Administrative Guidelines for the Use of Electronic Signatures

I. Introduction

To potentially increase the efficiency of University business that requires authorization, the University of Alaska System (hereafter "the University") may require that members of the University community to accept and use electronic signatures (e-signatures) as part of an electronic transaction (e-transactions) to conduct business processes that previously required handwritten signatures and approvals on paper documents.

It is the intent of this guidance that all internal University business units and processes will accept the use of e-signatures except in rare circumstances that require notarization, are prohibited by law, or when a heightened level of security and /or assurance is required as outlined in Section V.

II. Scope & Applicability

This administrative guide applies to all units of the University and all members of the University community. Members of the University community include students and employees, prospective students and employees, patients, business partners, and other individuals who are associated with the University.

The University may require members of the University community to conduct university transactions electronically and formally acknowledge their agreement to University transactions in which they are parties by affixing an e-signature.

III. Electronic Signature Acceptance & Use

A. The University accepts e-signatures as legally effective and enforceable consistent with *Alaska Statute AS 09.80.010 et seq., the Uniform Electronic Transactions Act (UETA).* Under Alaska law, electronic signatures are equivalent to handwritten signatures to signify an agreement wherever applicable.

B. Parties external to the University community as described above in Section II; will be strongly encouraged to use e-signatures. Whether the parties agree to conduct a transaction by electronic means is determined from the context and surrounding circumstances, including the parties conduct.

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

D. The University's right or option to conduct a University transaction on paper or in non-electronic form shall not affect the University's right, option, or obligation to have documents provided or made available in electronic format.

E. The decision to use an e-signature should be weighed against the costs, complexity, and risk identified with the transaction.

F. The University provided DocuSign is the preferred and supported e-signature method for the University other systems using electronic verification appear in section V.

IV. E-Signature Approval & Initialization

It is the intent of this guidance that all university business units and processes will accept the use of e-signatures wherever a wet signature is currently acceptable; however, the University reserves the right to designate specific transactions that are not to be conducted using e-signatures. These exceptions shall be limited to those documents requiring the highest level of security or level 3 Assurance as outlined in section V below or are otherwise prohibited by law.

A. For enterprise level transactions the appropriate vice-president in consultation with the Chief Information Technology Officer will determine if a document or process meets the criteria for exception.

B. For internal campus-level transactions, the Chancellor or his/her designee will identify those documents that meet the criteria for exception.

C. Units will review annually the e-signature exceptions based on risks, security levels, and methodologies.

V. Implementation and Security Procedures

A. Electronic signatures may be implemented using various methodologies depending on the risk tolerance and level of assurance required for the transaction, and all relevant state, federal, and university policies, regulations, and guidelines. Examples of transaction risks include fraud, integrity, non-repudiation, and financial loss. The quality and security of the electronic signature method shall be commensurate with the risk and needed assurance of the authenticity of the signer (See Appendix A - Ink Signature to E-Signature Level of Assurance Versus Risk Matrix).

B. The University shall adopt security procedures for e-signatures that are practical, secure, and balance risk and cost.

C. The security requirements for a University transaction include, but are not limited to, password policies, secure transmission policies, access control policies and other relevant policies and regulations, as well as pertinent federal and state regulations.

D. Levels of Security

1. Minimal level of security:
   a. General information found on a web site
   b. Any document accepted not requiring a signature is suitable for this level
   c. Any document whose disclosure that would not have an adverse impact on the University
2. Heightened level of security:
   a. An internal official business communication
   b. An internal approval that requires a signature
   c. Items that could have an adverse effect on the university, assets, or public interest
3. Highest level of security:
   a. The transaction would initiate an irreparable action
   b. Any transaction that would require a witnessed signature (notarized) in written form
   c. Where electronic signatures are prohibited by law

E. Levels of Assurance for Authenticity (See Appendix A-Institutional Risk Vs Level of Assurance Diagram)

1. Level 1 assurance of the authenticity. A level 1 assurance of authenticity corresponds to communications or information that do not require a signature or authentication.
2. Level 2 assurance of the authenticity. A level two assurance requires a UA-system single factor authentication against a trustworthy UA-system that provides assurance and reliability of the process. A level two assurance corresponds to a University provisioned e-signature such as DocuSign or an internal system Workflow. An example is the electronic time sheet process that relies on a banner workflow (UA trustworthy reliable process) along with employee and supervisor access to the system.
3. Level 3 Assurance. A level three assurance for authentication corresponds to a verified and witnessed signature in the presence of a notary to document title transfer, deed, or trust.

F. Systems Utilizing Electronic Verification

System	Type of Signature
Banner (INB, SSB, & UAOnline)	Password/login authentication
OnBase	Captured signatures and/or records processed via DocuSign Password/login authentication
Email	Cryptographic signatures and/or DocuSign processed attachments
DocuSign	Password/login authentication, multi-factor

VI. Misuse or Abuse of Electronic Signatures and Transactions

Misuse or abuse of electronic signatures and transactions may violate Board of Regents' Policy, University Regulation, and Office of Information Technology policies. Sanctions for misuse or abuse of electronic signatures and transactions may include disciplinary action, up to and including termination of employment for employees and action under applicable Student Codes of Conduct for students, and criminal prosecution under applicable Federal and state laws.

Appendix A – Ink Signature to E-Signature Level of Assurance Versus Risk Matrix

Levels	**E-signature or Transaction**	**Ink Signature**	**Type of Transactions**	**Wet Signature Required by Law or Regulation Governing Transaction**	**E- Signature Required by Law or Regulation Governing Transaction**	**Risk**
Level 0	None	None	All other Transactions	Signature not needed	Signature not needed	None
Level 1	UA Domain E-mail access or not required	Unwitnessed ink-signature or not required	Standard business practices	E-signature not recommended	E-signature not required	Minor-significant can be absorbed
Level 2	Identity requires single factor authentication against a UA system	Unwitnessed signature Verify with Signature card	There is a need for Emphasizing Seriousness of Transaction	Signature Required by both parties (signer and approver)	Recommend E-signature	Substantial warrants effort to recover loss
Level 3	Identity requires multi-step or factor authentication	Witnessed signature/ Notarized	There is a need to Bind a Party to specific intent	Witnessed Signature Required/ Notarized	Currently not available at UA	Major irreparable action or damage

Appendix B - Glossary

Authentication

Authentication means the process of securely verifying the identity of an individual prior to allowing access to an electronic University service. Authentication 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

Authorization means verifying that an authenticated user has permission to access specific electronic University services and/or perform certain operations.

Electronic

Electronic means a technology that has electrical, digital, magnetic, wireless, optical or electromagnetic capabilities or similar capabilities.

Electronic record or e-record

Electronic record or e-record means a record of information that is created, generated, sent, communicated, received or stored electronically.

Electronic signature or e-signature

Electronic signature or e-signature means an electronic sound, symbol or process that is attached to or logically associated with a record and that is executed or adopted with the intent to sign the record.

Electronic transaction or e-transaction

Electronic transaction or e-transaction means an action or set of actions that is conducted or performed, in whole or in part, electronically or via electronic records.

Information

Information means data, text, images, sounds, codes, computer programs, software, databases or similar items.

Non-Repudiation

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

Record

Record means information that is inscribed on a tangible medium or that is stored in an electronic or other medium and that is retrievable in perceivable form made or received by the university that is evidence of its operations, and has value requiring its retention for specific period of time. Recorded information, regardless of medium or characteristics, made or received by the university that is evidence of its operations, and has value requiring its retention for a specific period of time.

[State of Alaska Records Definition – AS sect 40.21.150 (6)] "Record means any document, paper, book, letter, drawing, map, plat, photo, photographic file, motion picture film, microfilm, microphotograph, exhibit, magnetic or paper tape, punched card, electronic record, or other document of any other material, regardless of physical form or characteristic, developed or received under law or in connection with the transaction of official business and preserved or appropriate for preservation by an agency or a political subdivision, as evidence of the organization, function, policies, decisions, procedures, operations, or other activities of the state or political subdivision or because of the informational value in them; the term does not include library and museum material developed or acquired and preserved solely for reference, historical or exhibitions purposes, extra copies of documents preserved solely for convenience of reference, or stocks of publications and processed documents."

Repudiation

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

Security Procedure

Security Procedure means a procedure that is used to verify that an electronic signature, record, or performance is that of a specific person; to determine that the person is authorized to sign the document; and, to detect changes or errors in the information in an electronic record. This includes a procedure that requires the use of algorithms or other codes, identifying words or numbers or encryption, callback or other acknowledgment procedures.

Transaction

Transaction means an action or set of actions occurring between two (2) or more persons relating to the conduct of business, commercial, or governmental affairs.

Unit

Unit means the University organization conducting business by means of an e-signature such as a college, department, auxiliary, or administrative division.

University Transaction

A University Transaction means a transaction conducted in support of the University's teaching, service mission, research, or administration missions.