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).*

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

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 |
| [redacted] | DocuSign Password/login authentication |

# Accounting and Administrative Manual

Section 100: Accounting and Finance

## Appendix B - Glossary

Authentication

mUse( )-91(8S)-3(e)4(c)5(e)4(ive[(b1711(y)20( (m)-11(e)he uniher)(rsit2411(1)20( that is)-2( 4

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,81 0dn(m)-24BTrdl(i)-4(e)4s4( o( medium ad)-(. )]TJET EM

ID 6>BDC 1 g90.024 557.5590.02 Tm[( )]T>/784E16 in an

UNIVERSITY
of ALASKA