ALABAMA DIVISION OF

RISK MANAGEMENT

ELECTRONIC SIGNATURE POLICY

In order to increase the efficiency and effectiveness of the Alabama Division of Risk Management's (hereinafter, "DORM" or "the DORM") operations that require or request signatures to indicate approvals or acknowledgements, the DORM may accept electronic signatures to replace previously required handwritten original signatures on paper documents.

To the fullest extent permitted by law, the DORM accepts electronic signatures as legally binding and equivalent to handwritten signatures to signify agreement or approval. This policy establishes the process for designating transactions that can legally accept electronic signatures and how the DORM will accept and verify electronic signatures. Where nonrepudiation of the authenticity of a particular signature is required, a digital signature, as defined below, may be required.

1. FEDERAL AND STATE LAW

A. Enacted to aid and encourage electronic commerce, the federal Electronic Signatures in Global and National Commerce Act (E-SIGN) of June 2000 states that "With respect to any transaction affecting interstate or foreign commerce . . . a contract . . . may not be denied legal effect, validity, or enforceability solely because an electronic signature or electronic record was used in its formation. 15 USC § 7001(a)(2).

B. The Code of Alabama, 1975, Section 8-1A-7 also seeks to facilitate and promote electronic commerce and says that where an existing law requires a signature, then an electronic signature satisfies that rule of law:

> **Alabama Code, Section 8-1A-7:**
> **Legal recognition of electronic records, electronic signatures, and electronic contracts.**
>
> (a) A record or signature may not be denied legal effect or enforceability solely because it is in electronic form.
>
> (b) A contract may not be denied legal effect or enforceability solely because an electronic record was used in its formation.
>
> (c) If a law requires a record to be in writing, an electronic record satisfies the law.
>
> (d) If a law requires a signature, an electronic signature satisfies the law.

2. DEFINITIONS:

A. ELECTRONIC SIGNATURE:

The DORM defines an electronic signature as an electronic sound, symbol, or process attached to or logically associated with a contract or other record and executed or adopted by a person with the ability and intent to sign the record.

B. DATA CLASSIFICATION:

In the context of information security, data classification is based on its level of sensitivity and the impact to the DORM should that data be disclosed, altered or destroyed without authorization. The classification of data helps determine what baseline security controls are appropriate for safeguarding that data.

i. Public Data: Data should be classified as Public when the unauthorized disclosure, alteration or destruction of that data would result in little or no risk to the DORM or the State of Alabama. Examples of Public data include contracts, press releases, and program guidelines. While little or no controls are required to protect the confidentiality of Public data, some level of control is required to prevent its unauthorized modification or destruction.

ii. Private Data: Data should be classified as Private when the unauthorized disclosure, alteration or destruction of that data could result in a moderate level of risk to the DORM or the State of Alabama. By default, all data that is not explicitly classified as Restricted or Public data should be treated as Private data. A reasonable level of security controls should be applied to Private data.

iii. Restricted Data: Data should be classified as Restricted when the unauthorized disclosure, alteration or destruction of that data could cause a significant level of risk to the DORM or the State of Alabama. Examples of Restricted data include data protected by state or federal privacy regulations and data protected by confidentiality agreements. The highest level of security controls should be applied to Restricted data.

C. OTHER DEFINITIONS:

An Approved Electronic Signature Method is one that has been approved by the State of Alabama's Risk Manager, in accordance with this policy and all applicable state and federal laws, and which specifies the form of the electronic signature, the systems and procedures used with the electronic signature, and the significance of the use of the electronic signature.

Authentication is the process by which the DORM ensures that the user who attempts to perform the function of an electronic signature is in fact who they say they are and is authorized to "sign."

Authorization is the process by which the DORM verifies that an authenticated user has permission to access specific electronic DORM services and/or perform certain operations.

A Certificate is an electronic document used to identify an individual, a server, a company, or some other entity and to associate that identity with a public key. A certificate provides generally recognized proof of a person's identity.

Electronic relates to technology having electrical, digital, magnetic, wireless, optical, electromagnetic, or similar capabilities.

An Electronic Record is a contract or other record created, generated, sent, communicated, received, or stored by electronic means.

An Electronic Transaction is an operation conducted or performed, in whole or in part, by electronic means or electronic records.

Non-Repudiation is the inability of either party in a voluntary transaction to reject, disown, or disclaim the validity of that transaction.

Public Key Infrastructure is a form of information encryption that uses certificates to prevent individuals from impersonating those who are authorized to electronically sign an electronic document. A "public key" is a value provided by some designated authority as a key that, combined with a "private key" derived from the public key, can be used to effectively encrypt messages and digital signatures

A Private Key is an encryption/decryption key known only to the party or parties that exchange messages. In traditional private key cryptography, a key is shared by the communicators so that each can encrypt and decrypt messages.

A Record is information that is inscribed on a tangible medium or that is stored in an electronic or other medium and is retrievable in perceivable form.

Repudiation is the willful act of either party in a voluntary transaction to reject, disown, or disclaim the validity of that transaction.

A Transaction is a discrete event between a user and a system that supports a business or programmatic purpose.

3. SCOPE:

A. Wherever possible, the DORM encourages that those who utilize its services or provide it services do business electronically and use electronic signatures to conduct transactions that may have previously required handwritten signatures on paper documents.

B. Where a transaction requires that the authenticity of the signer be more rigorously proven and where the party to the contract or transaction cannot legally repudiate the authenticity of their signature on a document, then a digital signature will be required.

C. This policy establishes and implements the process for designating transactions that would accept digital signatures and how the DORM will implement digital signatures. Until the DORM establishes its preferred and approved methods for the use of digital signatures, such contracts or transactions will need handwritten signatures on paper documents.

D. Ultimately, the Risk Manager and/or each DORM Manager will be accountable for selecting the appropriate signature method along with documenting the selection procedure and reasons for selecting a signature method and the Information Technology Manager will be responsible for implementing the appropriate signature method.

E. Electronic signatures and digital signatures cannot be used for the following transactions:

i. Where a rule of law clearly indicates an intent for the transaction to be handwritten, as opposed to in an electronic format. In these situations, a law that simply requires the information to be "in writing", "written" or "printed" *can* be satisfied through an electronic signature.

ii. To any record that serves as a unique and transferable instrument of rights and obligations including, without limitation, negotiable instruments and other instruments of title wherein possession of the instrument is deemed to confer title.

F. External third parties are not required to accept or use electronic signatures in transactions. In those situations, the DORM and the external third party will need to come to an agreement on the acceptable form of signature on the transaction, or default to handwritten signatures on paper documents.

4. IMPLEMENTATION PROCEDURES:

Electronic signatures may be implemented using various methodologies depending on the associated risks that may include fraud, non-repudiation, and financial loss. The quality and security of the e-signature method should be commensurate with the risk and any requirements to assure the authenticity of the signer.

A. RISK ASSESSMENT:

The Risk Manager and DORM Departmental Managers should first consider the risk associated with the transaction, including but not limited to, taking care to assess the probability and impact of:

i. Inconvenience, distress, or damage to the DORM's reputation
ii. Financial loss or liability
iii. Harm to the DORM's programs or public interests
iv. Unauthorized release of Private or Restricted Data
v. Civil or criminal violations; and
vi. Bodily or financial harm to individuals

B. METHOD SELECTION:

Wherever possible, electronic signatures should be implemented. Digital signatures or handwritten signatures should be reserved for circumstances when they are required by law, regulation, or other applicable policy or authority.

C. RISK LEVELS:

LEVEL 1 RISK: NONE TO LOW:

i. Authentication: DORM Account IDs and passwords are not required for authentication, but a signer's identity could be authenticated using a government-issued identification document.

ii. Assurance Level: Little or no confidence in the asserted identity's validity.

iii. Recommendation: Basic Electronic Signature – A signatory clicks a checkbox in an electronic agreement to signify agreement or approval.

iv. Use Case: This is appropriate for low-risk transactions such as basic form submissions without legal implications.

LEVEL 2 RISK: LOW TO MEDIUM:

i. Authentication: DORM Account IDs and passwords are required for authentication to an electronic form or document, after which a signatory may click on a checkbox to signify agreement or approval.

ii. Assurance Level: Sufficient confidence in the asserted identity's validity.

iii. Recommendation: Electronic Signature – DORM Authentication with logging of signed in user and time stamp of signature.

iv. Use Case: This is the most common use case appropriate for individuals within the DORM community, encompassing most process flows, forms and approvals.

LEVEL 3 RISK: MEDIUM TO HIGH:

i. Authentication: DORM Account IDs and passwords are required to authenticate to an established Electronic Signature Service such as that utilized by Origami Risk.

ii. Assurance Level: High confidence in the asserted identity's validity.

iii. Recommendation: Electronic Signature using established Electronic Signature Service.

iv. Use Case: This is required in transactions involving external parties who do not have DORM credentials such as signatories on certification forms, change forms, contracts involving external vendors, and other similar documents.

LEVEL 4 RISK: HIGH:

i. Authentication: DORM Account IDs and passwords or approved Digital certificates are required to authenticate to a digital signature solution that provides encryption and nonrepudiation for selected electronic documents.

ii. Assurance Level: High confidence in the asserted identity's validity.

iii. Recommendation: Digital Signature, or other secure electronic signatures.

iv. Use Case: This is required in the smaller set of transactions where signature nonrepudiation is required by law, such as transactions involving sending/signing any documents that are going to the European Union.

LEVEL 5 RISK: VERY HIGH:

i. Authentication: A document is required to be printed and an individual must provide an original signature in ink.

ii. Assurance Level: Very high confidence in the asserted identity's validity.

iii. Recommendation: Handwritten Signature.

iv. Use Case: This is required in the smaller set of transactions where the law or requires original inked signatures, such as negotiable instruments and other instruments of title where possession confers title.

D. IMPLEMENTATION:

When implementing an electronic or digital signature process, all applicable laws, rules, regulations, and DORM policies and procedures must be followed. In addition, the transactions should comply with these requirements:

ELECTRONIC SIGNATURES:

i. The signer must perform an action to signify agreement or approval, such as clicking a checkbox, typing their name into a text box, or importing a graphic representation of a handwritten signature.

ii. Checkboxes alone may not be sufficient when it is necessary to verify the electronic signature or transaction's execution.

iii. The signer's first and last name must be visible and legible below or along with the electronic signature.

iv. The time and date of the electronic signature must be captured, stored, and available for retrieval along with the electronic record.

v. Should the State of Alabama establish minimum security

requirements for the use of electronic records and signatures at State Agencies, those requirements must be followed for the use of electronic signatures at the DORM.

vi. As a subset of electronic signatures, non-repudiated and encrypted digital signatures will use a digital signature software application and digital certificates that has yet to be purchased or implemented. Until this is available, any signature that requires this level of legal assurance or poses a high risk to the DORM will continue to use handwritten signatures.

5. COMPLIANCE:

Any individual that uses electronic or digital signatures for DORM operations in violation of this policy or other DORM policies, procedures, or applicable state and federal laws may be subject to appropriate sanctions that may include disciplinary actions up to and including termination. Staff violations will follow appropriate State of Alabama and Finance Department disciplinary processes.

Anyone aware of possible violations of this Policy must report them immediately to their manager and/or the Risk Manager.

ADOPTED AND IMPLEMENTED this 24th day of January, 2022.

Max Graham,

Risk Manager