TO: University Council

FROM: Karen Glover, Associate Vice President/Comptroller
Kay Lennon-McGrew, Assistant University Counsel

DATE: December 7, 2020

RE: Electronic Signature Policy

I. Introduction

The Electronic Signature Policy establishes when an electronic signature of a University employee may be utilized to bind the University in the course of conducting official business on behalf of the University. The initial public comment period for this policy began October 15, 2020 and concluded November 1, 2020. The policy was reviewed by University Council (UC) at the November 9, 2020. After discussion, the policy was referred to University Counsel's Office for a second legal review. Due to the nature of the changes suggested, the policy was posted again for public comment from November 16th to December 2nd.

II. Comments Received

Below is a summary of the comments and/or questions received during the second public comment period, as well as the applicable response from either the Originator or University Counsel's Office.

Comment from Sharon McGee: This policy is needed. People can buy and sell a home, sign income taxes, and other legal tasks through a secure electronic signature, and so it makes sense that ETSU would position itself to be able to sign electronically. This will keep official business moving smoothly.

Policy Originator's Response: N/A

Comment from Deborah Harley-McClaskey: I do not understand why the exceptions to financial transactions. I can invest funds with an electronic signature, deposit checks electronically, etc. Is this state law or local policy?

Policy Originator's Response: The policy addresses the receipt and acknowledgement of cash which would require in-person transactions. Per

discussion with internal audit, cash transactions would therefore require wet signatures.

Comment from Susan Epps: Noted in the version I sent to Karen and Kay earlier, the section below sounds like policy, not procedure (the formatting screws up when I copy/paste here)

1. Signatory Authority

Each person possessing the authority to sign documents on behalf of the University must have approval granting this authority and intent, describing the scope and limits of the signatory's authority.

All other changes were made - thank you!

Office of University Counsel's Response: The referenced section is not policy and is appropriate for the procedure section; no change was made after the requested legal review prompted by your recommendations during the UC meeting. We conducted an additional legal review and maintain this section is appropriate for procedure; in an effort to further alleviate your concern, a non-technical revision of the language to this section has been made to further clarify the procedure.

Comment from Janice Jones: The policy states "if approved electronic signature methods require the use of encryption technology that uses public or private key infrastructure and/or certificates, the Information Technology Services Department will be responsible for the administration of such public or private keys and certificates.". I recently had to receive approval from ITS for a two-factor authentication process for an electronic signature to incorporate with our Electronic Medical Record system. However, our EMR is hosted, and administration of the product is not completed through ITS. Will this be an issue based on the wording in the proposed policy?

Thanks for completing this policy. So needed!!!

Policy Originator's Response: The proposed policy would not affect the use of the Electronic Medical Record (ERM) system that has received approval from ITS.

III. Legal Review of the Proposed Policies

The Electronic Signature Policy complies with the Tennessee Uniform Electronic Transactions Act (T.C.A. § 47-10-101, et. seq), the Tennessee Public Records Act and the federal law related to Electronic Signatures in Global and National Commerce (15 U.S.C. § 7001, et seq.).

Use of Electronic Signatures	
Responsible Official: Chief Financial Officer for Business and Finance	Responsible Office: Business and Finance

Policy Purpose

The purpose of this policy is to establish when an electronic signature may replace a written signature to bind the University when conducting official business on behalf of the University.

Policy Statement

To the extent permitted by state and federal law, it is the policy of East Tennessee State University to recognize the validity of electronic signatures for contracts and other legally binding documents when an approved electronic signature method is utilized and each party has agreed to conduct transactions by electronic means.

I. Applicability and Scope.

A. This policy does not apply to internal administrative approval or acknowledgement processes or internal forms requiring departmental or supervisor approval, an employee's signature, or a student's consent for internal control purposes (e.g., internal routing forms, travel reimbursements, request forms, release of educational records, etc.).

B. Internal approval or acknowledgement processes that involve receipt of cash are not eligible for electronic signature.

C. This policy does not confer signature authority on any party.

II. Use of Electronic Signature.

A. Mutual Agreement by the Parties.

1. This policy applies to transactions where each party has agreed to conduct the transaction by electronic means. Whether the parties agree to conduct a transaction by electronic means is determined by the conduct of the parties and the context and circumstances surrounding the transaction.

2. This policy does not require the use of electronic or digital signatures. Electronic signatures may not be used when an applicable law, regulation, or University policy or process specifically requires a handwritten signature.

B. Signature Required by Law.

When a signature is required by law, that signature requirement is satisfied when the electronic record has associated with it an electronic signature using an approved electronic signature method.

C. Signatory Authority.

The signing of a record using an approved electronic signature method does not necessarily mean that the record has been signed by a person authorized to sign or approve that record.

Definitions

Approved Electronic Signature method	A method that has been approved in accordance with this policy and applicable state and federal laws. The inventory of approved electronic signature methods will specify the form of the electronic signature, the systems and procedures used with the electronic signature, and the significance of the use of the electronic signature, whenever possible.
Certificate	An electronic document used to identify an individual, server, a company, or some other entity and to associate that identity with a public key. A certificate provides generally recognized proof of an entity's identity.
Electronic	The technology having electrical, digital, magnetic, wireless, optical, electromagnetic, or similar capabilities.
Electronic signature	An electronic symbol, or process, attached to or logically associated with a record and executed or adopted by a person with the intent to sign the record. An electronic signature must be attributable (or traceable) to a person who has the intent to sign the record. Best practice for electronic signatures will include the use of adequate security and authentication measures that are contained in the method of capturing the electronic transaction. The recipient of the transaction must be able to permanently retain an electronic record of the transaction at the time of receipt.
Electronic transaction	A transaction conducted or performed, in whole or in part, by electronic means or electronic records.
Private key	An encryption/decryption key known only to the party or parties that exchange messages. In traditional private key cryptography, a key is shared by the parties so that each can encrypt and decrypt messages.

Public key	A value provided by some designated authority as a key that, combined with a "private key" derived from the public key, can be used to effectively encrypt messages and digital signatures.
Public-key infrastructure (PKI)	A form of information encryption that uses certificates to prevent individuals from impersonating those who are authorized to electronically sign an electronic document.

Authority

T.C.A. § 47-10-101, et.seq. – Tennessee Uniform Electronic Transactions Act
T.C.A. § 10-7-101, et.seq. – Tennessee Public Records Act
15 U.S.C. § 7001, et seq. - Electronic Signatures in Global and National Commerce

Policy History

Effective Date:

Revision Date:

Previous policy for reference: https://www.etsu.edu/bf/documents/fp/39.pdf

Procedure (s)

I. Signatory Authority.

A. Each person shall verify that they possess the requisite authority to sign documents on behalf of the University prior to signing documents electronically

B. Information Technology Services Department will inventory these approvals and verify the inventory yearly. This inventory will be provided to any University employee upon request to verify they are authorized to sign on behalf of the University and for what purpose.

II. Electronic Record.

A. If parties have agreed to conduct a transaction by electronic means and a law requires a person to provide, send, or deliver a signed document to another person, the requirement is satisfied if the information is provided, sent, or delivered in an electronic record capable of retention by the recipient at the time of receipt.

B. An electronic record is not capable of retention by the recipient if the sender or its information processing system inhibits the ability of the recipient to permanently retain the electronic record containing the signature.

III. Approval of Electronic Signature Methods.

A. In determining whether to approve an electronic signature method, consideration will be given to the systems and procedures associated with using that electronic signature, and whether the use of the electronic signature is at least as reliable as the existing method being used.

B. An inventory of all approved electronic signature methods shall be maintained by Information Technology Services Department. The inventory of approved electronic signature methods will be maintained and amended only after a review of the electronic signature method by the Information Technology Services Department in consultation with the Office of University Counsel.

C. If approved electronic signature methods require the use of encryption technology that uses public or private key infrastructure and/or certificates, the Information Technology Services Department will be responsible for the administration of such public or private keys and certificates.

D. In the event that it is determined that an approved electronic signature method is no longer trustworthy, the Information Technology Services Department in consultation with the Office of University Counsel shall consider removing the method from the inventory of approved electronic signature methods. If there is an on-going need for electronic signatures to continue by a previously approved but since revoked method, the Information Technology Services Department in consultation with the Office of University Counsel may permit such signatures to be accepted until such time as steps have been completed to ensure appropriate electronic signatures are obtained by an approved electronic signature method.

IV. Non-Legal Internal Processes.

Internal administrative or acknowledgement approvals may be obtained by electronic or digital means if departments adopt processes to ensure they maintain appropriate documentation of the approvals and ensure that any system or process utilized for an electronic signature does not result in institutional data being shared or stored inappropriately without proper safeguards.

V. Sanctions.

Any individual who makes inappropriate or illegal use of electronic signatures and/or records is subject to sanctions up to and including dismissal, suspension, and criminal prosecution.

Procedure History
Effective Date: Revision Date:

Related Form(s)