



ADMINISTRATIVE POLICIES

Office of the City Manager

Policy Number CM-22
Version 1
Effective Date 10/8/2024
Responsible Department City Manager

TITLE: Electronic Signature Use

- New
 Supersedes

APPROVAL

Marc Mondell
Marc Mondell (Oct 8, 2024 11:03 PDT)

10/8/24

City Manager Signature

Date Approved

- PURPOSE.** The purpose of this policy is to permit the City of Tulare (“City”) to use electronic signatures in lieu of manual signatures, when permitted by law. This policy will increase productivity and ensure convenient and timely access to City information by using electronic signature technology to collect and preserve documents quickly, securely, and efficiently. In addition, the use of electronic signatures will promote and advance the creation of paperless processes and thereby reduce the consumption and storage of paper documents.
- SCOPE.** This policy is applicable to all City employees who utilize electronic signatures in the course of conducting City business. It covers the creation, use, and management of digital signatures for official documents and transactions.

This policy applies to documents requiring a signature of any person where the signature is intended to show authorship, approval, authorization, or certification, as allowed by law. It is the policy of the City to encourage the use of electronic signatures in all internal and external activities, documents, and transactions where it is operationally feasible to do so, where existing technology permits, and where it is otherwise appropriate based on the department’s preference. In such situations, affixing an electronic signature to the document in a manner consistent with this policy shall satisfy the City’s requirements for signing a document.

While the use of digital signatures is suggested and encouraged, this policy does not require any department to use digital signatures, nor can the City mandate that any third party signing a document use digital signature. The parties to a transaction must agree to conduct the transaction by electronic means using a signature method that complies with applicable laws and regulations, including the capability of all parties to retain and accurately reproduce the electronically signed document or record. This policy permits a mix of handwritten and electronic signatures on a single document so long as all parties agree.

3. DEFINITIONS.

- 3.1. Digital Signature. As defined by California Government Code Section 16.5, an electronic identifier, created by computer, intended by the party using it to have the same force and effect as the use of a manual signature so long as it embodies the following attributes:
- It is unique to the person using it;
 - It is capable of verification;
 - It is under the sole control of the person using it;
 - It is linked to data in such a manner that if the data are changed, the digital signature is invalidated; and
 - It conforms to regulations adopted by the California Secretary of State.
- 3.2. Electronic. Relating to technology having electrical, digital, magnetic, wireless, optical, electromagnetic, or similar capabilities (see Civil Code Section 1633.2).
- 3.3. Electronic Record. A record that is created, generated, transmitted, communicated, or stored using electronic means.
- 3.4. Electronic Signature or eSignature. An electronic sound, symbol, or process attached to or logically associated with an electronic record and executed or adopted by a person with the intent to sign the electronic record. For purposes of this title, a “digital signature” as defined in subdivision (d) of Section 16.5 of the Government Code is a type of electronic signature with stricter security requirements.
- 3.5. Manual Signature. An original wet signature applied to a document.
- 3.6. Proxy Signature. When Person A authorizes Person B to sign Person A’s signature on their behalf. As e-mails can’t be forwarded in electronic signature software platforms, when signature authority has been granted from Person A to Person B, the document should be sent to Person B for signature with a copy of the Signature Authority attached to the electronic document. Proxy signatures are prohibited under this policy.
- 3.7. Record. Information that is inscribed on a tangible medium, or that is stored in an electronic or other medium and is retrievable in perceivable form (see Civil Code Section 1633.2).

4. POLICY.

- 4.1. Legal Authority. This policy authorizes the City to accept and use electronic signatures in lieu of manual signatures in compliance with the following legal requirements.

In 1995, the California Legislature enacted AB 1577 which, among other things, added Government Code Section 16.5 authorizing public entities to accept digital signatures if they comply with stringent verification requirements.

In 1999, California adopted a version of the Uniform Electronic Transactions Act (UEAT) (California Civil Code Sections 1633.1 to 1633.17) providing that electronic signatures would have the same legal effect as a wet or manual signature.

In 2000, the Federal Government enacted the Electronic Signatures in Global and National Commerce Act (ESIGN) (15 USC Section 7001 et seq.) which mandated the same treatment of electronic signatures in interstate or foreign commerce.

In 2016, the California Legislature enacted AB 2296, clarifying that a digital signature may be used to satisfy the requirements of an electronic signature under UETA. An electronic signature includes a digital signature under Government Code Section 16.5 and a digital signature under those provisions is a type of an electronic signature as set forth in the UETA. The bill also revised Government Code Section 16.5 by specifying that if a public entity elects to use a digital signature that meets specified requirements, the digital signature has the same force and effect of a manual signature in any communication with the public entity.

4.2. Acceptable Technologies. For a digital signature to be valid for use by a public entity, it must be created by a technology that is acceptable for use by the State of California and able of creating signatures that conform to the requirements of Government Code Section 16.5 (2 Cal. Code Regs. Section 22005). Public entities may utilize digital signatures that are created by one of two different technologies:

- Public Key Cryptography (PKC) occurs when a signer electronically signs a document, as the signature is created using the signer's private key, resulting in the signature being marked with the time that the document was signed. PKC signatures have a greater degree of verifiability signature dynamics signatures, are designed to be immediately verifiable, and are affixed to documents using software enhancements to existing applications and web browsers.
- Signature Dynamics signatures require additional steps (including handwriting analysis) to verify the document's signer and are designed to allow future verification of the signature (similar to a non-notarized, paper-based signature), but do not provide the level of security that is inherent in PKC signatures.

Adobe Acrobat Sign, DocuSign, and GMO GlobalSign, Inc. are three providers that offer digital signature services backed by PKC technology with digital certificates providing proof of identity.

4.3. Security Requirements and Approved Uses. Security requirements for electronic signatures range from simple to complex, depending on the transaction. A digital signature (a subset of electronic signature with stricter security requirements) is intended by the party using it to have the same force and effect as a manual signature and must meet certain attributes; therefore, certain types of documents require a digital signature under this policy, whereas others allow use of electronic signatures (including a digital signature). Below are examples of documents for which electronic and digital signatures are approved.

- 4.3.1. Approved Uses for Electronic Signature. Under this policy, the use of an electronic signature is allowed on a variety of documents, to the extent permitted by law. This includes but is not limited to:
- Contracts, Agreements, Memorandums of Understanding, Change Orders, and Task Orders
 - Internal Memos and Correspondence
 - Human Resource or Employee Forms
 - Certificates
 - Permits and Applications
 - Internal Financial Approvals
 - Oaths of Office
 - Record Destruction Requests
 - Most City-generated forms used to verify, authorize, submit, or request information.
 - The City also requires that various internal transactions be approved by an employee, supervisor, division manager, department head, or other City staff, and these approvals may be signified by electronic signature.
- 4.3.2. Documents Requiring a Digital Signature. The following list of documents require a digital signature, if signed electronically in accordance with this policy. The use of any other type of electronic signature is not permitted for the following:
- Brown Act Body Minutes, Resolutions, Ordinances
 - FPPC Reports, Statements, Forms or other documents filed under the Political Reform Act and filed with the City. (FPPC reg. 18104)
 - Grant Documents
 - Waivers (limited to City events, recreation classes, and camps; waiver should be reviewed by the City Attorney and Risk Management prior to distributing it for signature)
- 4.3.3. Prohibited Uses of Electronic or Digital Signature. The following is a list of prohibited uses of electronic signatures (including digital signatures) under this policy:
- Documents or transactions that require a wet signature to be notarized or acknowledged or recorded by the County Recorder, including but not limited to subdivision maps, deed, and regulatory agreements.
 - Documents or transactions that require a wet signature, including but not limited to transfers of interests in real property and banking- and securities-related documents or transactions.
 - Documents or transactions that are not signed using approved electronic signature technologies.
 - Bonds
 - Initiative, Referendum, or Recall Petitions

- Any other document required by law to contain a manual signature.

4.4. Responsibilities.

- 4.4.1. The City Manager, in consultation with the City Attorney, shall have the authority to develop administrative policies and procedures to the extent necessary to implement the terms of this policy.
- 4.4.2. The City Manager, in consultation with the City Attorney, shall further determine the documents for which the City will accept electronic signatures. Periodic reviews will be implemented for appropriateness and continued applicability of electronic signatures.
- 4.4.3. Each department within the City has discretion to decide whether to permit the use of electronic signatures. Departments will work with the City Clerk and City Attorney to determine where applicable laws permit a digital signature to be used. In addition, each department that opts to use digital signatures must adopt or amend their business practices to support the requirements of this policy. Additionally, departments utilizing electronic signatures shall develop procedures for use of electronic signatures within their department processes.
- 4.4.4. The City Manager has the discretion to accept or authorize the acceptance of an electronic signature when, in consultation with the City Attorney as necessary, the circumstances surrounding the transaction address authentication and security concerns and electronic signatures are not otherwise prohibited by applicable law.
- 4.4.5. Staff initiating agreements must ensure that all parties agree to conduct the transaction by electronic means when using electronic signatures. Contracts signed by electronic signatures should specifically state that the parties to the contract agree to execution by electronic means.
- 4.4.6. All City users of electronic signature technology shall conform to the rules set forth in this policy.
- 4.5. Digital Solution Providers. The Information Technology division will be responsible to determine acceptable technologies and digital providers consistent with current State legal requirements and industry best practices to ensure the security and integrity of data and the digital signature.
- 4.6. Signing Authority Limited to City's Purchasing Policy. Signing authority should be in accordance with the City's purchasing limits as outlined in the City's adopted purchasing policy.
- 4.7. Storing and Archiving of Electronically Signed Documents. If a document exists only electronically, steps should be taken by each department to ensure that a fixed version of the final document is stored in an appropriate location, dependent upon the type of

document. All permanent records should be maintained in the City's trusted system (Laserfiche) while all other records should be maintained in a shared location on the City's network. The department should work with the City Clerk in developing an electronic filing system in a manner that is consistent with the City's Records and Information Management Program Policy, retention schedule, and applicable laws. Records should be sent to the Office of Record for proper storage (refer to the City's retention schedule). Contact the City Clerk's Office for assistance.

4.8. Implementation. To begin using electronic signatures, the following criteria should be followed:

4.8.1. The department head provides authorization to their staff.

4.8.2. Staff's signature authorization aligns with the City's purchasing policy.

4.8.3. If needed, the department head or authorized employee will notify IT Help Desk at helpdesk@tulare.ca.gov to request an approved electronic signature provider license. The IT Help Desk ticket must include the selected provider, authorization to use electronic signature, and whether or not training materials are needed.

5. REVISION HISTORY.

<u>Version #</u>	<u>Date</u>	<u>Reviewed/Approved By</u>
1	10/8/2024	Executive Team; City Manager