E-Signature Policy Overview and General Guidance

POLICY

Unless otherwise required by law, the University is not required to send or accept e-signatures for transactions. Rather, state law allows the University to determine whether and to what extent to allow the use and acceptance of e-signatures (electronic signatures) on records (e.g., completed forms and documents) to authenticate transactions. (*RCW* 19.360)

Based on business assessments and risk analyses, the University has determined that it will permit University units to utilize e-signatures for transactions, except as indicated under Restrictions.

The University has developed a standard policy regarding e-signatures (this section, *BPPM* 90.50) and accompanying standard procedures regarding e-signature use for University transactions (see *BPPM* 90.51). The standard policy and procedures apply to University transactions for all units. EXCEPTION: Individual units are permitted to establish their own policies, processes, and methodologies for e-signatures, as provided under Individual University Units and Customized Policies.

Restrictions

E-signatures may *not* be used or accepted for *any* of the following types of transactions:

- Willed body agreements
- Promissory notes, except related to student loans serviced by a third party
- Real property title documents
- Sureties and guarantees of payment from a third party
- Transactions which require a notarized signature, sworn signature, witnessed signature, an apostille, or a recorded document
- Assumption of risk and release of liability documents for high risk transactions or situations

  NOTE: The Risk Management Advisory Group (RMAG) reviews and assists with drafting assumption of risk and release of liability waivers on a case-by-case basis. The RMAG must approve electronically-signed risk and release of liability waivers prior to use. See also Business Assessment and Risk Analysis.
- Assignments of intellectual property

E-Signature Policy Overview and General Guidance

Restrictions (cont.)

- Administrative or academic documents held to stricter standard for signatures as identified by a unit's customized e-signature policy and as posted on the college/area website
- For purposes forbidden by state or federal law

Responsibility

The divisions of Finance and Administration and Information Technology Services, in consultation with Internal Audit, are responsible for developing and maintaining the University's e-signature policy and procedures (*BPPM* 90.50 and 90.51).

Business Assessment and Risk Analysis

The following factors must be considered when determining whether to permit the utilization of e-signature:

- Potential efficiencies of the use of e-signatures;
- Potential risks of the use of e-signatures;
- Ability to correctly maintain the records;
- Ability to correctly associate the e-signatures to the records;
- Applicable University policies; and
- Applicable state and federal laws.

In order to reduce the scope of the risk, the University has established the limitations provided in this policy (*BPPM* 90.50) and the standard University e-signature procedures in *BPPM* 90.51.

For assistance with risk analysis, contact the Risk Management Advisory Group; e-mail riskmanagement@wsu.edu; telephone 509-335-3682. See also *Executive Policy Manual (EPM)* EP6.

Additional Guidance

Additional guidance and assessment tools for conducting business assessments and risk analyses are available in the state e-signature guidelines at:

ocio.wa.gov/sites/default/files/Electronic_Signature_Guidelines_FINAL.pdf

Individual University Units

An individual University unit may adopt customized policies for the use of e-signatures for that unit's transactions. Such policies may include, but are not limited to, transaction size thresholds or limitations, additional processes, and particular methodologies.

Any such customized policies must be consistent with this policy and relevant state and federal laws. The customized policies may be more restrictive than the standard policy and procedures, but may not be less restrictive. See Customized Policies for individual unit policy requirements.

E-Signature Policy Overview and General Guidance

Individual University Units (cont.)

Unless a unit establishes and publishes a customized e-signature policy in accordance with the requirements in this section (*BPPM* 90.50), the standard procedures (*BPPM* 90.51) must apply to that unit's University transactions.

Exceptions

Individual University units must submit an E-Signature Use Exception Request to the Contracts Office to request exceptions to the e-signature use restrictions in this policy (*BPPM* 90.50). (See Restrictions.) The Contracts Office coordinates with the Risk Management Advisory Group on analysis and possible approval of such exceptions.

The E-Signature Use Exception Request form is available in PDF format on the Procedures, Records, and Forms (PR&F) website at:

policies.wsu.edu/prf/index/forms/

REQUIREMENTS

Customized Policies

Any customized policy developed by an individual unit must also meet the requirements below and reflect this guidance.

The unit's college or area executive administrator (e.g., dean, vice president, or chancellor) must review and approve any customized e-signature policies before implementation.

The customized policies are to be published on the college or area website, in order to be clearly available to clients and all employees responsible for compliance.

The college or area must send the link for the customized policies webpage to the Office of Procedures, Records, and Forms (PR&F) for inclusion in the list in Appendix 1. The college or area must provide PR&F with link updates, as applicable.

To contact PR&F, send email to:

prf.forms@wsu.edu

Signature Authority

All employees with signature authority are accountable for properly and appropriately executing records on behalf of the University, including when such records are executed using e-signatures.

E-Signature Policy Overview and General Guidance

Signature Authority (cont.)

NOTE: Signature authority is established separately for contracts, expenditures, employee appointments, and budgets. See *BPPM* 10.10, 60.10, 70.02, and EP29 for further information regarding various types of University signature authority.

E-Signature Methods and/or Processes

The state policy requires the University to identify the specific e-signature methods and/or processes that the University intends to use or accept for specific transactions. (*RCW* 19.360.020) WSU identifies such methods and/or processes in *BPPM* 90.51.

The e-signature methods and/or processes used by the University conform to the guidelines established by the state Office of the Chief Information Officer (OCIO). See:

ocio.wa.gov/sites/default/files/Electronic_Signature_Guidelines_FINAL.pdf

E-Signature Authenticity and Reliability

All employees accepting legally-binding documents from another party are accountable for properly and appropriately vetting the authenticity and determining the reliability of the documents. Reliability includes, but is not limited to, ability to retain the e-signature and associate it with the record it authenticates.

Reasonable Access and Transaction Reliability

The University takes into account the need for reasonable access and the ability of persons to participate in and rely upon University transactions that are conducted electronically. (See EP7 and EP8.)

Notify the State OCIO

The University must send a link to the e-signature policy and applicable University contact information to the state Office of the Chief Information Officer (OCIO) for posting on the OCIO website. (*RCW* 19.360.020(4)(b))

Update Policy

The University must update the e-signature policy and procedures as transactions, processes, or procedures for accepting and using e-signatures are revised. (See *BPPM* 90.51.)

SIGNATURE GUIDANCE

Purpose of a Signature

A signature on a document identifies the signer and signifies that the signer and/or the entity authorizing the signature understands and intends to carry out whatever is stipulated in the signed record. The act of signing alerts the signer that they may be making a legally-binding commitment.

E-Signature Policy Overview and General Guidance

Definitions

E-Signature

An e-signature is:

- 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 the record.

(*RCW* 19.360.030(2))

An e-signature may be used with the same force and effect as a signature affixed by hand, unless specifically provided otherwise by law or University policy.

Record

A record is defined by the state as any paper, machine-readable material, completed form, or other document, regardless of physical format, made or received by the state in connection with the transaction of public business. (*RCW* 40.14.010) See also *BPPM* 90.01.

REQUIRED COMPONENTS

In order for an e-signed record to be considered valid, it must satisfy five major signing requirements:

- The electronic form (method) of signature must be authorized and accepted by law and policy;
- The identification and authentication of the signer must be possible based on the e-signature;
- The signer must intend to sign;
- The e-signature must be reliably associated with the record;
- The signed record must have integrity (e.g., legibility, no indication of alteration, secure and reliable storage process, access limited to authorized persons).

Further information regarding the required components of valid e-signatures is available at:

ocio.wa.gov/sites/default/files/Electronic_Signature_Guidelines_FINAL.pdf

E-Signature Policy Overview and General Guidance

Form of E-Signature	Methods used to create an electronic form of signature that may be adopted at Washington State University include, but are not limited to:
Click Through or Click Wrap	The signer signs or types their name or personal identifier and clicks an agreement button.
PIN or Password	The signer enters identifying information, which may include a name or identifying number and a personal identification number (PIN) or password, which is verified to "authenticate" the person.
Digitized Signature	A digitized signature is a graphical image of a handwritten signature. The graphical image may be created by scanning an image of a handwritten signature or using a computer input device, such as a digital pen and pad.
Digital Signature	The digital signature process uses a private user signing key and a public validation key to verify that the document was not altered after signing. The signature is indicated by a unique mark (called a *signed hash*). The public key is often issued by a trusted third party (certification authority), that binds individuals to private keys and issues and manages certificates.
Autopen Signature	An autopen signature is created by a mechanical device that copies and stores a template (or digital pattern) of a user's real signature and recreates the signature using a mechanical arm and pen, pencil, or marker.
Hybrid Approaches	Hybrid approaches involve combining techniques from several methods to provide increased security, authentication, record integrity, and nonrepudiation.
Identification and Authentication of Signer	A signature must be the act of a specific person. To be enforceable, there must be proof that the alleged signer actually signed the record. The level of confidence required by a given identification and authentication process should be based on the level of business impact or loss if the alleged signer later denies their involvement in the transaction.
Intent to Sign	The overall signing process should be designed to clearly identify the reason for signing and clearly specify the actions to be taken by the signer to signify intent.

E-Signature Policy Overview and General Guidance

Association of Signature to Record

For a paper transaction, the handwritten signature is permanently affixed to the record. Likewise, the sound, symbol, or process that constitutes an e-signature must in some way be attached to, or associated with, the electronic record being signed.

The method used to attach or associate the signature with the record must provide evidence that a specific e-signature was applied to or used in connection with a specific electronic record.

Integrity of Signed Record

Electronic records can be easily altered in a manner that is not detectable. To preserve the integrity of a signed record, the University or University departments must implement controls to preserve the accuracy and completeness of electronic records sent over the Internet or stored in electronic systems. Further measures should be taken to ensure that no unauthorized alterations are made to electronic records either intentionally or accidentally.

Integrity Control Measures

Integrity control measures include, but are not limited to:

- Encrypted transport protocols
- Message hashing (method for providing rapid access to data items which are associated with a key)
- Message encryption
- Multifactor authentication

See also EP8.

RECORDS MANAGEMENT

University electronic records must be maintained in accordance with University records retention requirements. See *BPPM* 90.01 for further information regarding retention factors and other records management requirements.

APPENDIX 1: Customized Unit Policies	
Unit Name	**Policy Webpage / URL**
Graduate School	*Graduate School Policies and Procedures Manual*, Chapter One E.6: gradschool.wsu.edu/chapter-one-e/