Office/Contact: Division of Technology and Security
Source: 15 U.S.C. Ch. 96, Sub Ch. I – Electronic Records and Signatures in Commerce; SDCL Ch. 53-12; SDBOR Policy 5.3; SDBOR Records Retention Manual; University Policies 3:2 and 5:1
Link: https://www.law.cornell.edu/uscode/text/15/chapter-96/subchapter-I; https://sdlegislature.gov/Statutes/Codified_Laws/DisplayStatute.aspx?Type=Statute&Statute=53-12; https://public.powerdms.com/SDRegents/documents/1722915; https://sdbor.edu/financial-reports/; https://www.sdstate.edu/policies/upload/Student-Records-FERPA.pdf; https://www.sdstate.edu/policies/upload/Contract-Agreement-and-Memorandum-of-Understanding-Review-and-Approval.pdf

SOUTH DAKOTA STATE UNIVERSITY
Policy and Procedure Manual

SUBJECT: Electronic Signatures
NUMBER: 7:2

1. Purpose

   To increase the efficiency of internal transactions that require authorization, the University may require that members of the University community use electronic signatures to conduct certain transactions that previously required handwritten signatures and approvals on paper documents.

   This policy and its procedures identify the requirements by which the University designates its transactions for which e-signatures are required and recognizes and authenticates e-signatures.

2. Definitions

   a. Agreement: The bargain of the parties in fact, as found in their language or inferred from other circumstances and from rules, regulations, and procedures that are given the effect of agreements pursuant to laws applicable to a transaction and as set forth in SDBOR Policy 5.3 and University Policy 5:1.

   b. Authentication: The process of securely verifying the identity of an individual prior to allowing access to an electronic University service. Authentication ensures that the user who attempts to perform the function of an electronic signature is in fact who they say they are and is authorized to "sign."

   c. Authorization: The process of verifying that an authenticated user has permission to access specific electronic University services, perform certain operations, or both.

   d. Electronic: Relating to technology that has electrical, digital, magnetic, wireless, optical or electromagnetic capabilities or similar capabilities.

   e. Electronic Record (or e-record): A record of information that is created, generated, sent, communicated, received or stored electronically.

f. Electronic Signature (or e-signature): An 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.

g. Electronic Transaction (or e-transaction): An action or set of actions that is conducted or performed, in whole or in part, electronically or via electronic records.

h. Information: Data, text, images, sounds, codes, computer programs, software, databases or similar items.

i. Non-Repudiation: The inability of either party in a voluntary transaction to reject, disown, or disclaim the validity of that transaction.

j. Record: Information that is inscribed on a tangible medium or that is stored in an electronic or other medium and that is retrievable in perceivable form.

k. Repudiation: The willful act of either party in a voluntary transaction to reject, disown, or disclaim the validity of that transaction.

l. Security Procedure: A procedure that is used to verify that an electronic signature, record, or performance is that of a specific person; to determine that the person is authorized to sign the document; and, to detect changes or errors in the information in an electronic record. This includes a procedure that requires the use of algorithms or other codes, identifying words or numbers or encryption, callback or other acknowledgment procedures.

m. Signature Authority: Permission given or delegated to sign instruments, contracts, or other documents on behalf of the University.

n. Transaction: An action or set of actions occurring between two (2) or more persons relating to the conduct of business, commercial, or governmental affairs.

o. Unit: the University organization conducting business by means of an e-signature such as a college, department, auxiliary, or administrative division.

p. University Transaction: A transaction conducted in support of the University's teaching, research, or service mission.

3. Policy

a. This policy and its procedures apply to all units of the University and all members of the University community. Members of the University community include students and employees, prospective students and employees, business partners, and other individuals who are associated with the University, such as affiliate entities.

b. To the fullest extent permitted by law, the University accepts e-signatures as legally binding and equivalent to handwritten signatures to signify an agreement.

c. Students shall use electronic signatures to authorize all designated internal records and transactions, as required by University policies and procedures. Examples include, but are

not limited to: registering for courses, accepting financial aid awards, paying student bills, obtaining unofficial transcripts, completing electronic forms, etc.

d. Employees shall use electronic signatures to authorize all designated internal documents. Examples include, but are not limited to: submitting grades, viewing personal payroll data, accessing protected data through the administrative computing system and web applications provided by the unit, signing off on timesheets, etc.

e. Only those employees with Signature Authority delegated in accordance with SDBOR Policy 5.3 and University Policy 5:1 are authorized to execute Agreements on behalf of the University.

    i. University employees with delegated Agreement Signature Authority who execute Agreements on behalf of the University must use a secure electronic signature application that has been approved by the Vice President for Technology and Security, designee, or successor, when signing electronically. Approved and properly conforming electronic signatures are legally binding and equivalent to handwritten signatures.

    ii. University employees with delegated Agreement Signature Authority are equally accountable for properly and appropriately executing Agreements on behalf of the University whether they sign the document manually or electronically.

f. University employees who lack delegated Agreement Signature Authority, but have been designated another specified approval authority, may use an electronic signature for approving non-legal, internal documents.

g. In accordance with University Policy 5:1, the Office of the Vice President for Finance and Budget, or successor, is responsible for maintaining and making available documentation and information concerning individuals with delegated Agreement Signature Authority at the University.

h. The Vice President for Technology and Security, designee, or successor, is responsible for approving requests by University employees for the use of electronic signatures to ensure that requestors have specified or delegated Signature Authority.

i. Other members of the University community, upon mutual agreement with the University, may use electronic signatures to conduct designated University transactions and to formally acknowledge their agreement to University transactions in which they are parties by affixing an e-signature.

j. The University's right or option to conduct a University transaction on paper or in non-electronic form shall not affect the University's right, option, or obligation to have documents provided or made available in paper format.

k. The Division of Technology and Security shall maintain information on implementation of this policy, Signature Authority authorizations, and use guidelines and provide training to users prior to their authorized use of e-signatures.

l. It is a violation of this policy for an individual to sign a University transaction on behalf of another individual, unless they have been granted specific authority by that individual.

m. Individuals shall report any suspect or fraudulent activities related to electronic signatures immediately to the University Controller.

n. Employees who falsify electronic signatures or otherwise violate this policy and its procedures are subject to disciplinary action, up to and including termination of employment and referral for criminal prosecution under applicable federal and state laws.

o. Students who falsify electronic signatures or otherwise violate this regulation are subject to disciplinary action under the Student Conduct Code and referral for criminal prosecution under applicable federal and state laws.

p. Other members of the University community who falsify electronic signatures or otherwise violate this regulation are subject to appropriate sanctions, including but not limited to termination of the relationship and referral for criminal prosecution under applicable federal and state laws.

4. Procedures

a. Enterprise-Level Transactions:

i. The principal University administrators, data custodians, and enterprise application system owners shall assess the potential for replacing a manual process, signature, or both with an electronic process, signature, or both to automate a process and propose joint recommendations for implementation of automation, subject to approval by the Vice President for Technology and Security, designee, or successor and their Vice President. Once a process for a University transaction is approved and automated, it is automatically subject to the provisions of this policy.

b. Other transactions:

i. For all other transactions, the transaction to be enabled by e-signatures shall be evaluated by the unit, in conjunction with the Vice President for Technology and Security, designee, or successor. For risk assessment and review purposes, similar types of transactions may be grouped together under one agreement. Implemented e-signatures shall be reviewed periodically for appropriateness and continued applicability.

ii. Individuals with Signature Authority who wish to sign legal documents on behalf of the University electronically must submit a request to the Vice President for Technology and Security, designee, or successor to request approval. The Vice President for Technology and Security, designee, or successor will verify with the Office of Finance and Budget whether the employee has Agreement Signature Authority before authorization.

c. Implementation and Security

i. Electronic signatures may be implemented using various methodologies depending on the risks associated with the transaction, and all relevant state, federal, and University policies and procedures. Methodologies are determined, approved, and deployed by the Vice President for Technology and Security, designee, or successor. Examples of transaction risks include: fraud, non-repudiation, and financial loss. The quality and security of the electronic signature method shall be commensurate with the risk and needed assurance of the authenticity of the signer.

ii. The e-signature methodology shall be commensurate to the assurances needed for the risks identified. Specifications for recording, documenting, and/or auditing the electronic signature as required for non-repudiation and other legal requirements shall also be determined by the unit.

iii. The University shall adopt security procedures for e-signatures, e-transactions and e-records that are practical, secure, and balance risk and cost. It is not the intent of this policy and its procedures to eliminate all risk, but to provide a process for undertaking an appropriate analysis prior to approving the use of e-signatures, e-transactions or e-records for specific University transactions; and, based on such analysis, to designate those University transactions in which e-signatures, e-transactions and e-records shall be required in place of handwritten documents.

iv. The security requirements for a University transaction include, but are not limited to, password policies, secure transmission policies, access control policies and other relevant University and SDBOR policies, as well as pertinent federal and state regulations.

5. Responsible Administrator

The Vice President for Technology and Security, or designee, is responsible for the bi-annual and ad hoc review of this policy and its procedures. The University President is responsible for approval of this policy.

SOURCE: Approved by President on 09/08/2015. Revised 01/31/2024 (clerical).