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.

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.

. 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.

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

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.

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. 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.

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.

	Yes	Yes	Yes	Yes
	Yes	Yes	Yes	Yes
	No	Yes	Yes	Yes
	No	No	Yes	Yes
	No	No	No	Yes
	No	No	No	Yes