5.25.1 Use of Electronic Signatures

Part 1. Purpose. This procedure establishes requirements for the consistent, secure implementation and use of electronic signature technologies and prescribes the steps that must be followed prior to the implementation of electronic signatures.

Part 2. General. Use of electronic signatures for official business by colleges, universities, and the system office is permitted but not required. Any use of electronic signatures must comply with applicable state and federal law, board policies, including but not limited to, 1B.4, Access and Accommodation for Individuals with Disabilities, and adhere to delegation of authority as established under System Procedure 1A.2.2 Delegation of Authority.

Colleges and universities shall adopt, maintain, and appropriately disseminate policies and procedures approved by the president that define the terms under which electronic signatures may be used, create a process for approval of electronic signature technologies, and a process for authorizing and tracking employees that are permitted to use electronic signatures including any limitations. Colleges, universities, and the system office shall identify a local electronic signature manager to oversee implementation and to manage all actions related to electronic signatures.

Multiple methods of electronic signatures may be acceptable for college, university and system documents or transactions. The acceptable electronic signature technologies will depend on the level of assurance required to ensure the authenticity of the signer. Colleges, universities and the system office shall document the electronic signature technologies acceptable for each type of transaction.

Part 3. Categories of Transactions. A transaction is the act or process of doing business with another person, company, agency, or entity.

The electronic signature manager at each college, university, or the system office shall place all transactions into one of four categories according to their potential negative financial, legal or reputational impact to the college, university, or system office. These categories are Critical, High, Medium or Low impact.

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.

Subpart A. 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.

Subpart B. 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.

Subpart C. 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.

Subpart D. 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.

Part 4. Electronic Signature Technology Selection. There are a number of electronic signature technologies available. The technologies provide varying levels of security, authentication, record integrity, and protection against repudiation. A transaction's assessed level of impact, as identified in Part 3, must meet the minimum level of technology required to mitigate potential risks, as described in Part 5.

Minnesota State Colleges and Universities has identified the following electronic signature technologies for use, subject to the requirements in Parts 5 and 6 below.

Subpart A. Digital signatures. Validation of the signer's identity through a mathematical cryptographic process used to assure message originator authenticity, integrity, and non-repudiation. Use of digital signatures is appropriate for transactions needing very high confidence in the asserted identity's validity. Selection and use of a particular digital signature technology must be approved by the System Chief Information Officer.

Subpart B. Single or multi factor authentication. Validation of the signer's identity using a MnSCU-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.

1. **Single factor authentication.** Under this method the signer executes one authentication action that is recognized by MnSCU.

2. **Multi factor authentication.** Under this method the signer executes multiple authentication actions that are recognized by MnSCU.

These forms of authentication may include situations where no actual signature is applied, but a person must have access rights (usually password protected) to the system in order to perform the action. Use of single or multi factor authentication is appropriate for transactions needing high confidence in the asserted identity's validity. Use of single or multi factor authentication technology as an electronic signature must be approved by the System Chief Information Officer.

Subpart C. Digitized signatures.

1. **Graphical images.** Validation of the signer's identity through recognition of a graphical image of an original, handwritten signature applied to an electronic document, which may be rendered read-only after the application of the graphical image. Access controls can be applied to a signature library where such images are stored.

2. **Faxed or scanned signatures.** Validation of the signer's identity on a facsimile or scanned document through verification that the faxed signature was received from a facsimile number that belongs to or is traceable to the party that signed and transmitted the document or a scanned signature was received from an email address known to belong to the party that signed and transmitted the document.

Part 5. Process for Approval and Use of Electronic Signature Technologies. In determining whether to approve use of an electronic signature technology, consideration will be given to the systems and procedures associated with using that technology, and whether the use of that electronic signature technology is at least as reliable as the existing method being used.

For each unique application of an electronic signature, the electronic signature manager at each college, university, or the system office shall, using the matrix below, ascertain the level of technology 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 electronic signature manager shall document and retain evidence of this assessment.

Transaction Category **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 college, university or system office, an electronic signature used outside of the system-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.

Part 6. Electronic Signature Implementation Requirements. Regardless of the technology selected, any use of electronic signatures must conform to system guidelines and the following minimum requirements.

Subpart A. 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.

Subpart B. Opt-out. Users must be allowed to opt out of using an electronic signature and use a handwritten signature.

Subpart C. 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.

Subpart D. 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.

Subpart E. 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.

Subpart F. Records retention. All electronically-signed documents shall be retained in accordance with the applicable records retention schedule.

Subpart G. Audit capability. All electronic signature transactions must include audit capability.

Part 7. Governance, Oversight and Training.

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

Subpart B. Authority. Employee use of electronic signatures must be in alignment with the standard Delegation of Authority requirements established under System Procedure 1A.2.2 Delegation of Authority.

Subpart C. Training. Colleges, universities, and the system office shall ensure that any employee involved in the administration of the electronic signature process receives appropriate training on a continuing basis.

Subpart D. Review.

1. **Transaction categories**. At a minimum of every three years, the electronic signature manager shall reexamine and document the placement of transactions into the four designated categories as defined in Part 3 above with particular attention paid to continuing changes in technology and law.

2. **Electronic signature technologies**. At a minimum of every three years, the electronic signature manager shall reassess and document 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 electronic signature manager may revoke approval of that technology.

Part 8. Use of a Third-Party's Electronic Signature System. The use of any third-party electronic signature technology must conform to all requirements set forth in this procedure.

Part 9. Reporting Fraudulent Activity. Users shall report any suspected or fraudulent activities related to electronic signatures in accordance with Board Policy 1C.2 Fraudulent or Other Dishonest Acts.

Date of Implementation: 02/25/15,
Date of Adoption: 02/25/15,

Date and Subject of Revision: