***** Faculty Senate acceptance contingent upon university-provided supply of appropriate software (such as Adobe Acrobat Pro) campus-wide to all units/faculty/staff needing to provide electronic signatures***

THE UNIVERSITY OF ALABAMA IN HUNTSVILLE

ELECTRONIC SIGNATURES

Number 02.02.XX

Division Office of Information Technology (OIT)

Date September 2019 (as revised Sept. 24 2020)

Purpose The purpose of this policy is to establish proper user practices for electronic signatures.

Policy Federal and state law recognizes that an electronic signature has legal effect and is enforceable. To increase the efficiency of transactions that require approval or authorization by signature, the University supports the use of electronic signatures as long as their use meets legal and security requirements.

This policy governs all uses of electronic signatures when conducting business on behalf of the University, including all business units and affiliated foundations. This policy applies to all University persons using electronic signatures.

Definitions

For purposes of this policy, the following definitions apply:

Authentication. The assurance that an electronic signature is that of the individual purporting to sign a record or otherwise approving an electronic transaction.

Electronic Signature. A computer data compilation of any symbol or sound, or a series of symbols or sounds, attached to, or logically associated with, a record and executed and adopted by an individual with the intent to affix a signature to approve the record.

Record. A record created, generated, sent, communicated, received, or stored and signed or approved by electronic means.

Signature Authority. Permission given or delegated to an individual to sign a record (electronically or by hand), access specific University services, and/or perform certain University operations, including executing agreements that bind the University.

Procedure

Electronic signatures may be used to conduct University business as provided for by this policy. Electronic signatures may not be used when an applicable law, regulation, or University policy or process specifically requires a handwritten signature.

1.0 General

The University supports and may require the use of electronic signatures when conducting University business. The University, at its discretion, may elect to opt out of conducting business electronically with any party or in any transaction, for any reason or no reason. The University accepts an electronic signature in place of a handwritten signature in University transactions when a signature is required, **except:**

- in instances in which the other contracting party will not accept an electronic signature; or
- where applicable law, regulation, or University policy or process requires a handwritten signature or otherwise does not allow an electronic signature.

To determine if electronic signatures are used in an internal workflow/approval process, contact the applicable systems administrator or University office.

2.0 Validity

To the fullest extent permitted by law, the University accepts electronic signatures as legally binding.

An electronic signature is **not** valid if:

- applicable law, regulation, or University policy or process requires a handwritten signature; or
- the individual does not have signature authority to sign the record to approve the transaction.

The mere fact that an individual signs a record with an electronic signature does not guarantee that the record has been signed by an authorized person with the ability to sign, approve, or bind the University with such record. As defined by The Board of Trustees of The University of Alabama in Board Rule 406, only certain UAH officials have signature authority to sign contracts, agreements, and similar documents, which commit UAH to a course of action and bind the University on behalf of the Board of Trustees for The University of Alabama. For more information, see Board Rule 406. The individuals that have this authority are named in a Board Resolution and cannot delegate the authority to others.

Appropriate procedures must be used to confirm that the person signing the record has the appropriate authority. Authority to use an electronic signature to sign a document is the same as authority to sign using non-electronic methods.

3.0 Authentication

All electronic signature methods must be approved before use to sign documents. This includes all electronic signatures, whether internal only that do not commit the University or external and commit the University.

3.1 Electronic Signature Method Approval Process

For an electronic signature method to be approved, it must be approved by the Chief Information Security Officer (CISO) of the Office of Information Technology and the Vice President of the area utilizing the method or the President of the University.

In order to be approved, an electronic signature method must:

- Include the ability to verify the authenticity of the signatory through a secure process that includes an audit trail and a final, tamper-evident digital certificate that is either embedded into the completed signed document, or bound to the document using encryption.
- Support the applicable business purpose and workflow; and
- Permit the information to be retrievable in the future and auditable.

When a method is approved, it will be added to the list described below.

3.2 List of Approved Electronic Signature Methods

The Chief Information Security Officer (CISO) for the Office of Information Technology will establish and keep an approved list of methods for electronic signatures. The listing will describe how to access the approved method(s). As additional electronic signature methods are approved, each method and how to access the method will be added to the list. The standard approved method is an Office of Information Technology issued digital certificate.

The Chief Information Security Officer, the Vice President of the area utilizing the method, or the President of the University have the authority to revoke approval of any approved method at any time and for any reason.

4.0 Retention

Electronic signatures and the associated data to validate the electronic signature are an integral part of the record. Electronically signed documents must follow the same record retention as those using handwritten signatures. The signature and means to verify it need to be maintained for the full records life cycle.

5.0 Responsibilities

All individuals with signature authority are responsible for activities conducted under their digital signature and are expected to take all precautions to safeguard their password, personal identification number (PIN), and signature files to prevent inappropriate use. Sharing of digital signatures, passwords, pins, accounts or other access tokens is prohibited by the Appropriate Use of IT Resources policy, located at:

https://www.uah.edu/images/administrative/policies/02.02.03-AA-appropriate-use-of-it-resources.pdf.

University employees are expected to report any actual or suspected fraudulent activities related to electronic signatures immediately to any manager or supervisor in the appropriate department, school/college, or other applicable unit or through other appropriate channels such as described in the IT Incident Reporting and Breach Notification policy, located at:

https://www.uah.edu/images/administrative/policies/02.02.07-OIT-IT-incident-reporting-and-breach-notification.pdf.

6.0 Non-Compliance

OIT personnel may take immediate action to abate identified issues impacting network, system or security operations.

Violations that constitute a breach of the Student Conduct Code, the Faculty Handbook, the Staff Handbook, University policy or [illegible]

7.0 Implementation

The Chief Information Security Officer (CISSIO) of the Office of Information Technology is responsible for the implementation of this policy, including developing and providing training to the University community prior to their authorized use of electronic signatures and developing and maintaining the repository of approved electronic signature methods on the OIT website in MyUAH, https://my.uah.edu/.

Review The UAH Chief Information Officer (CIO) is responsible for the review of this policy every five years (or whenever circumstances require).

Approval

Campus Designee	Date
University Counsel	Date
Provost and Executive Vice President for Academic Affairs	Date

APPROVED:

President	Date