

TOWN OF APEX
ELECTRONIC SIGNATURE POLICY
MARCH 5, 2019

BE IT RESOLVED by the Town Council of the Town of Apex that the following policies apply to the use of digital, digitized, facsimile, and electronic signatures on Town contracts or purchase orders.

1. INTRODUCTION

1.1 Purpose

The purpose of this Policy is to authorize the use of electronic signatures on Town contracts while allowing the Town to balance the need for flexibility with the need for signature security and integrity. Electronic signatures reduce the amount of paper and time as well as cost associated with exchanging, transmitting, submitting and approving physical documents while also providing an audit trail indicating when documents were signed and/or modified.

1.2 Scope

This Policy:

1. Establishes that electronic signatures shall be effective on Town contracts as long as guidelines in this policy regarding security and integrity are followed; and
2. Establishes standards for acceptance of different forms of electronic signatures; and
3. Authorizes the Town Manager, or his designee, to determine the particular technology, software, and vendors that will satisfy the above referenced guidelines.

1.3 Legal Framework

In 1998 the North Carolina legislature passed the Electronic Commerce Act (Chapter 66, Article 11A) to facilitate “electronic commerce with public agencies and regulate the application of electronic signatures when used in commerce with public agencies.” In 2000, North Carolina enacted the Uniform Electronic Transactions Act (UETA) which provides in part “...if a law requires a signature, an electronic signature satisfies the law provided it complies with the provisions of this Article.” N.C.G.S §66-58.4 authorizes public agencies to use and accept electronic signatures pursuant to either Article 11 or Article 40 (UETA) of Chapter 66 of the NC General Statutes. On June 30, 2000 the United States Congress passed the Electronic Signatures in Global and National Commerce Act (E-SIGN) which established that a contract or signature “may not be denied legal effect, validity, or enforceability solely because it is in electronic form” which guarantees on the federal level that electronic signatures will have the same legal effect as a manual or “wet” signature.

2. DEFINITIONS

Authentication – The process of verifying that a document is genuine or original or in the case of electronic documents, it is the process of confirming a user's identity.

Contract - An agreement between two parties creating legally enforceable obligations to include service contracts, design contracts, certain construction contracts, purchase contracts, interlocal agreements, purchase orders, reimbursement agreements, and memorandums of understanding. This does not include notices of cancellation or termination of utility services, notices of default, or notices of civil penalties. The definition of contract as applied to this Policy also does **NOT** include bonds, deeds, easements, encroachment agreements, or any contract that is required to be formally bid in accordance with Chapter 143 of the North Carolina General Statutes.

Digital Signature – A string of electronic data that is embedded in an electronic document for the purposes of verifying document integrity and signer identity.¹ A digital signature uses public key infrastructure technology to protect the document from tampering and creates a date/time stamp. A digital signature is a type of electronic signature.

Digitized Signature – A scanned image of a manual or “wet” signature. For the purposes of this Policy, digitized signatures shall be considered electronic signatures.

Electronic Record – A record created, generated, sent, communicated, received, or stored by electronic means.²

Electronic Signature - An electronic sound, 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.³

Metadata – Structured information that describes, explains, and/or locates an electronic file and can determine who created the document and where it originated.⁴

Security Procedure – A procedure employed for the purpose of verifying that an electronic signature, record, or performance is that of a specific person or for detecting changes or errors in the information in an electronic record. The term includes a procedure that requires the use of algorithms or other codes, identifying words or numbers, encryption, or callback or other acknowledgment procedures.⁵

¹“Digital Signature Policy Guidelines Version 1.1.” Office of State Controller, and the North Carolina Department of the Secretary of State, and North Carolina Department of Cultural Resources, Division of Archives and Records, March 2014.

²Uniform Electronic Transactions Act – N.C.G.S. Chp. 66, Art. 40.

³ESIGN, 15 U.S.C. chp. 96

⁴Metadata as a Public Record in North Carolina: Best Practices Guidelines for Its Retention and Disposition.” North Carolina Dept. of Cultural Resources, Nov. 2010, Metadata Guidelines.

⁵ Uniform Electronic Transactions Act – N.C.G.S. Chp. 66, Art. 40.

3. SECURITY PROCEDURE

The use of an electronic signature shall have the same force and effect of a manual signature if all of the following conditions are satisfied:

1. The signature is capable of verification.
2. The signature is under the total and sole control of the individual using it.
3. The parties to the agreement consent to the use of electronic signatures.
4. The signature is linked to the data in a manner that is readily ascertainable if the data is changed after the signature is applied.

The Town Manager or his designee shall determine acceptable technologies and vendors under this Policy that are consistent with industry best practices and North Carolina state law to ensure the security and integrity of the data and signature.

3.1 Digital Signature

Digital Signatures from vendors, contractors, and other third parties shall utilize public-key infrastructure cryptography to ensure the validity of submitted documents. Any digital signature software provider must use either a Digital Signature Algorithm, a Reversible Digital Signature algorithm (RSA), or an Elliptic Curve Digital Signature Algorithm as approved by the National Institute of Standards and Technology. Any other software utilizing an alternative authentication method must be approved by the Town Manager or his designee. The above requirements of this section shall not apply to Town staff signatures which shall either be manual ("wet"), digitized, or be applied using software that meets the requirements of UETA, is approved by the Town's Director of Information Technology, and is capable of retaining the following metadata: Date; File name; Name of Signatories; Time Stamp. Digital signatures by Town staff shall be exclusive to individual staff member accounts.

3.2 Digitized Signature

Digitized Signatures may be accepted by the Town, and applied by Town staff, when the following conditions are met:

1. The digitized signature must be authorized by the signing party and its appearance should be consistent with the signatory's usual style and format.
2. The digitized signature must be kept as a TIF, PDF file, or other format approved by the Director of Information Technology.
3. Both parties to the contract agree to accept digitized signatures.

3.3 Agreement of Parties

The parties to any contract governed by this Policy shall agree to conduct the transaction with electronic or digitized signatures as determined by the language of the contract, the context and surrounding circumstances and the parties' conduct.

4. ELECTRONIC RECORDS MANAGEMENT

4.1 Associated Metadata

Town will only utilize vendor software systems capable of maintaining the following metadata files:

- Date
- Title/file name
- Name of Signatories
- Time Stamp
- Custom tags

The software system shall also be capable of generating a summary report of the metadata that includes, but is not necessarily limited to, a certificate of completion, record tracking, and IP addresses, as well as any other data that can aid in authenticating the document.

4.2 Record Retention

All records retention and public records law applicable to government records in hard copy format apply equally to electronic records. All electronic records signed electronically shall be maintained in accordance with the Town of Apex Electronic Records & Imaging Policies & Procedures. Automatic retention and disposition features shall not be used unless first approved by the Town's Director of Information Technology.

5. E-NOTARIZATION

Electronic notarizations must meet the requirements for electronic signatures provided by the UETA as well as this policy as well as any other applicable laws. The notarization must be performed in accordance with North Carolina's Electronic Notary Act (Chp. 10B, Article 2, N.C.G.S.) as well as the North Carolina Electronic Notary Administrative Rules.

6. PREAUDIT STATEMENT

The Town Council has provided that the Town's Finance Director may sign the preaudit certificate on contracts or purchase orders through the use of facsimile signature machines, a signature stamp, or similar device in accordance with N.C.G.S. §159-28.1.