STATE OF ALABAMA

INFORMATION TECHNOLOGY POLICY

Policy 115: Electronic Signatures		
Document/Version: 115-01	Version Date: 01/05/2021	Effective Date: 02/01/2021

PURPOSE

The purpose of this Electronic Signatures policy is to enable the development and use of electronic signature (e-sign) to support full legal effect and enforceability when conducting transactions by or with Alabama government agencies.

This policy establishes the State of Alabama executive branch approach for adopting e-sign technology and best practices to ensure electronic signatures applied to official state documents are legally valid and enforceable.

SCOPE

Electronic signature is used to authenticate identity and to verify the integrity of signed electronic records. Electronic signatures document the signer's intent, provide evidence that a specific individual signed the electronic record, and maintain an auditable electronic record of the signature that cannot be changed without detection.

This policy formalizes and standardizes the State's electronic signature requirements for agencies that have implemented or are planning to implement e-sign technologies to sign agency electronic records. Agency policies as well as external federal mandates (e.g., Federal Information Processing Standards (FIPS) and Privacy Act) drive the scope of the requirements with which electronic signature implementations must comply.

This policy applies primarily to new implementations of e-sign technology. Existing e-sign implementations developed prior to the approval date of this policy will be grand-fathered, as long as applicable requirements (i.e., FIPS, Privacy Act, and Records Management) are met by the existing implementation. System owners must adopt the requirements of this policy in any future major upgrades or modernization efforts.

The requirements and responsibilities defined herein shall apply to state agencies, vendors under contract with state agencies, and other stakeholders conducting business with state agencies as a means to enforce technology standardization and assist in making the usage, support, and/or purchase of technologies more consistent and efficient

AUDIENCE

The audience for this policy includes all State of Alabama executive branch agencies, licensure boards, employees, contractors, and other individuals who need to sign electronic records (e.g., documents, forms, contracts, and other correspondence) in support of state business, services, and administrative operations. This policy may also be voluntarily adopted by Alabama public entities outside the authority of the Office of Information Technology.

AUTHORITY

This policy is promulgated under the authority of the Office of Information Technology (OIT) as described in Policy 101: IT Governance.

DEFINITIONS

In this document, the following words have the following meanings.

Authentication: Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to a system's resources.

Digital Signature: A subset of electronic signature technology. Digital signatures encrypt documents with digital codes to verify the user's identity and support authentication, data integrity and signer non-repudiation.

Electronic Signatures or E-sign: Legal concept that uses technology to ensure the signature may not be denied legal effect, validity or enforceability.

Identity: An attribute or set of attributes that uniquely describe a subject within a given context.

Integrity: Maintaining the accuracy and completeness of data over its entire lifecycle.

Non-Repudiation: Assurance that the signer cannot deny the authenticity of their signature.

Uniform Electronic Transactions Act (UETA): Chapter 1A of Title 8, Code of Alabama 1975; provides legal recognition of electronic records, electronic signatures, and electronic contracts.

STATEMENT OF POLICY

It is the policy of OIT that:

a) OIT shall implement an electronic signature system compliant with these requirements and offer e-sign capabilities to state agencies. State Agencies shall work with OIT to determine whether the enterprise e-sign system satisfies agency needs.

b) Agencies may use any valid electronic signature solution that meets their business requirements so long as it also complies with applicable federal standards and statutes and with the requirements stated herein and in other applicable policies.

c) Agencies using (or requiring) an e-sign system that is different from the enterprise system shall inform OIT of the system being used. OIT may request additional information on the agency system to validate policy compliance.

d) To facilitate statewide adoption of e-sign technology, agencies shall coordinate with OIT prior to acquisition of new e-sign systems.

e) Agencies may develop agency-specific policies and administrative rules on electronic signature to further clarify this enterprise policy (administrative rule template attached hereto).

f) Agencies shall develop internal control processes defining the implementation and use of e-sign technology.

g) The State agency initiating the transaction (owner of the document) shall be responsible for any costs associated with use of the e-sign technology by that agency, except as otherwise agreed between the signers.

REQUIREMENTS

1. THE E-SIGN TECHNOLOGY SOLUTION MUST:

1.1. Provide an identical copy of the original signed and executed document to the signer.

1.2. Ensure non-repudiation; that the signer cannot deny the fact that he or she electronically signed the document.

1.3. Capture information about the process used to capture signatures (i.e. create an audit trail), including but not limited to:

- IP address
- Date and time stamp of all events
- All web pages, documents, disclosures, and other information presented
- What each party acknowledged, agreed to, and signed

1.4. Encrypt, end-to-end, all communication within the signature process. Encryption technologies shall comply with state encryption standards, including the requirements that cryptographic modules be validated to the current Federal Information Processing Standards (FIPS).

[Adobe Sign, for example, uses RSA BSAFE Crypto-C]

RECOMMENDATIONS

The following processes and system attributes are recommended.

2. E-SIGN PROCESS RECOMMENDATIONS:

2.1. Agencies should ensure their electronic signature process meets security, legal, records management and other agency business requirements.

2.2. Verify that all document approvers are able/allowed to sign the document electronically prior to initiating an e-sign transaction.

3. E-SIGN SYSTEM RECOMMENDATIONS

3.1. The e-sign system should provide a two-step signing process prior to submitting the document to ensure knowledge and intention verification:

3.1.1. The signer should acknowledge having read the on-screen document by selecting a checkbox or answering a challenge question prior to enabling the ability to provide an electronic signature.

3.1.2. The signer should then be allowed to electronically sign the document, via the technology solution, before submitting it.

3.2. The e-sign system should be capable of two-factor authentication. Validating signer identity via email fulfills requirements for a legal electronic signature; however, there may be circumstances when a second authentication factor is desired. Examples of signer authentication include a password or verification code (something the signer has or receives from the sender) or may be knowledge-based (something the signer knows).

3.3. The e-sign system should allow signers to sign with ink signature then scan and attach the document within the electronic signature process.

3.4. The e-sign system should allow a flexible document retention policy capable of complying with Alabama State Records Commission requirements.

3.5. To simplify long-term document retention requirements, the e-sign system should provide the ability to index, store, and retrieve the e-signed document in the system of record of your choice, not in the service provider's cloud storage.

3.6. Assess the e-sign provider's security practices, track record, frequency of security audits, and compliance with IT standards for security and data protection, including but not limited to ISO 27001, SOC 1/2/3, HIPAA, FIPS 140-2, FISMA, etc.

3.7. The e-sign system should support and provide a secure electronic signature API to enable integration into web applications or business processes.

3.8. The e-sign system should allow for use and signature on mobile platforms (e.g., Apple IOS and Android devices).

3.9. If in-country data residency is a requirement, verify the locations of data centers used by the e-sign provider. Data location requirements should be specified in contracts with e-sign providers or in Service Level Agreements.

SUPPORTING DOCUMENTS

The following documents support this policy and may aide in its implementation:

- FIPS 186-4: Digital Signature Standard (DSS) (https://csrc.nist.gov/publications/detail/fips/186/4/final)
- FIPS 180-4 Secure Hash Standard (SHS) (https://csrc.nist.gov/publications/detail/fips/180/4/final)
- Uniform Electronic Transactions Act (UETA); Code of Alabama 1975, 8-1A-01 et seq.
- Administrative Rule Template

DOCUMENT CHANGE HISTORY

Version	Version Date	Comments
115-01	01/05/2021	Initial version

Attachment: Administrative Rule Template (next 2 pages)

xxx-x-x-.xx Electronic Records Policy.

(1) Legal Basis: The Alabama Uniform Electronic Transactions Act ("UETA"), Section 8-1A-1 et seq. of the Code of Alabama 1975, enacted in 2002, is intended to facilitate the use of electronic documents in business, commercial, and governmental transactions. The Act promotes but not require the use of electronic signatures and creation of electronic documents. Section 8-1A-18(a) provides that "each government agency of this state with rule-making authority...may determine by rule whether, and the extent to which, it will send and accept electronic records and electronic signatures to and from other persons and otherwise create, generate, communicate, store, process, use, and rely upon electronic records and electronic signatures." Section 8-1A-12(a) provides that an electronic record meets other state law requirements for record retention if the electronic record both accurately reflects the original document and is accessible for later reference. Section 8-1A-13 provides that an electronic record may not be excluded from evidence in court solely because it is in electronic form. Section 8-1A-12(g) provides that the State Records Commission is not precluded by the Act from placing additional requirements for record retention on agencies.

(2) Definitions: Except as otherwise specified in this rule, undefined terms have the respective meanings set forth in the Act. Notwithstanding the forgoing, the following words where used in this rule shall have the following meanings:

(a) Act or UETA. Alabama Uniform Electronic Transaction Act, Code of Alabama 1975, Section 8-1A-1 et seq.

(b) OIT. The State of Alabama Office of Information Technology, as established in Code of Alabama 1975, Section 41-28-1.

(c) Records Disposition Authority or RDA. An agency-level records retention schedule issued by the State Records Commission under the authority granted by the Code of Alabama 1975, Sections 41-13-5 and 41-13-20 through 21.

(d) State Records Commission. The State Records Commission, as established in Code of Alabama 1975, Section 41-13-20.

(3) Use of Electronic Signatures and Electronic Records: In accordance with Section 8-1A-18(a) of the Code of Alabama 1975, [AGENCY] hereby establishes that to the fullest extent permitted by the Act and except as otherwise provided in this administrative rule, [AGENCY] will send and accept electronic records and electronic signatures to and from other persons and otherwise create, generate, communicate, store, process, use, and rely upon electronic records and electronic signatures. In accordance with Section 8-1A-18(b), [AGENCY] use of electronic records and electronic signatures will comply with the following requirements:

(a) Provide an identical copy of the original signed and executed document to the signer.

(b) Ensure non-repudiation; that the signer cannot deny the fact that he or she electronically signed the document.

(c) Capture information about the process used to capture signatures (i.e. create an audit trail), including but not limited to:

1. IP address
2. Date and time stamp of all events
3. All web pages, documents, disclosures, and other information presented
4. What each party acknowledged, agreed to, and signed

(d) Encrypt, end-to-end, all communication within the signature process. Encryption technologies shall comply with state encryption standards, including the requirements that cryptographic modules be validated to the current Federal Information Processing Standards (FIPS).

The information contained in this subsection constitutes the minimum that is required for a valid electronic signature. Any authorized person within [AGENCY] may require additional reasonable information from a signer in order to establish the identity and signature authority of the signer. [AGENCY] may provide additional requirements subject to a State of Alabama information technology policy as promulgated by OIT.

(4) Creation and Retention of Electronic Records: In accordance with Section 8-1A-17 of the Code of Alabama 1975, [AGENCY] hereby establishes that to the fullest extent permitted by the Act and except as otherwise provided in this administrative rule, it will create and retain electronic records and convert written records to electronic records. Any such electronic records will be retained in compliance with State Records Commission requirements, including the records retention schedules set forth in the [AGENCY] Records Disposition Authority. [AGENCY] may create a retrievable electronic record or copy, by optical scan or otherwise, of paper original documents or make other images or paper copies which accurately reproduce the originals and may destroy original paper documents so copied as specified in the RDA. Electronic copies of original documents, when certified by an authorized [AGENCY] record custodian, are admissible in [AGENCY] administrative proceedings as authorized by the Act as though they were the original document. The electronic document retains the confidential or public document characteristics of the original document.

Author: [AUTHOR]

Statutory Authority: Code of Ala. 1975, §§8-1A-7, 8-1A-12, 8-1A-13, 8-1A-17, 8-1A-18.

History: New Rule: Filed _____; effective _____.