



Policy Number: AC048

Revised Date: January 22, 2024

Rick Evans, Executive Director

Title: Electronic & Digital Signature Policy

Statement:

TUC employees may use electronic and digital signatures to conduct many transactions that traditionally used handwritten signatures and approvals on paper documents. This policy allows TUC employees to conduct transactions, accept approvals by other parties, and sign agreements on TUC's behalf by using electronic means.

This procedure does not change any signature policy requirements or limitations as to which employees are authorized to approve expenditures or enter into contracts (TUC Policy AC033). This policy is not intended to replace all wet signature requirements.

This procedure was developed to be consistent with CSU Information Security Policy and Standards, section F, ISO Domain 10: Cryptography Policy.

Purpose:

To provide The University Corporation (TUC), with a procedure that identifies the permissible types of electronic and digital signatures and the requirements for their use. It permits the use of electronic transactions and the electronic version of supporting documentation in conducting business operations at The University Corporation (TUC).

Electronic Signature and Acceptable Forms

An electronic signature (e-signature) is an:

- **electronic sound** (e.g., audio files of a person's voice)
- **symbol** (e.g., a graphic representation of a person in JPEG file)
- **process** (e.g., a procedure that conveys assent)

...attached to or logically associated with a record, and executed or adopted by a person with the intent to sign the record. Electronic signatures may be used for internal and external forms, legal documents, and contracts where permitted.

Electronic signatures convey the intent of an individual to sign and are often easier to implement, but usually cannot provide satisfactory assurance if authentication, non-repudiation, and integrity are legally required.

Below are acceptable forms of electronic signature:

1) Electronic Forms

The selection of an option (e.g. tick box or button) on an electronic form to indicate agreement can be used as replacement for written signatures when the appropriate functional requirements are met and system safeguards and technology used recorded:

- Intent of agreement
- Information that clearly identifies (e.g. by recording the login username) the individual who has signed the agreement
- Within an auditable trail that the form was signed

Furthermore, the signatory's identity must be accessible for the length of the retention period required for the form. The technology used should also restrict the form once 'signed' such that the contents of the form cannot be changed without the signature being invalidated.

2) Scanned Image of a Handwritten Signature

A scanned image of a handwritten signature can be used as an equivalent to a written signature when the appropriate security requirements have been met. Scanned images of a signature must only be used where express permission has been granted by the author and is considered acceptable for high volume processes such as mass mailings. Given the ease with which images may be manipulated, images without other forms of authenticity should be used for low-risk transactions only.

3) Authorization by Email

Acceptance or agreement of intent through an official, controlled email system may be used when the appropriate functional requirements, risk, and security have been considered.

Given the ease with which emails can be manipulated, email receipts without other forms of authenticity should only be used for low-risk transactions.

Email receipts may not be accepted from "generic or shared" email accounts unless the appropriate controls, (e.g. phone verification) are in place to establish the actual sender.

Digital Signature Use and Requirements

A digital signature is a specific type of electronic signature that uses cryptographic transformation of data to provide authenticity, message integrity, and non-repudiation. It is a digital signature is an electronic identifier, created by computer, intended by the party using it to have the same force and effect as the use of a handwritten signature. A digital signature can be affixed to any written communication in which a signature is required.

Digital signatures must be used instead of a simple electronic signature when legally required or when greater risk exists. The appropriateness of a simple electronic signature vs. a digital signature must be based on the level of risk. A higher assurance level signature may be required for legal enforceability.

To affix a digital signature or scramble electronic content, a signatory must obtain a digital signature from an accepted authority, which typically consists of an electronic asymmetric key-pair (includes a private (secret) key and publicly distributable key). For a digital signature to be considered valid, it must be:

- Unique to the person using it;
- Capable of verification;
- Under the sole control of the person using it;
- Linked to data in such a manner that if the data is changed, the digital signature is invalidated (and where appropriate and necessary, removed).
- In conformity with Title 2, Division 7, Chapter 10, of the California Code of Regulations

Valid documents signed with a digital signature must include a clear and unambiguous email trail/chain of approval of all those required to sign that document.

Each approval must be clear and unequivocal. It must be clear that each approver has approved the same document and that document is attached.

Acceptable Type of Signatures for TUC Transactions

Transactions that formerly required original (or “wet”) signatures may be processed using electronic and digital signatures. TUC may exercise discretion to conduct a transaction on paper or in non-electronic form.

The choice to use electronic and digital signatures does not affect the obligation to have documents be provided or made available on paper when required by applicable policies, laws or regulations. The use of electronic and digital signatures in lieu of original signatures should be implemented in a consistent manner. A combination of handwritten and electronic and / or digital signatures is acceptable for the same transaction.

Electronic Supporting Documentation

TUC may accept supporting documentation (invoices, receipts, delivery notes, etc.) that is required to support or substantiate an expenditure request (Purchase Order, Check Request, etc.) in electronic form.

Documents processed via electronic means must be processed completely, including all supporting documentation. Processing of partial documents (e.g. signature page only) or without all related supporting documentation is not permissible.

Exceptions

This procedure is not applicable when explicitly prohibited by policies, laws or regulations. Electronic and digital signature on transactions containing Level 1 or Level 2 data is strictly forbidden unless the system used is designed to secure the transmission and storage of such data.