



UNIVERSITY OF RICHMOND

Policy Manual

Policy #:	FIN-4412	Policy Title:	Electronic Signature Policy
Effective:	05/21/2024	Responsible Office:	Office of General Counsel
Date Approved:	05/20/2024	Approval:	Executive Vice President and Chief Operating Officer Vice President and General Counsel
Replaces Policy Dated:	N/A	Responsible University Officials:	Vice President and General Counsel Director of Procurement

PURPOSE:

This policy provides guidelines for the use of Electronic Signatures (as defined herein) at the University of Richmond (the “University”), including defining the circumstances under which Electronic Signatures may be used and accepted in conducting University business.

SCOPE:

This Policy applies to University faculty, staff, business partners, affiliates, and associates acting in their authorized capacities in connection with official University activities. It applies to all uses or potential uses of Electronic Signatures for the creation, approval, and execution of Contracts (as defined herein).

This Policy does not require the use of Electronic Signatures or prohibit the ability to engage in contracts or other transactions on paper.

This Policy does not apply: (a) to University systems with existing built-in electronic approval workflows, such as Workday, Ellucian Banner, Chrome River, ESM and OnBase; (b) when a handwritten signature on paper is required by law; (c) to facsimile signatures used on checks issued by the University; or (d) to Internal Agreements (as defined herein) or other documents or records that are solely internal to the University.

INDEX:

- FIN-4412.1.....Definitions
- FIN-4412.2.....Use of Electronic Signatures
- FIN-4412.3.....Approved Electronic Signature Methods and Products

FIN-4412 – Electronic Signature Policy

FIN-4412.4..... Acceptance of Third-Party Electronic Signatures

FIN-4412.5..... Violations

POLICY STATEMENT:

FIN-4412.1 – Definitions

Assurance — The degree of confidence in the identity of the individual providing an e-signature.

Authentication — The process of securely verifying the identity of an individual providing an electronic signature.

Authorization — Verifying that an authenticated user has permission to access specific electronic University services and/or perform certain operations on behalf of the University.

Contract — A contract is a binding commitment by or on behalf of the University that is in oral or written form, regardless of the title of the operative document or documents. For purposes of this policy, the term “contract” includes but is not limited to contracts, agreements, leases, memoranda of understanding (“MOU”), gift agreements, mutual aid agreements, settlement agreements, resolution agreements, letter agreements, and binding letters of intent. This policy applies to contracts in hardcopy or electronic form.

Internal Agreement — For purposes of this policy, internal agreements are written or electronic documents that describe a formal understanding between two or more University units, departments, schools, or divisions regarding operational matters, such as use of space, allocation of funds, service level commitments, or similar internal matters. Internal agreements may take several forms but they are typically documented in the form of MOU’s.

Electronic Record or E-record — A record, including a contract, that is created, generated, sent, communicated, received, or stored by electronic means.

Electronic Signature or E-Signature — An electronic sound, symbol or process, attached to or logically associated with an electronic record and executed or adopted by a person with the intent to sign such record.

Electronic Transaction or E-transaction — An action or set of actions that is conducted or performed, in whole or in part, by electronic means or via electronic records.

Electronic Signature Method — The method by which the identity of the applicable signatory and his/her intent to use an electronic signature has been verified.

FIN-4412.2 – Use of Electronic Signatures

Subject to this Policy and other applicable University policies, and applicable law, a Contract or other Electronic Record may be executed via an Electronic Signature obtained using an Approved Electronic Signature Method, as described in Section FIN-4412.3 of this Policy. An Electronic Signature must be attributable or traceable to a person who has the intent and authority to sign the Contract or Electronic Record, with the use of adequate security and authentication measures contained in the method of capturing the Electronic Signature.

Only those University employees who are authorized to sign Contracts on behalf of the University under the University’s Delegation of Contract Approval and Signature Authority Policy may execute a Contract on

behalf of the University using an Electronic Signature. This requirement applies to click-through contracts for software or software as a service.

FIN-4412.3.....Approved Electronic Signature Methods and Products

Electronic Signatures must be obtained by using an Electronic Signature Method that meets the following requirements: For an e-signature method to meet the requirements of this Policy, the proposed e-signature method must:

- a. Use commercially reasonable and current electronic security protocols;
- b. Appropriately verify the identifies of the signatories;
- c. Maintain the information in a retrievable format for the time period prescribed in the University’s Record Retention Policy; and
- d. Be auditable.

Except as provided in this Policy, University employees or others signing a Contract or Electronic Record on behalf of the University shall only use an Electronic Signature product (*e.g.*, Box Sign) that has been approved by the University and for which the University has a current enterprise Contract. If required to use the Electronic Signature product of a third-party vendor that has not been approved by the University, the University employee authorized to sign the vendor Contract must consult with the University’s Director of Information Security or their designee prior to using such Electronic Signature product.

FIN-4412.4..... Acceptance of Third-Party Electronic Signatures

In general, when the University enters into a Contract or is a signatory to an Electronic Record involving a third party, the University and third party should consent to the use and acceptance of Electronic Signatures. Preferably, the Contract or Electronic Record will contain language that the respective signatories certify that they are authorized to sign documents on behalf of their organization and consent to the use of Electronic Signatures. In situations where obtaining such consent is impossible or impracticable, consent may be implied by the context or the parties’ conduct or course of dealing.

FIN-4412.5.....Violations

Individuals who falsify Electronic Signatures may be subject to disciplinary action under applicable University policies and handbooks and criminal prosecution under applicable federal and state laws. Individuals are required to report any suspected or fraudulent activities related to e-signatures immediately in accordance with the University’s Reporting and Investigating Suspected Financial Fraud, Waste, and Abuse policy.

RELATED POLICIES:

FIN-4408 Contract Management Policy

FIN-4409 Delegation of Contract Approval and Signature Authority Policy

FIN-16001 Reporting and Investigating Suspected Financial Fraud, Waste, and Abuse

[Record Retention Policy](#)

POLICY BACKGROUND:

Reviewed by President’s Cabinet and approved on May 20, 2024

POLICY CONTACTS:

Director, Procurement, Procurement Office
Vice President and General Counsel