Rice University Policy No. 849

USE OF ELECTRONIC SIGNATURES

I. General Policy

Employees must have signature authority in order to execute contracts and other legal documents and procurements on behalf of Rice University (see Policy 810). Rice encourages the use of electronic records and signatures whenever they can increase efficiency and save resources, so long as their use meets legal and security requirements.

Recognizing that electronic transactions promote efficiency, federal and state statutes now provide that a record or signature may not be denied legal effect or enforceability solely because it is in electronic form. This policy is intended to promote efficiency and save resources by providing general guidance on the use of electronic signatures and records at Rice.

This policy codifies how the University will designate those University transactions for which e-signatures will be required and how the University recognizes e-signatures. This policy also requires that the University establish Security Procedures regarding the use of e-signatures, e-transactions, and e-records in connection with University transactions.

This policy applies to all individuals who are affiliated with the University, whether paid or unpaid, including but not limited to faculty, staff, students, affiliates and volunteers. This policy may require members of the University community to conduct University transactions electronically and to formally acknowledge their agreement to University transactions in which they are parties by affixing an e-signature.

II. Definitions

Electronic record - any combination of text, graphics, data, audio, pictorial, or other information in digital form that is created, modified, maintained, archived, retrieved, or distributed by a computer system.

Electronic signature - a computer data compilation of any symbol or series of symbols executed, adopted, or authorized by an individual to be the legally binding equivalent of the individual’s handwritten signature.

Signature authority - permission given or delegated to sign instruments, contracts, receipts or other documents on behalf of the University.

III. Elaboration of Policy

A. Approval of Electronic Signature Methods

Because those with signature authority are executing legal documents on behalf of the University, their electronic signatures must use a secure certificate-based electronic signature service that has been approved by the Office of Information Technology (OIT). This OIT-endorsed service and a step-by-step description of its use are provided in procedures. This electronic signature service is available to those with signature authority, as well as to those that would create and send documents for signatures.

OIT must approve all electronic signature services used for signature authority to ensure that (i) the services have appropriate security procedures that can accurately attribute electronic records or electronic signatures to the individuals that created them, and (ii) the services do not result in the remote storage of confidential or sensitive University records without proper safeguards.
In addition, OIT must approve all requests by employees to use the secure, authenticated electronic signature application to create and send documents for signature. Anyone with signature authority will be able to sign the documents whether they have access to the system or not.

Members of the Rice community with signature authority may use only those electronic signature methods that are stated in OIT procedures, unless:

- the electronic signature is part of an electronic workflow system that has been approved by OIT; or
- they have received written permission from the Information Security Office to use a different signature method; or
- the signature method is part of a document management service provided to Rice under a contract approved by the Office of the General Counsel and the Information Security Office.

B. Use of Electronic Signatures and Electronic Records

Except as stated below, when the law or Rice policy requires a written signature on a document binding the University, you may use an approved certificate-based electronic signature. Approved certificate-based electronic signatures are legally binding and equivalent to handwritten signatures.

Except as stated below, when the law or Rice policy requires a written document, you may meet this requirement by creating and retaining an electronic record. Electronic records are legally binding and equivalent to written documents.

Except as stated below, when the law or Rice policy requires that a record be retained in its original form, you may retain the record as an electronic record so long as:

- the electronic record is maintained in reasonable order and in a safe and accessible place so that it can be readily inspected or examined;
- the electronic record is legible in its electronic form; and
- the electronic record is readily convertible into a legible paper copy.

If you are unsure whether a document may be signed or retained electronically, you may consult the Office of the General Counsel.

C. Exceptions to Use of Electronic Signatures and Electronic Records

You may not use electronic signatures or electronic records when Rice policies or federal or state laws or regulations do not allow their use. The following are important examples of records that cannot be signed or retained electronically:

- wills and testamentary trusts;
- promissory notes;
- any document required to accompany any transportation or handling of hazardous materials, pesticides or other toxic or dangerous materials;
- notices involving mortgages or leases that could lead to the loss of a primary residence; and
- notices of the cancelation or termination of health insurance, health benefits, or life insurance benefits.

If you are unsure whether a document may be signed or retained electronically, you may consult the Office of the General Counsel.
D. Accountability

Employees with signature authority are equally accountable for properly and appropriately executing documents on behalf of the University whether they sign the document manually or electronically.

E. Electronic Signatures for Internal Non-Legal Approvals

If you would like to use an electronic signature application for approving internal documents or workflows, there are no University requirements to use a specific application. However, you should consult with Information Technology to ensure that you select an application that is appropriate for the task, and will maintain an appropriate audit trail.

IV. Cross Reference to Related Policies

Policy 808. Protection of University Data and Information
Policy 810. Signature and Approval Authority for Contracts

V. Responsible Official and Other Key Offices

Responsible Officials: Vice President for Information Technology
Other Key Offices: Vice President for Finance
Information Security Office
Office of the General Counsel

Signed David W. Leebron
David W. Leebron
President

Policy History
Issued: May 21, 2019