Minnesota State Colleges and Universities
System Guideline
Chapter 5 – Administration

Guideline 5.25.1.1 Appropriate Use and Implementation of Electronic Signatures

Part 1. Purpose.
To establish requirements and responsibilities for acceptable use and implementation of electronic signatures. The requirements are designed to provide the appropriate level of security, authentication, and record integrity when implementing or using electronic signatures for transactions. Colleges and universities may adopt additional conditions of use, consistent with board policy, procedure, and this guideline.

Part 2. Authority.
Board policy delegates authority to the chancellor to develop system guidelines for purposes of implementing policy and procedure.

Part 3. Definitions.

Subpart A. Authentication. A verification that substantiates that a person is who the person says he or she is.

Subpart B. Data. Information collected, stored, transferred, or reported for any purpose, whether in computers or in manual files. Data can include: financial transactions, lists, identifying information about people, projects, or processes, and information in the form of reports.

Subpart C. Electronic Signature Manager (ESM). The ESM is appointed by the president at each college or university to carry out the duties associated with implementing electronic signature use on campus.

Subpart D. ESM Group. The group of all college, university, and system office ESMs. This group will meet on a regular basis and manage the electronic signature process.

Subpart E. Information Resources. Data collected, created, received, maintained, or disseminated by any Minnesota State Colleges and Universities user, regardless of its form, storage media, security classification, or conditions of use.

Subpart F. Information Technology Resources. Facilities, technologies, and information resources used for system member information processing, transfer, storage, and communications, including but not limited to computer labs, classroom technologies, computing and electronic communications devices and services, such as modems, e-mail, networks, telephones (including cellular), voice mail, fax transmissions, video, multimedia, and instructional materials.

Subpart G. Transaction. The act or process of doing business with another person, company, agency, or entity.

Subpart H. Signature types. The following include expanded definitions from board policy, and related additional definitions of signature types:

1. **Digital signature.** A type of electronic signature produced by two linked 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. The method used to link the two keys is called cryptography. It is a mathematical method to encrypt and decrypt a message.

2. **Multi-factor authentication.** Any two or more combinations of authentication methods. Authentication method examples may include: password/passphrase (something you know), token, smart card, digital certificate (something you have), fingerprint, retina scan, etc. (something you are). Often one method of authentication is something you know such as a username/password and a second authentication method that is something you have such as a token or smart card. An everyday example of multi-factor authentication is using a bank ATM card (something you have) where you input the card followed by a PIN (something you know). Although biometrics are not widely used yet, they would be considered something you are.

3. **Single-factor authentication**. A security process that requires one method of authentication before granting access to the user, typically a username with a password.

4. **Digitized signatures**. A digitized signature means a graphic image of a handwritten signature in any digitized form, then that digital signature image is applied to a digital document.

5. **Faxed/scanned signatures**. A paper document with an original, handwritten signature(s) that is converted into a digital document.

Part 4. Guidelines.

Subpart A. Responsibilities.

1. **College or university president responsibilities.** The president of the college or university must appoint an electronic signature manager (ESM) to oversee responsibilities for their institution as defined in board policy and procedure. The ESM should be an individual with knowledge of the employees who are delegated the responsibilities for business and/or academic functions or processes of the college or university where electronic signatures will be used.

2. **Electronic signature manager responsibilities.** The ESM is responsible for overseeing and ensuring that implementation and proper use of electronic signature requirements are met at their institution.

3. **Delegating electronic signature responsibilities.** The ESM may appoint a designee or delegate responsibilities to other college or 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.

4. **Revoking electronic signature capabilities.** 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.

Subpart B. Implementation oversight and management.

1. **Transaction categorization.** ESMs or their designees will ensure processes are implemented for categorizing each transaction into one of the four transaction impact levels: Critical, High, Medium, or Low.

   A Transaction Category tool to help determine transaction categorization is available on the electronic signature SharePoint site, and is meant to document the selection process and provide consistency of the process across the system. The Transaction Category tool is owned by the ESM group and is expected to evolve as experience warrants. The FAQ document related to this guideline also provides guidance with regard to document categorization.

   The Transaction Category tool will guide an ESM through evaluation of transaction impact levels for financial, legal, and reputational risk. College and university ESMs may consider other factors when categorizing their transactions including the: relationships between the parties; value of the transaction; potential for fraud; unauthorized access to, modification of, loss, or corruption of protected data; and/or probability that a damaging event will occur.

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

2. **Assigning signature type.** Based on the identified transaction impact level, the ESM or their designees will also approve and ensure that the type of signature selected for each transaction meets at least the minimum acceptable signature type as identified in Table A below.

3. **Documenting transaction categorization.** Once a transaction has been categorized and a minimum acceptable signature type has been assigned, it must be documented by the ESM with the transaction impact level: Critical, High, Medium, or Low, and with the minimum acceptable signature type. The table below can also be found in System Procedure 5.25.1 Use of Electronic Signatures.

4. **Identity verification for digital signature use.** Before being given a digital signature, a person must have his/her identity verified through an approved identity vetting process. Self-proclaimed identification is prohibited and is not an approved identity verification.

Table A. Acceptable Signature Type

Transaction Impact Level **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

Subpart C. Technical implementation.

ESMs are responsible for overseeing and ensuring that technical implementation requirements are met for electronic signature technologies in use at their institution. Business processes and/or electronic signature technologies must conform to the following 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 must 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 must be retained in accordance with the applicable records retention schedule.

7. **Audit capability.** All electronic signature transactions must include audit capability.

The requirements above may be met in different ways depending on the identified transaction impact level. Table B below illustrates acceptable examples for meeting the above requirements for each transaction impact level.

Table B. Technical Implementation Requirements

	Critical	**High**	**Medium**	**Low**
Consent	Capture date and time of consent, with user ID and consent text.	Capture date and time of consent, with user ID and consent text.	Overall consent form signed to cover all medium transactions.	Overall consent form signed to cover all low transactions.
Opt-Out	Capture date and time of opt out response with user ID and opt-out text.	Capture date and time of opt out response with user ID and opt-out text.	Overall consent form will state the ability to opt out. Reply by electronic means can be used to opt-out.	Overall consent form will state the ability to opt out. Reply by electronic means can be used to opt-out.
Reproduce **(cont'd next pg)**	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.	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.	Email with signed document in unalterable format (i.e., PDF, JPEG) will be the reproducible record or the fields in the system log.	Email with signed document will be the reproducible record or the system log.

Table B. Technical Implementation Requirements (cont'd)

	Critical	High	Medium	Low
Transmission	An electronic receipt or some form of electronic acknowledgement of a successful submission of the electronic record and signature must be provided.	An electronic receipt or some form of electronic acknowledgement of a successful submission of the electronic record and signature must be provided.	Email system or system log will acknowledge transmission.	Email system or system log will acknowledge transmission.
Alteration	Cryptographic key is used to validate document has not been changed.	Multi-factor product or process will be used to validate document has not changed.	Email with the signed attachments in unalterable format (i.e. PDF, JPEG) or the system log.	Email with the signed attachments or the system log.
Retention	All electronically-signed documents must be retained in accordance with the applicable records retention schedule.	All electronically-signed documents must be retained in accordance with the applicable records retention schedule.	Retained within email system or a system log.	Retained within email system or a system log.
Audit	Transaction audit log.	Transaction audit log.	Email log or a system log.	Email log or a system log.

Subpart D. Training

Colleges, universities, and the system office shall ensure that any employee involved in the administration or usage of electronic signatures receives appropriate training prior to use. At a minimum, refresher training must be conducted every three years or when a new or replacement electronic signature technology is implemented. ESMs are responsible for documenting training completion including the person's name, job title or position, and date of completion.

Subpart E. User responsibilities.

1. Electronic signature users must not share or disclose any authentication information they use for signing transactions with any other person, including but not limited to digital signature private key, passwords, PINs, multi-factor tokens, and answers to security questions.

2. **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.

Subpart F. Reviews

1. **Frequency.** At a minimum of every three years, the ESM shall reexamine the placement of transactions into one of the four designated categories with particular attention paid to continuing changes in technology and law. At a minimum of every three years, the ESM shall also determine the appropriate signature type for transactions, consistent with Table A above. The ESM shall document the review and any changes.

   At a minimum of every three years, the System Chief Information Officer shall facilitate a reassessment to determine the appropriate electronic signature technologies for each transaction category.

2. **Revocation of approved technologies**. In the event it is determined that an approved electronic signature technology is no longer trustworthy, the System Chief Information Officer may revoke approval of that signature technology at any time.

3. **Transition.** If an electronic signature technology is currently being used that has not been approved by the System Chief Information Officer, migration to an approved electronic signature technology must be completed within one (1) year. A request for an exception may be submitted to the System Chief Information Officer for consideration on a case-by-case basis.

4. **Notarization**. If a document or transaction requires notarization, electronic signatures along with the notarial stamp may be used to sign the documents or transactions in accordance with applicable laws and state statutes.

5. **Use of a third-party's electronic signature technology.** The use of any third-party electronic signature technology must conform to all requirements set forth in policy and procedure.

Date of implementation: 12/09/15,
Date of adoption: 12/09/15,
Date of last review:

Date and Subject of Revision: