MINNESOTA STATE

Chapter 5 - Administration

Board Policy 5.25 Use of Electronic Signatures

Part 1. ~~Policy Statement~~Purpose~~.~~
This policy authorizes ~~colleges, universities, and the system office~~Minnesota State to use electronic signatures to conduct official business, to the extent such use meets the requirements of Minn. Stat. Ch. 325L and other applicable law, board policy, and system procedure.

Part 2. Definitions~~.~~
Terms used in this policy or ~~in~~ system procedure ~~shall~~ must be interpreted consistent with Minn. Stat. Ch. 325L and other applicable law.

~~Subpart A.~~ Authentication. ~~Authentication means the~~The process used to ascertain the identity of a person or the integrity of specific information. Authentication ensures that the user applying an electronic signature is in fact who they say they are and is authorized to sign.

~~Subpart B.~~ Digital signature. ~~Digital signature means a~~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~~their private key to create a unique mark (called a "signed hash") on an electronic document.

~~Subpart C.~~ Digitized signature. ~~Digitized signature means a~~A graphic image of a handwritten signature in any form, including but not limited to facsimile or scanned documents in ~~.pdf~~PDF (Portable Document Format) files.

~~Subpart D.~~ Electronic signature. ~~Electronic signature means a~~A digital or digitized signature made by electronic sound, symbol, or process that is attached to or logically associated with a record and that is executed or adopted with the intent to sign the record.

~~Subpart E.~~ Electronic record. ~~Electronic record means~~ A~~a~~ny record that is created, received, maintained, ~~and/~~ or stored through electronic means, regardless of the method used to create that record. Examples of electronic records include, but are not limited to, electronic mail, word processing documents, spreadsheets, and databases.

Part 3. Methodology to Reflect Level of Risk.

Prior to approving use of electronic signatures for any transaction category, a college, university, or the system office shall ensure that applicable legal requirements are met and that any operational risk is offset by the anticipated benefit, consistent with system procedure.

System procedures may provide for various methodologies, such as use of digital or digitized signatures, depending on the risks associated with the particular transaction, including fraud, repudiation, and financial loss. The quality and security of the electronic signature method must be commensurate with the risk and needed assurance of the authenticity of the signer, including whether to require a digital or digitized signature.

Part 4. Authority and Responsibilities.

Subpart A. Procedures.

The chancellor shall adopt system procedures to implement this policy, meet all applicable legal requirements, and ensure practical and secure application of electronic signatures.

Subpart B. Delegated authority.

Nothing in this policy ~~is intended to~~ authorizes any individual to sign on behalf of the Board of Trustees if ~~he or she~~the individual has not been granted such authority in accordance with board policy and system procedure.

Subpart C. Use of other formats.

This policy shall not be construed to require use of electronic signatures by a college, university, or the system office, or to limit the right of a college, university, or system office to conduct official business on paper or in non-electronic form, or to affect the right of a college, university, or system office to have documents provided or made available on paper.

Subpart D. Maintenance of electronic records.

Colleges, universities, or the system office may ~~must~~ maintain official records in an electronic format provided that the relevant record retention schedule is updated to reflect electronic record management and the college, university or system office has determined that the electronic records are trustworthy, complete, accessible, and durable.

Part 5. Sanctions.

Employees or students who falsify or misuse electronic signatures for college, university or system office transactions are subject to disciplinary action, up to and including termination or expulsion, and civil and criminal remedies.

Date of Adoption: 11/18/14,
Date of Implementation: 03/01/15,
Date and Subject of Revision:

MINNESOTA STATE

Chapter 5 - Administration

Board Policy 5.25 Use of Electronic Signatures

Part 1. Purpose

This policy authorizes Minnesota State to use electronic signatures to conduct official business, to the extent such use meets the requirements of Minn. Stat. Ch. 325L and other applicable law, board policy, and system procedure.

Part 2. Definitions

Terms used in this policy or system procedure must be interpreted consistent with Minn. Stat. Ch. 325L and other applicable law.

Authentication. The process used to ascertain the identity of a person or the integrity of specific information. Authentication ensures that the user applying an electronic signature is in fact who they say they are and is authorized to sign.

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 their 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 but not limited to facsimile or scanned documents in PDF (Portable Document Format) files.

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

Electronic record. Any record that is created, received, maintained, or stored through electronic means, regardless of the method used to create that record. Examples of electronic records include, but are not limited to, electronic mail, word processing documents, spreadsheets, and databases.

Part 3. Methodology to Reflect Level of Risk

Prior to approving use of electronic signatures for any transaction category, a college, university, or the system office shall ensure that applicable legal requirements are met and that any operational risk is offset by the anticipated benefit, consistent with system procedure.

System procedures may provide for various methodologies, such as use of digital or digitized signatures, depending on the risks associated with the particular transaction, including fraud, repudiation, and financial loss. The quality and security of the electronic signature method must be commensurate with the risk and needed assurance of the authenticity of the signer, including whether to require a digital or digitized signature.

Part 4. Authority and Responsibilities

Subpart A. Procedures

The chancellor shall adopt system procedures to implement this policy, meet all applicable legal requirements, and ensure practical and secure application of electronic signatures.

Subpart B. Delegated authority

Nothing in this policy authorizes any individual to sign on behalf of the Board of Trustees if the individual has not been granted such authority in accordance with board policy and system procedure.

Subpart C. Use of other formats

This policy shall not be construed to require use of electronic signatures by a college, university, or the system office, or to limit the right of a college, university, or system office to conduct official business on paper or in non-electronic form, or to affect the right of a college, university, or system office to have documents provided or made available on paper.

Subpart D. Maintenance of electronic records

Colleges, universities, or the system office may maintain official records in an electronic format provided that the relevant record retention schedule is updated to reflect electronic record management and the college, university or system office has determined that the electronic records are trustworthy, complete, accessible, and durable.

Part 5. Sanctions.

Employees or students who falsify or misuse electronic signatures for college, university or system office transactions are subject to disciplinary action, up to and including termination or expulsion, and civil and criminal remedies.

Date of Adoption: 11/18/14,
Date of Implementation: 03/01/15,
Date and Subject of Revision: