# Bemidji State University Policies

| **Policy Name:**<br>Electronic Signature | **Effective Date:**<br>July 1, 2022 |
|---|---|
| **Policy Owner:**<br>• Chief Information Officer<br>• Director of Business Services | Last Review: |
| | Next Review:<br>September 1, 2025 |

**Policy Statement**
Bemidji State University will establish requirements for the consistent, secure implementation and use of electronic signature technologies.

**Scope and Purpose of Policy**
This policy is applicable to documents or transactions using electronic signatures for official university business. The purpose of this policy is to establish acceptable use and implementation of electronic signatures that comply with applicable state and federal law, board policies, and system procedures and guidelines.

**Rationale**
The rationale for this policy is to provide procedures that will deliver the appropriate level of security and authentication when implementing or using electronic signatures for documents or transactions used in the course of official university business.

**Definitions**
Authentication: A verification that substantiates that a person is who the person says he or she or they is. Single or multi factor authentication validate the signer's identity using a Minnesota State recognized authentication technology system or process, in combination with an "approval" action by the signer acknowledging they are signing the document or conducting the transaction.

Electronic Signature: A digital or digitized signature made by electronic sound, symbol, or process that is attached to or logically associated with a document or transaction and that is executed or adopted with the intent to sign the document or transaction.

Digital Signature: A type of electronic signature produced by two mathematically linked cryptographic keys – a private key used to sign, and a public key used to validate the signature. A digital signature is created when a person uses his or her private key to create a unique mark (called a "signed hash") on an electronic document.

Digitized Signature: A graphic image of a handwritten signature in any form, including facsimile, where the digital signature image is applied to a digital document.

Faxed/Scanned Signature: A paper document with an original, handwritten signature that is converted into a digital document.

Electronic Signature Manager (ESM): The ESM is appointed by the president to carry out the duties associated with implementing electronic signature use on campus.

**Procedures**

Responsibilities

The president will appoint an electronic signature manager (ESM). The ESM will be an individual with knowledge of the employees who are delegated the responsibilities for business and/or academic functions or processes where electronic signatures will be used.

The ESM is responsible for overseeing and ensuring that implementation and proper use of electronic signaturerequirements are met.

The ESM may appoint a designee or delegate responsibilities to other university managers, supervisors, or key personnel to implement and/or oversee electronic signature requirements. If responsibilities are delegated, the ESM must document who receives delegation, his/her title or job position, the date of the delegation, and the person's electronic signature responsibilities. The ESM retains overall responsibilities to ensure requirements are met by all designees or delegates.

The ESM or their designee(s) are responsible for revoking electronic signature capabilities for employees, contractors, or third-party entities that no longer are authorized to use electronic signatures. The revocation must be documented including the person's name, job title or position, and the revocation date.

General

Use of electronic signatures for official business is permitted but not required. Any use of electronic signatures must comply with applicable state and federal law, board policies, and system procedures and guidelines.

Multiple methods of electronic signatures are acceptable for documents or transactions. The acceptable electronic signature technology type will depend on the level of assurance required to ensure the authenticity of the signer. The universities will document the electronic signature technology type acceptable for each type of transaction.

Categories of Transactions

A transaction is the act or process of doing business withanother person, company, agency, or entity.

The ESM shall place all transactions into one of four categories according to their potential negative financial, legal, or reputational impact to the university. These categories are Critical, High,Medium, or Low.

Factors to consider when categorizing may include the: (1) relationships between the parties; (2) value of the transaction; (3) potential for fraud or repudiation; (4) unauthorized access to, modification of, loss, or corruption of protected or sensitive data; and (5) probability that a

damaging event will occur.

- **Critical impact transactions.** These transactions will generally involve external parties and either exceptionally high dollar values, extremely sensitive data, or large volumes of private data. Repudiation of such transactions would result in catastrophic financial impact, extreme public distrust and media scrutiny, or high likelihood of adverse legal consequences. Examples of critical impact transactions may include but are not limited to master contracts, construction contracts, or collective bargaining agreements.
- **High impact transactions.** These transactions will generally involve external parties and either high dollar values, sensitive or private data. Repudiation of such transactions would result in significant financial impact, media scrutiny or public distrust, or the likelihood of adverse legal consequences. Examples of high impact transactions may include but are not limited to professional/technical and services contracts, lease agreements, or facilities use agreements.
- **Medium impact transactions.** These transactions will generally involve internal parties, moderate dollar values, and no sensitive or private data. Repudiation of such transactions would result in moderate financial impact, media scrutiny, public distrust, or low likelihood of adverse legal consequences. Examples of medium impact transactions may include but are not limited to intra-agency agreements, construction change orders, or human resources forms.
- **Low impact transactions.** These transactions will generally involve internal parties, non-material dollar values, and no sensitive or private data. Repudiation of such transactions would result in insignificant or no financial loss, no loss of public trust, or no likelihood of adverse legal consequences. Examples of low impact transactions may include but are not limited to time sheets or employee expense forms.

<u>Electronic Signature Technologies</u>

There are a number of electronic signature technology types. The technologies provide varying levels of security, authentication, record integrity, and protection against repudiation. A transaction's assessed level of impact, as identified in the 'Categories of Transactions' section above, must meet the minimum level of signature type required to mitigate potential risks, as described in the 'Process for Approval and Use of Electronic Signature Technologies' section below.

The following electronic signature technology types have been identified for use, subject to the requirements in the 'Process for Approval and Use of Electronic Signature Technologies' and the 'Electronic Signature Implementation Requirements' sections below. Definitions for these technologies are contained in the 'Definitions' section of the policy.

- Digital signatures
- Single or multi factor authentication
- Digitized signatures, to include graphical images and faxed or scanned signatures

Process for Approval and Use of Electronic Signature Technologies

In determining whether to approve use of an electronic signature, consideration will be given to the systems and procedures associated with using that technology type, and whether the use of that electronic signature technology type is at least as reliable as the existing method being used.

For each unique application of an electronic signature, the ESM shall, using the matrix below, ascertain the type of electronic signature required to minimize the risk of repudiation. This assessment is not intended to identify if the signer is authorized to sign or conduct the transaction. The ESM shall document and retain evidence of this assessment.

The ESM shall select the highest-level impact category applicable to a transaction.

| Transaction Category<br><br>Signature Type | Critical Impact | High Impact | Medium Impact | Low Impact |
|---|---|---|---|---|
| Original, Handwritten Signatures | Yes | Yes | Yes | Yes |
| Digital Signatures | Yes | Yes | Yes | Yes |
| Multi Factor Authentication | No | Yes | Yes | Yes |
| Single Factor Authentication | No | No | Yes | Yes |
| Digitized Signatures | No | No | No | Yes |
| Faxed/Scanned Signatures | No | No | No | Yes |

At the sole discretion of the university, an electronic signature used outside of the defined parameters may not be considered valid. In no circumstance is a typed name or stylized font to be used in place of an original, handwritten signature.

Electronic Signature Implementation Requirements

Regardless of the electronic signature technology type, any use of electronic signatures must conform to system guidelines and the following minimum requirements.

1. **Consent to conduct business electronically.** Both parties must agree to the use of electronic signatures for a transaction and users must be presented with language that informs them that an electronic signature is as legally binding as a handwritten signature. Users must affirm that they have read and understood this language. That affirmation shall be part of the permanent record retained for the transaction.
2. **Opt-out.** Users must be allowed to opt out of using an electronic signature and use a

handwritten signature.

3. **Reproduction of records.** Electronically signed records must contain all of the information necessary to reproduce the entire electronic record and all associated signatures in a format that permits the person viewing or printing the record to verify: a) the contents of the electronic record; b) the method used to sign the electronic record, if applicable; c) the full name of the person(s) signing the electronic record; and d) the date and time of each signature.
4. **Transmission.** After signing, a document must be transmitted in secure fashion to all parties in a format capable of being printed or stored. An electronic receipt or some form of electronic acknowledgement of a successful submission of the electronic record and signature must be provided.
5. **Alterations.** If an electronically signed document changes in any way, the document must indicate that it has been altered and that signatures affixed before alteration are now invalid.
6. **Records retention.** All electronically signed documents shall be retained in accordance with the applicable records retention schedule.
7. **Audit capability.** All electronic signature transactions must include audit capability.

Governance, Oversight, and Training

Selection and use of a particular digital signature technology, or password/PIN authentication technology must be approved by the Chief Information Officer.

Employee use of electronic signatures must be in alignment with the standard Delegation of Authority requirements established by the University.

Any employees involved in the administration of the electronic signature process shall receive appropriate training prior to use and when a new or replacement electronic signature technology is implemented.

At a minimum of every three years, the ESM shall re-examine and document the placement of transactions into the four designated categories as defined in the 'Process for Approval and Use of Electronic Signature Technologies' above with particular attention paid to continuing changes in technology and law.

At a minimum of every three years, the Chief Information Officer shall facilitate a re-assessment to determine the appropriate electronic signature technologies for each transaction category. In the event it is determined that an approved electronic signature technology is no longer trustworthy, the Chief Information Officer may revoke approval of that technology.

The use of any third-party electronic technology must conform to all requirements set forth in this policy.

**Supporting References**

- Minnesota State Board Policy 5.25: Use of Electronic Signatures

https://www.minnstate.edu/board/policy/525.html

- Minnesota State System Procedure 5.25.1: Use of Electronic Signatures https://www.minnstate.edu/board/procedure/525p1.html
- Minnesota State System Guidelines 5.25.1.1: Appropriate Use and Implementation of Electronic Signatures https://www.minnstate.edu/board/procedure/525p1g1.html