency;
e. Developing specific plans for responding to DoS and DDoS attacks in the agency incident management plan and the business continuity plan;
f. Managing excess capacity, bandwidth, or other redundancy to limit the effects of information flooding denial of service attacks;
g. Providing detection and monitoring capabilities to detect indicators of denial-of-service attacks against the agency and to determine if sufficient resources exist to prevent effective denial of service attacks.

SC-7 BOUNDARY PROTECTION

The following shall be done for boundary protection:

a. Connect to external networks or systems only through managed interfaces with boundary protection devices meeting State security architecture and privacy requirements. Managed interfaces include but are not limited to gateways, routers, firewalls, or encrypted tunnels

implemented within the security architecture.

b. Monitor and control communications at the external managed interfaces to the system and at key internal managed interfaces within the system.
c. Implement subnetworks for publicly accessible system components that are physically and logically separated from internal agency network.
d. Limit the number of external network connections to the information system.
e. Network routing controls should supplement equipment identification by allowing specific equipment to connect only from specified external networks or internal sub networks (“subnets”).
f. Web applications should be developed to use a minimum number of ports to allow for easy integration in traditional demilitarized zone (DMZ—filtered subnet) environments.
g. Firewalls shall be configured to the following specifications:
    i. Local user accounts shall be configured on network firewalls for the sole purpose of eliminating possible extended outages.
    ii. Local accounts shall be configured to only be used when the device cannot contact the central unit. During normal operation, the local account exists but is not used.
    iii. Passwords on firewalls shall be kept in a secure encrypted form.
    iv. Agencies shall designate a minimum of two (2) authorized firewall administrators. At least one of the designated firewall administrators will be a security specialist who is consulted before firewall rule set changes are approved and implemented.
    v. For temporary or emergency port openings, the process shall establish a maximum time for the port to be open, which shall not exceed five (5) days. The authorized firewall rule set administrators, or the entity managing the firewall, shall subsequently close the port or develop additional hardening.
    vi. System administrators shall configure the firewall so that it cannot be identifiable as such to other network(s), or, at most, appears to be just another router.
    vii. Firewalls shall be installed in locations physically secure from tampering and shall not be relocated without the prior approval of agency management.
    viii. Firewall rule sets shall always block the following types of network traffic:
        1. Unauthorized scanning activity that originates outside of its network, within its network, and between information systems.
        2. Inbound network traffic from a non-authenticated source system with a destination address of the firewall system itself.
        3. Inbound network traffic with a source address indicating that the packet originated on a network behind the firewall.
        4. Inbound traffic to the State network containing ICMP (Internet Control Message Protocol) will be blocked at the perimeter except to allow testing.
        5. Inbound network traffic containing IP Source Routing information.
        6. Inbound or outbound network traffic containing a source or destination address of 0.0.0.0 and/or containing directed broadcast addresses.
    ix. Logging features on State Network firewalls shall capture all packets dropped or denied by the firewall and shall be reviewed at least monthly by authorized and qualified personnel.
    x. Each firewall rule set shall be reviewed and verified by staff at least quarterly. If an outside

entity, such as OIT, manages the firewall, then that entity shall be responsible for reviewing and verifying the firewall rule set at least quarterly.

xi. Additional requirements for protecting Federal Tax Information (FTI) on networks are provided in IRS 1075 Section 3.3.6 Network Boundary and Infrastructure.

xii. Firewall configurations and associated documentation must be treated as confidential information and must be available to only authorized personnel.

SC-7 (3) BOUNDARY PROTECTION – ACCESS POINTS

Limiting the number of external network connections facilitates monitoring of inbound and outbound communications traffic. Limiting the number of external network connections to the system is important during transition periods from older to newer technologies (e.g., transitioning from IPv4 to IPv6 network protocols). Such transitions may require implementing the older and newer technologies simultaneously during the transition period and thus increase the number of access points to the system.

All agencies must limit the number of external network connections to the system.

SC-7 (4) BOUNDARY PROTECTION – EXTERNAL TELECOMMUNICATIONS SERVICES

The following shall be done:

a. Implement a managed interface for each external telecommunication service.
b. Establish a traffic flow policy for each managed interface.
c. Protect the confidentiality and integrity of the information being transmitted across each interface.
d. Document each exception to the traffic flow policy with a supporting mission/business need and duration of that need.
e. Review exceptions to the traffic flow policy annually and remove exceptions that are no longer supported by an explicit mission/business need.
f. Prevent unauthorized exchange of control plane traffic with external network.
g. Publish information to enable remote networks to detect unauthorized control plane traffic from internal networks.

SC-7 (5) BOUNDARY PROTECTION – DENY BY DEFAULT – ALLOW BY EXCEPTION

This control enhancement applies to both inbound and outbound network communications traffic. Managed interfaces for all State information systems shall be set to use the “deny by default; allow by exception” principle. A deny-all, permit-by-exception network communications traffic policy ensures that only those connections which are essential and approved are allowed. Protective controls shall, at a minimum, include:

a. Positive source and destination address checking to restrict rogue networks from manipulating the State’s routing tables.
b. Firewalls must use an authentication mechanism that provides accountability for the individual and to ensure device configuration does not become corrupted with false entries.
c. Screen internal network addresses from external view.

SC-7 (7) BOUNDARY PROTECTION – SPLIT TUNNELING FOR REMOTE DEVICES

Information systems, in conjunction with a remote device, shall prevent the device from simultaneously establishing non-remote connections (i.e., split tunneling) with the system and communicating via some other connection to resources in external networks.

SC-7 (8) BOUNDARY PROTECTION – ROUTE TRAFFIC TO AUTHENTICATED PROXY SERVERS

Where technically configurable, routing agency-defined internal communications traffic to agency-defined external networks shall be achieved through authenticated proxy servers at managed interfaces, such as web content filtering devices.

SC-8 TRANSMISSION CONFIDENTIALITY AND INTEGRITY

The confidentiality and integrity of transmitted information shall be protected during the transfer process.

a. Organizations shall implement safeguards to protect network cabling from being damaged and to reduce the possibility of unauthorized interception of data transmissions that take place across such cabling. The organization must ensure that all network infrastructure, access points, wiring, conduits, and cabling are within the control of authorized personnel.
b. Network monitoring capabilities must be implemented to detect and monitor for suspicious network traffic.
c. Controls shall be deployed to ensure resources do not contribute to outside-party attacks. These controls include the following:
    i. **Securing interfaces between agency-controlled and non-agency-controlled or public networks.**
    ii. **Standardizing authentication mechanisms in place for both users and equipment.**
    iii. **Controlling users' access to information resources.**
    iv. **Monitoring for anomalies or known signatures via intrusion detection systems (IDS) and/or intrusion prevention systems (IPS). IDPS signatures shall be up to date.**
d. Employees, contractors, and others performing work for the State shall not intercept or attempt to intercept data transmissions of any kind that they are not authorized to access.
e. Employees, contractors, and others performing work for the State shall not use any utility, application, or service on a device used to access State systems that obfuscates or anonymizes user or device identity (e.g., IP address, MAC address, user identity, geographic location, etc.), except for authorized State-managed solutions. Prohibited services include, but are not limited to, the following: personal VPN, anonymizing/privacy features of a device or software, Private Relay, and Tor.
f. Each agency shall document and retain on file a case-by-case risk management determination for each type of sensitive or confidential information as to the appropriateness of its unencrypted transmission to a party not served by the agency's internal network.
g. Organizations shall address the risk involved in the transfer of different types of data and implement safeguards through the means of exchange used, such as through email, the internet, or exchange of electronic media and tapes.
h. Secure protocols, such as Secure Shell (SSH), Transport Layer Security (TLS), and Internet

Protocol Security (IPSec) shall be used for secure network management functions.

i. All communications that transfer confidentially sensitive data between web clients and web servers must employ the most current secure transport protocol or at a minimum a supported version of TLS. Any TLS version that is no longer supported shall not be used.
j. Instant messaging technologies, where allowed, must not be used to transmit any type of sensitive or confidential data.
k. The following types of transmission require enhanced protection using Federal Information Processing Standard 140 (FIPS 140) compliant cryptography mechanisms when integrity is an important consideration:
    i. **Internal traffic within the information system and applications**
    ii. **Internal traffic between two or more information systems**
    iii. **External traffic to or across the Internet**
    iv. **Remote access**
    v. **Email**
    vi. **FTP transmissions**
    vii. **Web services**
    viii. **Voice over Internet Protocol (VoIP)**
    ix. **Audio and video**
    x. **Wireless client to host communications**
l. Agencies shall protect the confidentiality of data transmitted on the network from corruption or data loss by prohibiting the extending, modifying, or retransmitting of network services, such as through the installation of new switches or other network devices, unless prior agency head or delegate approval is granted.

SC-8 (1) TRANSMISSION CONFIDENTIALITY AND INTEGRITY – CRYPTOGRAPHIC PROTECTION

Cryptographic mechanisms shall be implemented to prevent unauthorized disclosure of information and/or to detect changes to information during transmission. Cryptographic mechanisms implemented to protect information integrity include, for example, cryptographic hash functions which have common application in digital signatures, checksums, and message authentication codes.

SC-10 NETWORK DISCONNECT

Network disconnect applies to internal and external networks and requires terminating network connections associated with specific communications sessions. This includes, but is not limited to, de-allocating TCP/IP address or port pairs at the operating system level and de-allocating the networking assignments at the application level if multiple application sessions are using a single operating system-level network connection. Network connection sessions will be terminated as follows:

a. All information systems that store, process, transmit, or receive sensitive and/or confidential information shall be configured to terminate network connection sessions at the end of the session, or after 30 minutes of inactivity. This network disconnect shall require reconnection and authentication to re-enter the State network.
b. The information system must be configured to disconnect inactive remote VPNs.

SC-12 CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT

All State information systems, including those managed by a contractor/vendor or other third-party shall establish and manage cryptographic keys for all required cryptography employed within the system. The following requirements and configurations shall be set for each information system:

a. FIPS 140 compliant algorithms without known weaknesses shall be used when protecting sensitive or confidential data. Enablement of full FIPS mode in an application or operating system is not required. Organizations may enable additional cipher algorithms for transport encryption if they are not considered legacy or disallowed by FIPS and have no known weakness. Examples of known weaknesses include, but are not limited to, less than 128-bit for ciphers, weak configuration parameters that affect the whole, or a vulnerability.
b. Products and modules that have been validated by NIST as FIPS 140 compliant and are currently listed as validated products may be found at http://csrc.nist.gov/groups/STM/cmvp/validation.html.
c. Key-based data encryption systems shall implement a key escrow system to guarantee access to encrypted data when needed. Key escrow data shall be routinely backed up and recovery procedures tested at least annually to ensure access and availability.
d. Only State personnel shall have access to cryptographic keys. Encryption keys must be properly stored (separate from data) and available for decryption as needed. The following must also be ensured:
    i. **Separation of duties shall be enforced.**
    ii. **Any theft or loss of electronic keys requires immediate notification to both agency leadership and OIT.**
    iii. **All keys will be protected against modification, substitution, and destruction, and secret/private keys will be protected against unauthorized disclosure.**
    iv. **Cryptographic keys shall be replaced or retired when keys have reached the end of their life or the integrity of the key has been weakened or compromised.**
    v. **Physical security controls must be in place to protect all equipment used to synchronize, store, and archive keys.**
    vi. **An electronic key management and recovery system shall be used and documented, including all relevant key escrow procedures.**
    vii. **Custodians of cryptographic keys will be required to formally acknowledge they understand and accept their key-custodian responsibilities at least annually or as staff changes occur.**
    viii. **Encrypted data shall be recoverable at any point in time, even when the person(s) who encrypted the data is no longer available.**

SC-13 CRYPTOGRAPHIC PROTECTION

Cryptographic modules must be implemented for cryptographic uses as described below. Cryptographic requirements for each specified cryptographic use shall be defined:

a. All laptops used to conduct State business shall use encryption to protect sensitive and confidential information stored on the laptop.
b. All other mobile computing devices and portable computing devices such as smart phones,

tablets, and portable storage devices such as compact disks (CDs), digital video disks (DVDs), media players (MP3 players) and flash drives used to conduct State business, shall use encryption to protect all sensitive and confidential data from unauthorized disclosure.

c. Policies concerning the storage of the State's sensitive and confidential data on all portable and removable media devices shall be enforced.

SC-15 COLLABORATIVE COMPUTING DEVICES AND APPLICATIONS

The following shall be done when using collaborative computing devices and applications:

a. Prohibit remote activation of collaborative computing devices and applications, for example, networked white boards, cameras, and microphones.
b. Provide an explicit indication of use to all users physically present at the devices. Explicit indication of use includes, for example, signals to users when collaborative computing devices are activated.

SC-17 PUBLIC KEY INFRASTRUCTURE CERTIFICATES

All PKI certificates will be managed through system trust stores to ensure only approved trust anchors are maintained in the trust stores. This control is meant to address certificates with visibility external to State information systems and certificates related to the internal operations of systems, for example, application-specific time services.

a. PKI certificates shall be issued by, or obtained from, a State-defined certificate authority or State-approved service provider.
b. Authorization to register to receive a public key certificate must be provided by OIT or an OIT representative.
c. Public key certificates must be issued using a secure process that both verifies the identity of the certificate holder and ensures that the certificate is issued to the intended party.
d. Organizations shall include only approved trust anchors in trust stores or certificate stores managed by the organization.
e. Only digital certificates for transport encryption either issued by and/or approved by OIT can be used on end-user facing State applications and/or systems as well as system-to-system transport encryption where external connections are accepted. For internal system-to-system transport encryption, internally signed certificates may only be utilized if they adhere to the algorithm requirements defined in SC-12(a), are valid for no more than four years, and can be tracked and managed to prevent expiration.

SC-18 MOBILE CODE

A tamper protection program shall be implemented for the information system, system component, or information system service to protect the State network from mobile code that performs unauthorized and malicious actions.

a. Usage restrictions and implementation guidance shall be established for Voice over Internet Protocol (VoIP) technologies based on the potential to cause damage to the information system if used maliciously.

b. The use of VoIP within the information system shall be authorized, monitored, and controlled.

SC-20 SECURE NAME/ADDRESS RESOLUTION SERVICE (AUTHORITATIVE SOURCE

Providing authoritative source information enables external clients, including remote internet clients, to obtain origin authentication and integrity verification assurances for the host/service name to network address resolution information obtained through the service. Systems that provide name and address resolution services include domain name system (DNS) servers. Information systems shall require the following for domain name system (DNS):

a. Enable external clients, including remote Internet clients, to obtain origin authentication and integrity verification assurances for the host/service name to network address resolution information obtained through the service using DNS servers.
b. DNS servers shall not be configured to allow zone transfers to unknown secondary servers.
    i. If an agency maintains a primary DNS server, zone transfers will be allowed only to trusted (known) servers.
    ii. If an agency maintains a secondary DNS server, zone transfers will be allowed to the primary DNS server only.
    iii. When a domain has a US extension (e.g., state.al.us), the US Domain Registry requires the domain allow copies to be transferred to the US Domain Registry's Master Server. Therefore, all domains registered with US Domain Registry will allow transfers of copies of their zones to the Master Server for the US Domain Registry. *When OIT maintains the DNS, agencies may request OIT to allow additional IP addresses to receive zone transfers. Agencies must work with OIT to define acceptable IP addresses and/or IP address ranges.*

SC-21 SECURE NAME/ADDRESS RESOLUTION SERVICE (RECURSIVE OR CACHING RESOLVER)

a. Information systems shall request and perform data origin authentication and data integrity verification on the name/address resolution responses the system receives from authoritative sources using recursive resolving or caching domain name system (DNS) servers.
b. Recursion on an authoritative name server is prohibited.

SC-22 ARCHITECTURE AND PROVISIONING FOR NAME/ADDRESS RESOLUTION SERVICE

Information systems that collectively provide name/address resolution service shall be fault-tolerant and implement internal/external role separation.

a. At least two authoritative domain name system (DNS) servers shall be deployed to eliminate single points of failure and enhance redundancy (one configured as the primary server and the other configured as the secondary server).
b. Servers shall be deployed in two geographically separated network subnetworks (i.e., not located in the same physical facility).
c. Split DNS shall be used to prevent leaking internal system and IP information to external non-State clients to limit information exposure.

d. DNS servers with internal roles shall only process name and address resolution requests from within the organizations (e.g., from internal clients).
e. DNS servers with external roles only process name and address resolution information requests from clients external to organizations (e.g., on external networks including the internet).
f. Clients that can access authoritative DNS servers in particular roles (e.g., by address ranges, explicit lists) shall be specified.
g. Servers must be configured to provide redundancy, load balancing, and distributed access.

SC-23 SESSION AUTHENTICITY

Information systems must protect the authenticity of communications sessions. Protecting session authenticity addresses communications protection at the session level, not at the packet level. Such protection establishes grounds for confidence at both ends of communications sessions in the ongoing identities of other parties and the validity of transmitted information. Authenticity protection includes protecting against “man-in-the-middle” attacks, session hijacking, and the insertion of false information into sessions.

Information systems shall invalidate session identifiers upon user logout or other session termination.

Protection mechanisms shall be selected and implemented to ensure adequate protection of data integrity, confidentiality, and session authenticity in transmission. Mechanisms include, but are not limited to, the following:

- Security services based on IPsec
- VPNs
- TLS
- DNS
- SSH
- Digital signatures
- Digital certificates
- Digital time stamping
- FIPS 140 compliant encryption technology

SC-28 PROTECTION OF INFORMATION AT REST

Information systems shall protect the confidentiality and integrity of all sensitive or confidential data at rest. Information at rest refers to the state of information when it is stored on devices as specific components of information systems.

SC-28 (1) PROTECTION OF INFORMATION AT REST – CRYPTOGRAPHIC PROTECTION

The selection of cryptographic mechanisms is based on the need to protect the confidentiality and integrity of organizational information. The strength of mechanism is commensurate with the security category or classification of the information. Cryptographic mechanisms implemented on State information systems shall:

a. Cryptographic mechanisms shall be implemented to prevent unauthorized disclosure and modification of all sensitive or confidential data at rest: sensitive and confidential data stored in

non-volatile storage (e.g., disk drive) on all endpoints shall be encrypted with FIPS 140-2 compliant encryption during storage (regardless of location).

b. Organizations shall consider increasing integrity protection of data by recording data onto hardware-enforced, write-once media. Write-once, read-many (WORM) media includes, for example, Compact Disk-Recordable (CD-R) and Digital Video Disk-Recordable (DVD-R).
c. Organizations shall consider storing data at rest on a physically separate non-mobile storage device (e.g., disk drive, tape drive) with cryptographic protections in place.
d. Whereas a virtual machine may store or process confidential data, the virtual machine image file shall use appropriate controls to protect the data at rest.

SC-40 WIRELESS LINK PROTECTION

The confidentiality of data transmitted on external and internal wireless links shall be protected from corruption or data loss by doing the following:

a. Extending, modifying, or retransmitting network services, such as through the installation of new switches or wireless access points, is prohibited, unless prior approval is granted.
b. Wireless networks shall be physically or logically segregated from internal wired networks such that an unknown external user cannot access an organization's internal network.
c. All restricted and highly restricted data shall be encrypted when transmitted across wireless or public networks, including transmissions such as Secure File Transfer Protocol (SFTP) and electronic mail.
d. All network access points shall be identified, and safeguards for the network and individual systems shall be verified as adequate and operational. These systems include wireless access points, network ingress and egress points, and network-attached devices.
e. Use access points that require a key and which encrypt the wireless communication.
f. Configure wireless LAN settings to not allow automatic joining of any wireless network.
g. Wireless LAN communications shall be encrypted.
h. When end-to-end encryption is required across both an 802.11 wireless and a wired network, then in addition to WPA2 (802.11i), data transmitted between any wireless devices shall be encrypted using a proven encryption protocol that ensures confidentiality. Such protocols include TLS, SSH, IP Security (IPSec) and VPN tunnels.

Organizations Shall:

a. Establish usage restrictions and implementation guidance for information system components including, for example: hardware, software, or firmware components (e.g., VOIP, mobile code, digital copiers, printers, scanners, optical devices, wireless technologies, mobile devices).
b. Define the proper use of information assets through Acceptable Use Policies (AUPs) and include critical technologies such as remote access technologies, removable electronic media, laptops, tablets, smartphones, email usage, and internet usage.

SC-44 – Detonation Chambers

Agencies tasked with conducting incident response and forensics should employ a detonation chamber capability, also known as dynamic execution environments, in a secure, quarantined

environment to perform actions such as, but not limited to:

a. Opening suspect email attachments.
b. Allowing the execution of untrusted or suspicious applications.
c. Allowing the execution of Universal Resource Locator (URL) requests in the safety of an isolated environment or virtualized sandbox to quickly identify malicious code.
d. Reducing or preventing the likelihood of malicious code propagates to user environments of operation.

POLICY OWNER

Secretary of Office of Information Technology (OIT)

MATERIAL SUPERSEDED

This is the first State of Alabama System and Communications Protection Policy. All State agencies and vendors of the State are required to comply with the current implemented version of this policy.

REVISION HISTORY

Revision Date	Summary of Change
12/31/2024	Policy Created

REMAINDER OF PAGE LEFT INTENTIONALLY BLANK

APPROVED BY

Signature	Daniel Urquhart
Approved by	Daniel Urquhart
Title	Secretary of Office of Information Technology (OIT)
Date Approved	01/15/2025

REMAINDER OF PAGE LEFT INTENTIONALLY BLANK