UNIVERSITY OF OREGON
ESIGNATURE PROCEDURES

Effective as of August 5, 2019

UNIVERSITY OF OREGON
ESIGNATURE PROCEDURES

1. **Purpose**. In accordance with UO Policy IV.04.06 (the "E-Signature Policy"), and any applicable law or regulation, these procedures set out the requirements, authorized methods, and standards by which University students, faculty, and staff may electronically sign Documents or accept Documents with Electronic Signatures.

1.1. Definitions. In addition to the terms defined in the E-Signature Policy and the Data Classifications established in UO Policy IV.06.02, the following terms have the meanings specified below:

1.1.1. **Certification**. Electronic Signatures that a Signatory applies to either Internal or External Documents meant to demonstrate their approval, or an attestation of fact, when such an approval or attestation does not form a Contract.

1.1.2. **Contract**. An agreement between two or more persons or entities that the parties' intend to be enforceable by law.

1.1.3. **"Click-Through" or "Clickwrap" Contract**. A Contract where a party accepts an offer from another party by clicking a digital prompt that does not require an Electronic Signature.

1.1.4. **E-Signature System**. A software system that creates electronically signed Documents.

1.1.5. **External Documents**. Documents that may be electronically signed by individuals whose identity the University's Single Sign-On system cannot authenticate.

1.1.6. **High Risk Documents.** High Risk Documents are any Document that is not a Low Risk Document, as defined below.

1.1.7. **Internal Documents**. Documents only electronically signed by individuals whose identity is authenticated by the University's Single Sign-On system.

1.1.8. **Low Risk Documents.** Low Risk Documents include the following:

1.1.8.1. Contracts that contain only Low Risk Data under the University Information Asset Classification and Management Policy or call for parties to exchange only Low Risk Data, and have a value of $25,000 or less;

1.1.8.2. Purchase Orders in any amount that do not include High Risk Data (unless it was only a Vendor's requirements that classified data they are receiving as High Risk Data); and

1.1.8.3. Certifications on External or Internal Documents that only contain Low Risk Data.

1.1.9. **Signatory**. The individual signing a Document on their own behalf, or as an agent of a legal entity.

1.1.10. **Single Sign-On**. A system that allows users to log in with a single ID and password to gain access to any of several related systems.

2. Security and Authentication Requirements

2.1. High Risk Documents. E-Signature Systems the University uses to Electronically Sign High Risk Documents must meet the following security, identity authentication and Document authentication requirements.

2.1.1. **Security.** E-Signature Systems must meet the University's data security policies and facilitate end user compliance with the University's acceptable use policies. E-Signature Systems vendors must provide a valid SOC2 report, a valid ISO 27001 Certification, or be approved by the Chief Information Security Officer ("CISO") after completing the University's vendor data security questionnaire or providing a completed HECVAT.

2.1.2. **Identity Authentication.** Signatory identity authentication for Internal Documents must occur via the University's Single Sign-On system. Signatory identity authentication for External Documents may occur in the following ways: 1. via the University's Single Sign-On system; 2. when a Signatory provides their e-mail address, mailing address, and phone number that is separately confirmed by University staff or an authorized representative of entity for which the Signatory is signing; or 3. via a third-party authentication system approved by the CISO.

2.1.3. **Document Authentication.** The E-Signature System must record and maintain Document processing flow between users and the time and date a Signatory completes actions, including signing, in response to the E-Signature System's prompts. Additionally, the E-Signature System must produce final Documents in a format that complies with the University's Document retention policies.

2.2. Low Risk Documents. E-Signature Systems the University uses to Electronically Sign Low Risk Documents must meet the following security, identity authentication and Document authentication requirements.

2.2.1. **Security.** E-Signature Systems must meet the University's internal data security policies and facilitate end user compliance with the University's acceptable use policies.

2.2.2. **Identity Authentication.** Signatory identity authentication for Internal Documents may occur via the University's Single Sign-On system, or when the Signatory provide their e-mail address. Signatory identity authentication for External Documents may occur in the follow ways: 1. via the University's Single Sign-On system; 2. when the Signatory provides or confirms their legal name and either their physical address or e-mail address; or 3. via a third-party authentication system approved by the CISO.

2.2.3. **Document Authentication.** The E-Signature System must produce final Documents in a format that complies with the University's Document retention policies.

2.2.4. **Click-Through Contracts.** For purposes of these Procedures, Click-Through Contracts are not treated as creating or requiring an Electronic Signature. Execution of Low Risk Documents does not require execution via Electronic Signature, and may be evidenced via a "Click-Through" Contract, so long as the digital prompts and click-through process meets the requirements for security, identity authentication, and Document authentication for Low Risk Documents. Notwithstanding the foregoing, Signatories to Click-Through Agreements may authenticate their identity via Single Sign-On, or providing a valid e-mail address and the Signatory's full legal name.

3. Use of Non-University E-Signature Systems and acceptance of Electronic Signatures from Non-University Signatories. University employees with appropriate authority may use non-University E-Signature Systems, at their own discretion, when required by third-parties to both

Certify documents and execute Contracts. However, such systems should generally meet the Security, Identity Authentication, and Document Authentication requirements established under these Procedures. Furthermore, University employees may accept Electronic Signatures that are not the product of a University E-Signature System, at their discretion, so long as the Non-University Electronic Signature can be authenticated at the same level of certainty as a handwritten signature.

Images of handwritten ink signatures, either scanned as part of a physical Document or as an image pasted on an Electronic Record, are not Electronic Signatures. The employee responsible for managing that Electronic Record may accept such handwritten signatures at their discretion.

4. **Document Retention.** All electronically signed Documents, including the Electronic Signature and any data or metadata necessary to authenticate an Electronic Signature, must be retained in accordance with the University's Document Retention Schedule. Electronically signed Documents must be stored in a manner that allows the removal of all digital identity authentication measures that would impede access to permanent records while not altering the content of the records. No E-Signature System will act as a records retention system without prior approval by the University's Records Manager.