Electronic Signatures

University Operations – Administrative

EWU Policy 201-05	**Authority: EWU Board of Trustees**
Effective May 12, 2017	**Proponent: Business and Finance**

Purpose: This policy identifies Eastern Washington University (hereafter "the University") requirements and standards for the use of electronic signatures (hereafter "e-signatures") in conducting business operations in support of the institutional administration of the University's teaching, research, and service operations.

History: This policy is a new policy. It was adopted during open session of the EWU Board of Trustees on May 12, 2017 and is effective as of that date.

Applicability: This policy applies to all uses of electronic signatures for Eastern Washington University business, teaching, research, and service operations.

1. GENERAL

1-1. Purpose

This policy is intended to promote efficiency, save resources and provide parameters on the use of e-signatures in university transactions.

This policy codifies how the university will designate transactions for which e-signatures will be required and recognized by the university. This policy also requires the university establish security procedures regarding the use of e-signatures and does not replace any University Information Security Policies.

Employees must have delegated signature authority in order to execute legal documents on behalf of the University.

1-2. Definitions

"Agreement" is a negotiated and legally binding arrangement between parties as to a course of action.

"Electronic" means relating to technology having electrical, digital, magnetic, wireless, optical, electromagnetic, or similar capabilities.

"Electronic signature (e-signature)" is an electronic sound, symbol, or process attached to or logically associated with a contract or other record and executed or adopted by a person with the intent to sign the record.

"Electronic Record" is information captured through electronic means, which may or may not have a paper record to back it up.

1-3. E-Signatures Authorized

An electronic signature may be used with the same force and effect as the use of a signature affixed by hand, as long as the electronic signature and the writing conform to the definition in this policy. Electronic signatures may not be used for any documents that legally require a notarized signature, such as an affidavit or certain real estate transactions. An e-signature used that is not authorized per the requirements of this policy or is used outside of its limitations may be considered invalid by the University.

University employees with signature authority are executing legal documents on behalf of the University; therefore, their electronic signatures must use a secure certificate-based electronic signature service that has been approved by Information Technology.

2. WHEN E-SIGNATURES MAY BE USED

Before a department can use an e-signature method in place of a paper-based signature, such use must be authorized by the university's designated Risk Manager in accordance with the following process:

2-1. Department Level Risk Assessment

If a department wishes to use a non-paper based signature for an agreement, it must first conduct a department-level risk assessment. The assessment is intended to ascertain the benefits associated with using an e-signature compared to the risks associated with such use. The assessment should also identify the quality and security of the e-signature method required as it relates to operational and legal risk. The department must document its analysis and submit a request to the Risk Manager to approve the use of an e-signature for the transaction.

In conducting the risk analysis, the focus should be identifying risk factors that could lead to a challenge to the validity or enforceability of the e-signature. Guidelines for conducting this analysis are provided in the next section.

2-2. Risk Analysis Factors

The following analysis is a guide to how high or low risk transactions could be:

A. Parties to the Transaction - generally the closer the relationship, the lower the risk of repudiation. Individual

departments should consider whether the proposed transaction is:

i. A transaction between university department and/or employees

ii. An inter-agency transaction

iii. A transaction between the University and an outside, non-governmental entity

iv. The University and an individual

v. The University and a foreign government or organization

B. Nature of the Relationship and Frequency of Transactions - risks tend to be lower when there is an ongoing relationship and when they engage in frequent transactions. On the other hand, typically the highest risk usually involves a one-time transaction between a person and an agency that has financial or legal implications. Departments should consider whether the transaction involves:

i. An ongoing relationship,

ii. A new relationship with a known party,

iii. A new relationship with an unknown party, or

iv. An in-person signing or remote signing.

C. The Value of Significance of the Transaction - departments should consider the relative value of the type of transaction against the costs associated with implementing technology and management security controls to mitigate risk. Higher risks include:

i. Transactions involving transfer of funds,

ii. Transactions where parties are committing to actions or contracts that could give rise to legal of financial liability, and/or

iii. Transactions with information protected under state or federal law such as where the party is fulfilling a legal responsibility, which if not performed creates a legal liability or where the party is certifying information, which if not true creates a legal liability.

D. The Risk of Unauthorized Alteration or Other Compromise - this risk increases with the likelihood of a security intrusion to the stored record. The likelihood depends on the potential attacker's knowledge that the transaction will occur and value of information. The following transactions are at higher risk:

i. Regular or periodic transactions between parties,

ii. The value of information to outside parties can determine motivation to compromise the information, and

iii. Transactions with certain agencies who have a perceived image or mission that could warrant higher risk of attacks.

E. Whether the Lack of a Signature Invalidates the Transaction - The final overarching factor to consider is the extent of resulting loss or impact. If the signature is required by law then any challenge to the enforceability of the signature will usually invalidate the entire transaction. If the signature is not required but only desired than the transaction will most likely remain valid without a signature. In addition, some transactions require a provable, electronically signed record that can be produced in case of an audit, investigation, dispute, or litigation. Departments must consider the impact an invalidated agreement would have on operations.

2-3. Department Request

After completing the risk analysis above, the department must submit a request to the Risk Manager for use of an e-signature. The department should also identify the type of approved e-signature method (set forth in section 3) that it wishes to use.

2-4. Risk Manager Decision

The Risk Manager, in collaboration with the Data Custodian, Information Technology, and other appropriate university departments (e.g. finance, human resources, etc.) will review the department's request to use an e-signature in place of a paper-based signature. The Risk Manager will go through the same risk management analysis set forth in section 2-3. In addition to assessing the level of risk to the department, the Risk Manager is responsible for assessing the level of risk to the University if an e-signature method is used and to determine if there are mitigating measures that can be used, such as using a more secure e-signature method. The Risk Manager is also responsible for determining whether the department has the capabilities in place to properly maintain electronic signatures in compliance with chapter 4 of this policy and state law.

After completing the risk analysis, the Risk Manager will send the department a memo approving or disapproving the request. The Risk Manager may also place parameters over the use of such signatures or permit them for a limited period of time to test a certain method.

2-5. Periodic Review

A review of each e-signature implementation will be conducted periodically, but no less that every time an approach or solution changes by the department and Risk Manager. This will include an evaluation of the e-signature used to determine whether any applicable legal, business, or data requirements have changed. A determination will be made as to the continued appropriateness of the risk assessment and e-signature implementation method.

A record of this review will be documented and filed as part of the official record for this e-signature implementation maintained by the department. If as a result of the periodic review the risk level changes, a new risk assessment must be completed, including review and approval.

3. AUTHORIZED E-SIGNATURE METHODS

3-1. Process for Approving E-Signature Methods

There are many different methods of e-signatures. Before a department is permitted to utilize e-signatures, the particular e-signature method must be approved for use by the Vice President for Business and Finance and Vice President of Information Technology. Before approving an e-signature method, the Vice Presidents must assess whether it meets the following criteria:

A. Identification and Authentication of the Signer: A signature must be the act of the specific person identified in the agreement. If the alleged signer later denies signing, the signature could be unenforceable unless there is proof the alleged signer actually signed the record. The parties relying on the terms of a signed transaction must determine the type of electronic signature that best meets the university's needs to identify and authenticate a signature based on level of business impact or loss if the alleged signer denies their involvement in the transaction.

B. Intent to Sign: The signing process should clearly identify the reason for signing and specify the actions to be taken by the signer to signify intent. To avoid confusion regarding a signer's intent, any method used must give the signer an opportunity to review the entire document, ensure it contains the same signature elements as it would if it were a paper record, require the signer to indicate assent to the document by clicking an accept or reject button, and record and retain a copy of the date, time and the signer's indicated intent.

C. Association of Signature to the Record: The e-signature must be attached to, or associated with the electronic record being signed. The data comprising the e-signature must be saved. It is recommended that the following data be affixed with the e-signature:

i. Identify of the signer,

ii. Date and time of the signature,

iii. Method used to sign the record, and

iv. A reasoning for the signing.

Whichever method is used to associate the signature with the document, it is imperative that the university obtain and maintain proof that a specific e-signature was applied to or used in connection with a specific electronic record.

D. Integrity of the Signed Record: The integrity of the document relies on the ability of the storage process used to protect it from unauthorized persons and natural disasters. Steps must be taken to preserve the accuracy and completeness of the electronic information. Further measures should be taken to ensure no unauthorized alterations are made to the document. This protection is possible through the system that manages the electronic record. This system must ensure that a record, its signature, any associated data or links cannot be tampered with or modified.

If the e-signature is being used for interstate transactions or for documents required by the federal government, it must meet all of the requirements of the Electronic Signatures in Global and National Commerce Act (E-SIGN), 15 USC § 7001-7031.

3-2. Approved E-Signature Methods

The approval of an e-signature method can limit the use of that method to particular electronic records, particular classes of electronic records, or particular university departments.

Types of e-signature methods that may be considered include:

A. Click Through or Click Wrap – This method has a signer affirm his or her intent by clicking a button. Some versions require signers to type his or her name, some personal identifier or type "I agree" before clicking a button. These types of e-signature should only be used for low-risk, low-value transactions.

B. Personal Identification Number (PIN) or Password – This method requires a person to enter identifying information such as a PIN or password and the system verifying that the PIN or password is associated with the person accessing the system to authenticate the person. Examples would include requiring a student to type in a student identification number. This method is more secure than a click through agreement, but less secure than a digitized or digital signature because someone other than the person identified in the agreement could have obtained the other person's PIN or password.

C. Digitized Signature – This method is an image of a handwritten signature. It is most effective if applied at the time of signing and can be compared to copies of digitized signatures on file. If special software judges the two images comparable, the signature is deemed valid.

D. Digital Signature - this method is created when the signer uses his or her private signing key to create a unique mark on an electronic document. The recipient of the document employs the signer's public key to validate the authenticity of the private key to verify the document was not altered after signing. If approved e-signature methods require the use of encryption technology that uses public or private key infrastructure and/or certificates, Information Technology will be responsible for the administration of such public or private keys and certificates.

3-3. Repealing and Approved Method

In the event that it is determined that an approved e-signature method is no longer meeting university needs, the Vice President for Business and Finance and Vice President of Information Technology, may revoke the approval of that e-signature method. In the event authorization of a method is revoked, the university will take steps to minimize the risk, such as having people re-resign documents with an approved signature method.

4. PRESERVING ELECTRONIC AGREEMENTS AND SIGNATURES

Preserving the electronic document is a necessary step in the electronic records process. Electronic records must be retained for the same length of time as if it were signed in ink. Retention of the record means it needs to remain usable, searchable, retrievable and authentic for the entire length of time it must be preserved. For an e-signature, the record must include: what the signer is agreeing to, the signature, date and time of the signing and evidence of the process the person followed to establish their identity and a clear intention to sign. E-signatures must be displayed as close as possible to the other terms of the transaction. The more remote the signature on the display is from the other terms, the more difficult it becomes to prove intent.

Changes in technology need to be considered when retaining electronic records in the event that they need to be changed to other electronic formats.

The department also must maintain chain of custody of the record, including employing sufficient security procedures to prevent additions, modifications, or deletion of a record by unauthorized parities. If there is a break in chain of custody, it must be documented.

Printing and retaining a hard copy is not a substitute for the electronic version unless approved by the records custodian.

Additionally, a record of the risk assessment evaluation, approval from the Risk manager, and e-signature method selection must be maintained by the department.

5. AUTHORITY

5-1. Electronic Signatures and records, RCW 19.360

5-2. Electronic Signatures in Global and National Commerce Act (E-SING) 15 USCA §7001-7031