Responsible Executive: Chief Information Officer
Responsible Offices: Information Security Services
Effective Date: June 26, 2020
Last Revised: August 19, 2022

ELECTRONIC SIGNATURES

POLICY SUMMARY

This policy sets forth Northern Arizona University's authorization of and requirements for using Electronic Signatures to conduct Electronic Transactions. In accordance with its terms, University Community Members or third parties may have the option or be required to conduct University transactions electronically by employing Electronic Signatures. Where their use meets legal, policy, and security requirements, the University encourages, but does not require, the use of Electronic Signatures, Electronic Transactions, and Electronic Records to increase efficiency and save resources. University officials may designate University transactions to be conducted electronically by adding them to the *List of Approved Electronic Transactions*. Where the University relies on Electronic Signatures, accessible options, or other equally effective alternative means for completing the transaction will be provided. Students will have the opportunity to affirmatively consent to conducting their federal financial aid transactions with the University and to receive related notices electronically.

REASON FOR THIS POLICY

Guidance for the use of Electronic Signatures, Electronic Transactions, and Electronic Records supports the efficiency of University operations and compliance with applicable law, regulation, and policy.

ENTITIES AFFECTED BY THIS POLICY

- All units that engage in Electronic Transactions or use Electronic Signatures
- All units that administer documents that require a wet signature
- Disability Resources
- Information Security Services

WHO SHOULD KNOW THIS POLICY

- All faculty, staff, students, prospective students, agents, affiliates, associates, and volunteers who engage in Electronic Transactions with the University

DEFINITIONS

Access Credentials: information consisting of NAU User ID ("NAU UID") combined with a unique password used to access University information technology tools such as LOUIE and NAU electronic mail ("email") accounts. Pursuant to this policy, University access credentials may be used to authenticate the identity of signatories prior to application of their Electronic Signature.

Agreement: the bargain of the parties in fact, as found in their language or inferred from other circumstances and from rules, regulations, and procedures that are given the effect of agreements under laws otherwise applicable to a particular transaction. Rules, regulations, and procedures enacted by the Arizona Board of Regents ("ABOR") or the University that authorize Electronic Transactions or Electronic Signatures constitute such circumstances.

Digital Signature: a type of Electronic Signature that relies on public key or block chain infrastructure to authenticate both the signers of and the Electronic Record, as a means of maintaining the security and integrity of an Electronic Transaction.

Electronic Signature: a digital method of identification that is attached to or logically associated with an Electronic Record, which is executed or adopted by a signatory with the intent to be bound by and/or to authenticate the Electronic Record, and that meets the following requirements at the time of its execution:

i. Is uniquely linked to and under the sole control of the each NAU account holder using it;

ii. Is capable of reliable verification (*e.g.*, through multi-factor authentication and/or an audit trail that provides clear evidence of the signing process, such as the date, time, location, identity, etc.); and

iii. Is linked to the Electronic Record to which it relates in a manner that, if the Electronic Record is changed, the Electronic Signature is invalidated, or the Electronic Record maintains evidence that it was changed after signature.

Electronic Record: a record of information that is created, generated, sent, communicated, received, and/or stored by electronic means.

Electronic Transaction: an action or set of actions that is conducted or performed, in whole or in part, by electronic means and/or via Electronic Records. Agreements that are concluded, executed, and documented electronically are prime examples of Electronic Transactions.

Security Procedure: a method employed to verify that the application of an Electronic Signature, a Digital Signature, or a related performance is that of a specific person or to detect changes or errors in an Electronic Record. A Security Procedure may include the use of algorithms, codes, identifying words or numbers, encryption, callback, or other acknowledgment methods.

University Community Member: all University faculty, staff, student employees, students, alumni, affiliates, contractors, consultants, agents, and volunteers wherever located.

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

User Authorization: the process of securely verifying that an authenticated user has permission to access specific electronic University services and/or perform certain electronic operations, including the application of an Electronic Signature for the purpose of completing Electronic Transactions.

POLICY

A. Applicability

This policy applies to all University units and locations and all University Community Members. The applicability of this policy to third parties is governed by Agreements entered into between the University and the third party. This policy supplements and extends, but does not supersede or replace, the University's *Appropriate Use of Information Technology* and *Information Security* policies.

B. Terminology

For purposes of this policy, the term "electronic" refers to technology that has electrical, digital, magnetic, wireless, optical, electromagnetic or similar capabilities. The term "accessible options" refers to the ability to engage in Electronic Transactions using assistive technologies designed to allow persons with disabilities to successfully interact with electronic systems. The term "information" refers to data, text, images, sounds, codes, computer programs, databases, or similar items. The term "record" refers to information that is inscribed on a tangible medium or stored electronically and is thus retrievable to a physically perceivable form.

C. General

1. Where their use meets all applicable legal, policy, and security requirements, the University encourages the use of Electronic Signatures, Electronic Transactions, and Electronic Records to increase efficiency and save resources. To the fullest extent permitted by law, the University accepts Electronic Signatures as legally binding and equivalent to handwritten signatures to signify an Agreement. Where the University relies on Electronic Signatures, accessible options or other equally effective alternative means for completing the transaction will be provided.

2. University units may, at their discretion, request to conduct electronically University transactions for which they are responsible. Such requests are reviewed by the Chief Information Officer ("CIO"). The CIO is responsible for reviewing all requests submitted by University units to conduct University transaction by electronic means. To this end, the CIO will collaborate with other units as necessary or appropriate, including, but not limited to, Contracts, Purchasing, and Risk Management, Disability Resources, and the Office of General Counsel.

3. The consent of a party to agree to their Electronic Signature being effective may be inferred by the party's actions in conducting a transaction electronically; however, as set forth in Section G, students must have an affirmative opportunity to consent to conducting their federal financial aid transactions with the University and to receive related notices electronically.

4. The University may approve the use of Electronic Signatures, except in cases when doing so is prohibited by federal or state law or ABOR or University Policy (see section D for additional information).

5. This policy does not i) require the use of Electronic Signatures, Electronic Transactions, or Electronic Records; ii) limit the University's right or option to conduct a University transaction in non-electronic form on paper; or iii) affect the University's right or obligation to have documents be provided or made available on paper when required by applicable law, regulation, or policy.

6. The University will make available to the relevant parties an unaltered, fully executed, complete electronic copy of electronically signed Electronic Records. All Electronic Records shall be retained in accordance with the record retention requirements prescribed by the Arizona State Library, Archives and Public Records Division of the Arizona Secretary of State and University policy.

D. Approval of Electronic Transactions

Upon request by members of the President's Executive Team, the CIO will consider the appropriateness of and may designate specific University transactions to be conducted electronically using Electronic Signatures and Electronic Records. The CIO will ensure that all University transactions that are approved to be conducted electronically are listed in the *List of Approved Electronic Transactions*. Transactions that do not appear on the *List of Approved Electronic Transactions* are not approved by the University to be conducted electronically.

E. Security Procedures

1. The intent of this policy is to establish a framework for undertaking appropriate analysis and for approving the use of Electronic Signatures, Electronic Transactions, and Electronic Records on a case-by-case basis.

2. The University will adopt Security Procedures for its various uses of Electronic Signatures, Electronic Transactions, and Electronic Records that are practical, appropriately secure relative to the nature of the transaction or Agreement, that balance risk, cost, workability, and efficiency, and that comply with applicable law, regulation, and policy.

3. The Security Procedures for User Authentication may include, but are not limited to, use of the Central Authentication System ("CAS") or any successor, multi-factor authentication, or Digital Signatures.

4. User Authentication and User Authorization levels must be consistent with the security requirement appropriate for the specific University transaction or Agreement, including, but not limited to, password guidelines, secure transmission standards, and access control methodologies.

5. Based on this framework, the University may designate, in accordance with established procedures, certain University transactions or Agreements to be implemented via the use of Electronic Signatures, Electronic Transactions, and Electronic Records in the place of handwritten or paper documents.

F. Access Credentials

Pursuant to this policy, University Access Credentials may be used to verify an individual's identity for the purpose of conducting certain transactions electronically. Accordingly, as set forth in the *Appropriate Use of Information Technology Resources* policy, each NAU account holder is responsible for maintaining the integrity of their Access Credentials and preventing their unauthorized use. The intentional misuse of University Access Credentials is a serious violation of University policy that may result in disciplinary sanctions up to and including termination of employment or, in cases of student misconduct, expulsion from the University.

G. Electronic Financial Aid Transactions

Students must affirmatively consent in order to conduct federal financial aid transactions with the University electronically and to receive related notices via their NAU email accounts. Students who do not consent understand that they: i) will not be able to submit financial aid information online; ii) must submit financial aid documents in hard-copy form, which will extend processing time; iii) may not receive electronic reminder notices about financial aid disbursements or related matters. Students can update their financial aid consent preferences at any time.

H. Contract Signature Authority

Nothing in this policy is intended to authorize any individual to sign a contract or other written instrument on behalf of or that binds ABOR or the University if, pursuant to the *Contract Signature Authority* policy, the individual has not been granted such authority in advance.

I. Unauthorized Use and Responsibility to Report

All University Community Members are required to report any known or reasonably suspected fraudulent activities related to Electronic Transactions, Electronic Records, or Electronic Signatures immediately to an appropriate manager or supervisor in the individual's department, college, or division or to the Information Security Services by calling 928-523-3335. The recipient of such report will immediately notify the CIO. The CIO, in coordination with the appropriate executive leaders, will assemble an incident response team to investigate, preserve evidence, mitigate the situation, and analyze and report on the event.

J. Compliance and Enforcement

Individuals who intentionally falsify Electronic Records, Electronic Transactions, or Electronic Signatures are subject to disciplinary action, up to and including expulsion or termination of employment, and may also be subject to criminal prosecution pursuant to applicable federal or state law. Any corrective disciplinary response will be pursued in accordance with applicable ABOR and University conduct policies.

K. Construction

In the event of a conflict or inconsistency between this policy and any applicable law, regulation, or superior policy, the law, regulation, or superior policy will prevail.

RESPONSIBILITIES

Chief Information Officer: review and approve, while consulting with other officials or units as appropriate, all requests to conduct University transactions electronically; receive and act on reports of falsified Electronic Records in coordination with all affected parties; maintain the *List of Approved Electronic Transactions*.

Disability Resources: provide recommendations regarding the requirement to provide accessible options when the University uses Electronic Signatures and Electronic Transactions.

Executive Leaders: submit requests to the CIO when seeking to deploy or utilize Electronic Signatures or Electronic Transactions.

Information Security Services: provide information security recommendations regarding Electronic Transactions; receive and act on reports of falsified Electronic Records in coordination with the CIO.

PROCEDURES

There are no procedures associated with this policy.

RELATED INFORMATION

Forms or Tools

Cross-References

Appropriate Use of Information Technology

Contract Signature Authority

Electronic Mail

Sources

Arizona Revised Statutes §18-106

Arizona Revised Statutes § 44-7041

Americans with Disabilities Act of 1990, as Amended

Arizona Electronic Transactions Act (A.R.S. Title 44, Chapter 26, §§ 44–7001, –7051)

Electronic Signatures in Global and National Commerce Act ("ESIGN"), Public Law 106–229

Federal Student Aid Handbook, Volume 2, November 2019

APPENDIX*

Arizona Department of Administration Electronic and Digital Signature Policy

Standards for Electronic Signatures in Electronic Student Loan Transactions (U.S. Dept. of Education)

*Disclaimer: all documents, links, or other materials included in this policy's appendix are provided solely for the user's convenience and are not part of official University policy.