
 <b>City of Santa Ana Administrative Policies and Procedures</b>	 <b>City Manager's Authorization</b>	
	<b>Subject</b> <b>ELECTRONIC SIGNATURE POLICY</b>	<b>Date</b> 10/20/2020
		<b>Number</b> IT03

## 1. Purpose

The purpose of this Electronic Signature Policy ("Policy") is intended to broadly permit the use of electronic signatures. Incorporating electronic signatures into citywide processes will be beneficial internally and externally by increasing the efficiency of service delivery. Using electronic signatures for documents such as permits, plan approvals and contract executions will be more effective and provide a more user-friendly customer experience expected by our customers.

## 2. Scope and Applicability

This Policy enables the City of Santa Ana ("City") to accept an electronic signature, in lieu of a handwritten signature, on a document in which a signature is required or used, which complies with all applicable legal requirements. This Policy shall not supersede laws specifically requiring a written signature, and/or limit the right to conduct a transaction on paper or non-electronic form, and/or the right to have documents provided or made available on paper. It does not increase the scope of authority of the City's authorized signatories, but rather provides an alternative and efficient means to execute City-related documents.

This Policy defines the types of signatures available for use, provides the legal authority for use of electronic signatures, and establishes guidelines for the adoption of electronic signatures, including defining the circumstances under which the City may use and accept electronic signatures.

Electronic signatures may be authorized for a variety of documents utilized by the City, including both internal forms processed by City employees and external submissions from the public. As with any contract, the City must consider the type of transaction, and put measures in place that strike the right balance between ease of use and evidence of the intent to sign the record and agree to the terms.

### 2.1 Internal Forms:

Internal forms are submitted and processed by employees, whose identity the City already knows. Accordingly, the City can use a password scheme to tie the employee to the document being signed or submitted, so long as that employee is the only one who has access to sign or submit in their name, and that the document cannot be modified after the fact by anyone else.

### 2.2 External Submissions:

There are many different types of external submissions to the City that could be processed through electronic forms or applications, including, but not limited to, submissions of claims or applications for business licenses, building permits, or library cards. Conventions created that help establish intent for signatures on such forms include replicating the manual signing process (entering the signer's name on a signature line in a record), or utilizing clickwrap (placing language in immediate proximity to a checkbox or "I Agree" button informing the signer that by taking the requested action the signer is creating an electronic signature).

The evidence of consent created by clickwrap will typically be a record of the time and date that the party took action, their IP address and whatever information they provided in connection with accepting the terms. The City could require a party to click a box that is clearly marked as being part of forming an agreement, or provide notice language before a "Submit" button that lets a party know that by continuing, the party is agreeing to the linked legal terms. The type of click box or submit button and consent terms would need to be specially drafted by the City for each specific form or application, but sample clickwrap language includes the following:

- 2.2.1 "By clicking "Submit", you agree to the City's Terms and Conditions, and that you have read the City's Privacy Policy."
- 2.2.2 "Check here to indicate that you have read and agree to the Terms of the Agreement."
- 2.2.3 "By tapping to continue, you are indicating that you have read the Privacy Policy and agree to the Terms of the Agreement."
- 2.2.4 There are a number of different ways to request that parties agree to terms electronically. However, the clearer the required action, the more effective the consent will be.

### 3 Legal Authority

- 3.1 In 1995, in order to promote e-commerce and digital transactions with public agencies, California enacted *Government Code* section 16.5, which authorizes use of "digital signatures" in any written communication with a public agency in which a signature is required or used, provided that they conform with stringent verification procedures established by the Secretary of State.
- 3.2 In 1999, California enacted the Uniform Electronic Transactions Act ("UETA"), *Civil Code sections* 1633.1, et seq., which provides that an "electronic signature" is valid and enforceable under any law that requires a signature in any transaction between two or more persons, including a government agency. Under the UETA, "if a law requires a signature, an electronic signature satisfies the law," thereby guaranteeing that electronic signatures have the same legal effect as a "wet" or manual signature. The parties must have agreed to conduct the transaction by electronic means.

Whether the parties agree to conduct a transaction electronically is determined from the context and surrounding circumstances, including the parties' conduct.

- 3.3 In 2000, the federal government enacted the Electronic Signatures in Global and National Commerce Act (ESIGN), which gave electronic and digital signatures the same legal standing as handwritten signatures. ESIGN preserves the right of a party to use or accept handwritten signatures even if the documentation in questions is electronic. However, it is up to each organization to create its own policy around signatures. Normally a federal law would override a state law, but ESIGN expressly allows preemption by state law.
- 3.4 In 2016, California adopted AB 2296 to clarify that a digital signature authorized by *Government Code* section 16.5 and subject to regulations adopted by the Secretary of State, is one type of electronic signature that a public agency may choose to utilize under UETA. *Government Code* section 16.5(a) further provides that a "digital signature shall have the same force and effect as the use of a manual signature if and only if it embodies all of the following attributes:
  - 3.4.1 It is unique to the person using it.
  - 3.4.2 It is capable of verification.
  - 3.4.3 It is under the sole control of the person using it.
  - 3.4.4 It is linked to data in such a manner that if the data are changed, the digital signature is invalidated.
  - 3.4.5 It conforms to regulations adopted by the Secretary of State."
- 3.5 *Government Code* section 16.5 also states that the use or acceptance of a digital signature is at the option of the parties to the transaction and nothing in the law requires a public entity to use or accept the submission of a document containing a digital signature.
- 3.6 As required by *Government Code* section 16.5, the California Secretary of State has enacted regulations for the use of digital signatures. Notably, pursuant to section 22001 of these regulations, 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. In order to determine if a technology is accepted by the State of California, section 22003(a)(6) requires the California Secretary of State to maintain an "Approved List of Certification Authorities" authorized to issue certificates for digitally signed communication with public entities in California. Currently, there are five entities on the list, but the list is regularly updated by the Secretary of State. Accordingly, public entities shall only accept certificates from Certification Authorities that appear on the "Approved List of Certification Authorities" authorized to issue certificates by the California Secretary of State.

## 4 Policy

The guidelines listed below in this section are intended to enable the City to use electronic signatures, including digital signatures when applicable, to the fullest extent allowed by law, and should not limit the City's ability to use electronic signatures, including digital signatures, in any way:

- 4.1 To the fullest extent permitted by law, the City shall accept all forms of electronic signatures, including digital signatures, which comply with applicable laws, as legally binding and equivalent to handwritten signatures, for any record or document in which a signature is used or required by a City policy, or legal requirement beyond a City policy.
- 4.2 In many or most cases, the circumstances of the transaction (e.g., ordinary vendor contract) will permit the use of an electronic signature as defined above. However, there may be exceptions warranting the use of a digital signature where a higher level of signature verification and security is necessary. Any exceptions to the general rule allowing electronic signatures for records or documents, including any specific requirement for handwritten signatures or digital signatures, shall be determined by the City Manager, and a complete list of said exceptions shall be maintained by the Clerk of the Council.
- 4.3 This Policy shall apply to all employees of the City, and governs all uses of electronic signatures used to conduct the official business of the City. Such business may include, but not be limited to, electronic communications, transactions, contracts, permits and other official purposes, both internal and external to the City.
- 4.4 The City's right or option to conduct a transaction on paper, or in non-electronic form, shall not affect the City's right, option or obligation to have documents provided or made available in paper format.
- 4.5 If the parties have agreed to conduct a transaction by electronic means, the parties are required to utilize all applicable security processes for authentication.
- 4.6 No party to a contract or other document may be forced to accept an electronic signature. Rather, each party shall be permitted to decide if a document will be signed in hardcopy format.
- 4.7 When a document is electronically signed by all parties, the City will provide a copy of the electronically-signed document to the other parties in an electronic format that is capable of being retained and printed by the other parties.
- 4.8 This Policy shall not supersede laws that specifically require a handwritten signature.

- 4.9 This Policy shall not apply to any transaction that requires a person's signature to be signed in the presence of a notary public.
- 4.10 The final approval of any electronic signature technologies and vendors will be by the City Manager, with recommendation from the Clerk of the Council, the Chief Technology Innovations Officer, and the City Attorney. In determining whether to approve electronic signature technologies or vendors, consideration will be given to the systems and procedures associated with using that electronic signature, industry best practices, and whether the use of the electronic signature is at least as reliable as the existing method being used, in order to ensure the security and integrity of the data and the signature.
- 4.11 The Chief Technology Innovations Officer shall conduct periodic reviews for appropriateness and continued applicability of electronic signatures technologies and vendors.
- 4.12 If it is determined that an approved electronic signature technology or vendor is no longer trustworthy, the City Manager must revoke the approval of the electronic signature method. If there is continued significance for the electronic signatures, which used the revoked technology or vendor, the Clerk of the Council shall take steps to see that any valid records signed with the revoked electronic signature method are signed again either with a written signature or with an approved electronic signature method.
- 4.13 Any record or document requiring the additional security of a digital signature must comply with the requirement of *Government Code* section 16.5 and the Secretary of State guidelines, including the use of certificates from Certification Authorities that appear on the "Approved List of Certification Authorities" authorized to issue certificates by the California Secretary of State.
- 4.14 The Chief Technology Innovations Officer shall be responsible for determining acceptable technologies and digital signature certification providers consistent with current legal requirements and industry best practices to ensure the security and integrity of the data and the digital signature.
- 4.15 All use of electronic signatures, including digital signatures, by the City shall be in accordance with this Policy, as may be designated and amended from time to time by the City Manager.
- 4.16 Any use of electronic signatures, including digital signatures, by the City that is not in accordance with this Policy, or any unauthorized signing of any record or document, shall render such record or document invalid as not fully and properly executed by the City or party signing the document.

## 5 Consent Clause

Any record or document allowing the use of electronic signatures should include one of the below consent clauses.

- 5.1 “By signing this document, you are agreeing that you have reviewed this disclosure information and consent to transact business using electronic communications, to receive notices and disclosures electronically, and to utilize electronic signatures in lieu of using paper documents. You are not required to receive notices and disclosures or sign documents electronically. If you prefer not to do so, you may request to receive paper copies and withdraw your consent at any time.”
- 5.2 “By selecting the "I Accept" button, you are signing this Agreement electronically. You agree your electronic signature is the legal equivalent of your manual signature on this Agreement. By selecting "I Accept" you consent to be legally bound by this Agreement's terms and conditions. You further agree that your use of a key pad, mouse or other device to select an item, button, icon or similar act/action, or in accessing or making any transaction regarding any agreement, acknowledgement, consent terms, disclosures or conditions constitutes your signature (hereafter referred to as "e-signature"), acceptance and agreement as if actually signed by you in writing. You also agree that no certification authority or other third party verification is necessary to validate your e-signature and that the lack of such certification or third party verification will not in any way affect the enforceability of your e-signature or any resulting contract between you and the City. You also represent that you are authorized to enter into this Agreement for all persons who own or are authorized to access any of your accounts and that such persons will be bound by the terms of this Agreement. You further agree that each use of your e-signature in obtaining a City service constitutes your agreement to be bound by the terms and conditions of the City.”