Standard E-Signature Use for University Transactions

STANDARD PROCEDURES OVERVIEW

Unless a University unit establishes and publishes a customized e-signature policy in accordance with the BPPM 90.50, the following standard procedures apply to the use of e-signatures for University transactions.

Definition

For the purpose of the e-signature policy and procedures (BPPM 90.50 and 90.51), transactions are exchanges or interactions where a signature, declaration, acknowledgement, or assent of some sort is required by one or more parties to the transaction.

University transactions include, but are not limited to, transactions between:

- Two or more University departments;
- The University and employees or students; or
- The University and a non-University company, agency, group, or individual (other than a University student or employee).

Restrictions

E-signatures may not be used or accepted for any of the types of transactions listed under "Restrictions" in BPPM 90.50.

ACCEPTABLE E-SIGNATURE METHODS

The following e-signature methods may be utilized for University transactions, with the stated restrictions. (See "Forms of E-Signature" in BPPM 90.50 for definitions.)

Authorized Use

Any department using any type of signature methods/devices must ensure that:

- The person whose signature is used has approved signature authority for the document. See "Signature Authority" in BPPM 90.50 for further information.
- Anyone affixing the person's signature to a document has authority to use the signature on the specific document being signed.

Checkbox, Click Through, or Click Wrap

- An online checkbox, click through, or click wrap signature in which a signer is asked to affirm their intent or agree online by clicking a button, if all the following criteria are met:
  - Information is available that tends to validate that the e-signature clicking was done by the individual represented to be the person completing the form or document (e.g., the signer must use a log-in verification system with a unique ID and password to access the check-box, click-through, or click-wrap signature field); and
  - The e-signed document is retained in its entirety for WSU records.
Standard E-Signature Use for University Transactions

PIN or Password • An e-signature created through use of a personal identification number (PIN) or password, if all the following criteria are met:
  ◦ Information is available that tends to validate that the e-signature was affixed by the individual represented to be the person completing the form or document (e.g., the PIN and/or password are created and maintained in a secure fashion); and
  ◦ The e-signed document is retained in its entirety for WSU records.

Digitized Signature • A digitized signature (e.g., scanned image of an individual's signature) on a document, if all the following criteria are met:
  ◦ The document is sent as an attachment in an email message or other retainable technology;
  ◦ Information is available that tends to validate that the email or other retainable technology was sent either by:
    • The individual whose signature is represented to be on the document; or
    • An individual authorized to send the email or other retainable technology transmitting the document;
  ◦ The e-signed document is retained in its entirety for WSU records; and
  ◦ The transmittal document (for example, the transmittal email) is retained for WSU records where possible.

Digital Signature • A digital signature, if all the following criteria are met:
  ◦ A private user signing key and a public validation key is used to verify that the document was not altered after signing.
  ◦ The public key is issued by a certification authority that binds individuals to private keys and issues and manages certificates.
  ◦ The signature is indicated by a unique mark (called a signed hash).

Autopen Signature The signature device must be secured from unauthorized use and the person with signature authority is responsible for securing the device.
Standard E-Signature Use for University Transactions

Hybrid Approaches
Hybrid approaches combining techniques from several e-signature methods are acceptable if all of the applicable criteria listed above are met.

Software Program
Any type of e-signature may be created through a software program, if all the following criteria are met:

- The software system tracks the signature process;
- The software system logically associates all the signed record’s components, such as the identity of the signer and the date and time of signature;
- The circumstances surrounding the creation of the signature tend to validate that the signature was in fact affixed by the individual whose signature is represented to be on the document; and
- The e-signed document is retained in its entirety for WSU records.

Contact ITS regarding allowable software programs for creating e-signatures or to review potential software programs.

Specific Transactions
The divisions of Finance and Administration and Information Technology Services may recommend or require the use of specific e-signature methods for specific transactions based upon the levels of risk involved (e.g., amount of money at issue).

End User Instructions and Training Materials
University departments which use or accept e-signatures are responsible for providing clear instructions and training materials for users.

COMPLIANCE
University employees and areas which utilize e-signatures for University transactions are responsible for following all laws and policies applicable to e-signatures, as well as laws and policies applicable to University transactions. NOTE: All transaction laws and policies apply regardless of whether or not signatures are obtained on paper copies or using e-signatures.

An employee and their area must bear the liability that arises from the failure of the employee and/or area to follow applicable laws and policies.

Records Retention
Requirements regarding retention of University records apply regardless of the media or technology used to create and store the records. (See BPPM 90.01.)