**Austin Peay State University**

# Acceptance of Electronic Signatures

**POLICIES**

**Issued:** March 25, 2017
**Responsible Official:** Vice President for Finance and Administration
**Responsible Office:** Information Technology

## Policy Statement

The intent of this policy is to allow for e-signature use and the acceptance of system, faxed, emailed, and scanned signatures at APSU by means of methods that are practical, secure, and balance risk and cost. It is not the intent of this policy to eliminate all risk but rather to provide a process that gives parties assurance that appropriate analysis was completed prior to implementation of e-signature or the acceptance of system, faxed, emailed, and scanned signatures, and that the level of user authentication used is reasonable for the type of transaction conducted.

## Purpose

To establish protocol for the conducting of paperless transactions and approvals through reliance upon verifiable electronic signatures.

## Contents



## Definitions

| | |
|---|---|
| **Authentication** | To establish as genuine and verify the identity of a person providing an electronic signature. |
| **Credential** | An object that is verified when presented to the verifier in an authentic transaction. |
| **Electronic Record** | A contract or other record created, generated, sent, communicated, received, or stored by electronic means. |
| **Electronic Signature** | An electronic signature/approval (e-signature) is defined as an electronic identifier that is created by a computer and is intended by the party using it to have the same intent, affect and authority as the use of a manual (either written or facsimile) signature. An electronic signature can be the person's typed name, their email address or any other such identifying marker. |
| **Transaction** | A discrete event between a user and system that supports a business or programmatic purpose. |

## Procedures

| | |
|---|---|
| **General Procedures** | E-signatures may be implemented using various methodologies depending on the risks associated with the transaction. Examples of transaction risks include: fraud, non-repudiation, and financial loss. The quality and security of the e-signature method should be commensurate with the risk and needed assurance of the authenticity of the signer. Authentication is a way to ensure that the user who attempts to perform the function of an electronic signature is in fact who they say they are and is authorized to "sign".<br><br>An e-signature may be accepted in all situations if requirement of a signature/approval is stated or implied. This policy does not supersede situations where laws specifically require a written signature. This policy cannot limit the right or option to conduct the transaction on paper or in non-electronic form and the right to have documents provided or made available on paper at no charge. The e-signature must be protected by reasonable security measures as applicable to established computer functions of the University. |
| **System/Faxed/Emailed/ Scanned Signatures** | The electronic process expedites obtaining required contractual information. |

A system, faxed, scanned, or emailed signature shall be considered just as valid as an original written signature except when an actual original signature is required by state or federal law; when the system, faxed, scanned, or emailed signature cannot be verified; or when the other party desires original signatures.

In order to accept a system, faxed, scanned, or emailed signature in lieu of an original written signature, the authenticity of such system, faxed, scanned, or emailed signature must be verified by the receiving party. Such means of verification shall include:

A. The entry of a system signature within an application that is is intended by the party using it to have the same intent, affect and authority as the use of a manual (either written or facsimile) signature.

B. The receipt of a faxed signature from a facsimile number verified as belonging to or traceable to the party that did so sign and transmit the document.

C. The receipt of a scanned or emailed signature from an email address verified as belonging to the party that did so sign and transmit the document. E-mail access being based on unique credentials (username/password) will be accepted as the electronic record for the e-mail and associated attachments from vendors. Electronic signature will be the scanned document containing the authorized written signature from the vendor/contractor.

Furthermore, in order for a system, faxed, scanned, or emailed signature to be considered valid, both parties must agree that a system, faxed, scanned, or emailed signature, or a copy of the same (including an electronic copy) may be used for any and all purposes for which the original signature may have been used.

**Online Approvals**

Online approval expedites obtaining required approvals for internal processes and can be established by contract with other parties.

Online approvals shall be accepted as valid when the online process requires authentication such as user name and password.

As appropriate, online approval systems should implement technologies in alignment with industry best practices including

secure data transmission standards, password expiration and complexity policies, etc.

**Revision Dates**

APSU Policy 4:018 (previously 1:019) - Rev.: March 25, 2017
APSU Policy 4:018 – Issued: November 18, 2015

**Subject Areas:**

| Academic | Finance | General | Human Resources | Information Technology | Student Affairs |
|---|---|---|---|---|---|
| | | ☑ | | ☑ | |

**Approved**

President: signature on file