FORT BEND COUNTY

FORT BEND COUNTY ELECTRONIC AND DIGITAL SIGNATURE POLICY

FORT BEND COUNTY COMMISSIONERS COURT

COUNTY JUDGE
KP GEORGE

COUNTY COMMISSIONERS
VINCENT MORALES JR., PRECINCT 1
JAMES "GRADY" PRESTAGE, PRECINCT 2
W. A. "ANDY" MEYERS, PRECINCT 3
KEN DEMERCHANT, PRECINCT 4

ADOPTED JUNE 11, 2019

FORT BEND COUNTY ELECTRONIC AND DIGITAL SIGNATURE POLICY

On June 11, 2019 the Commissioners Court of Fort Bend County, Texas, met in regular session with the following members present and participating to-wit:

KP George	County Judge, Presiding
Vincent Morales, Jr.	Commissioner, Precinct 1
Grady Prestage	Commissioner, Precinct 2
W. A. "Andy" Meyers	Commissioner, Precinct 3
Ken DeMerchant	Commissioner, Precinct 4

WHEREAS, during such session, the Court considered adoption of the following Policy to authorize Fort Bend County officials and employees to conduct internal and external business using electronic signatures in accordance with the Uniform Electronic Transaction Act, Tex. Bus. & Com. Code Ann. §§ 322.001, et. seq.

NOW THEREFORE, BE IT ORDERED by the Commissioners Court of Fort Bend County, Texas as follows:

Table of Contents

1. Policy Statement

1.1. Fort Bend County ("County") adopts Electronic Signatures as a means of signing documents and records to promote paperless processing, to reduce the reliance on and cost of paper transactions, and to allow quicker access to documents. Fort Bend County Commissioners Court adopts this Electronic Signature Policy ("Policy") in consideration of the Texas Department of Information Resources' Guidelines for the Management of Electronic Transactions and Signed Records.

1.2. Under this policy, an Electronic Signature shall be used by County departments to conduct transactions internally, unless prohibited by law, and so long as the employee is an authorized signatory for the department. Additionally, Electronic Signatures shall be used, unless prohibited by law, by Authorized Officials, defined herein, who are legally authorized to bind the County in external business matters.

2. Purpose & Scope

2.1. Fort Bend County is committed to doing business in the most efficient and effective way possible and has adopted this policy as a means of signing documents and records to promote paperless processing, to reduce the reliance on and cost of paper transactions, and to allow quicker access to documents. This policy is adopted in accordance with the Uniform Electronic Transactions Act ("UETA"), Tex. Bus. & Comm. Code Ann. §§ 322.001, *et. seq.*, (West 2009 as amended).

2.2. Under this policy, an Electronic Signature may be used by County departments to conduct transactions both internal and external to the County. However, only the County Judge, Purchasing Agent, Sheriff, and those who have been designated authority by Commissioners Court or other official legally authorized to delegate signatory authority to legally bind the County may use Electronic Signatures for external business matters.

3. Definitions

Unless otherwise defined herein, terms having specific meaning shall have the meaning defined in the UETA.

3.1. Authorized Official: Any official of the County whose signature is required or permitted to be placed on a document or record that legally binds the County or authenticates the document or record.

3.2. Certification Authority: A person or entity that issues a digital certificate.

3.3. Digital Certificate or Certificate: An electronic document that uses a Digital Signature to bind together a public key with an identity (person's name or an organization) to a private key in an unalterable fashion. A Digital Certificate:

(a) Contains the Digital Signature of the certificate-issuing authority (See Certification Authority) so that anyone can verify that the certificate is authentic, and the certificate can be used to identify the party sending the message without encrypting the text.

(b) Is issued by the Certification Authority (CA).

3.4. Digital Signature: For purposes of this policy, "Digital Signature" shall include and be interchangeable with the term "Electronic Signature" and shall also include the subgroup of Electronic Signatures that is defined in the Government Code, Tex. Gov't Code Ann. § 2054.060(e)(1) (West 2011), as amended from time to time, which as of the date of issuance of this policy, reads as follows: Electronic identifier intended by the person using it to have the same force and effect as the use of a manual signature, and which provides authentication and integrity protection by using an asymmetric key operation where a private key is used to digitally sign an electronic document and the public key is used to verify the signature.

(a) Non-cryptographic technologies are the most commonly used for Digital Signatures and

include the following:

(i) Personal Identification Number (PIN) or password: A user accessing an electronic application is requested to enter a "shared secret" (called "shared" because it is known both to the user and to the system), such as a password or PIN.

(ii) Smart Card: A smart card is a plastic card, the size of a credit card, containing an embedded integrated circuit or a chip that can generate, store, and/or process data.

(iii) Digitized Signature (not to be confused with Digital Signature): A digitized signature is a graphical image of a handwritten signature.

(iv) Facsimile Signature: When the reproduction of the manual signature is in a graphic image format, the Facsimile Signature may be a Digitized Signature and a Digital Signature.

(v) Biometrics: Individuals have unique physical characteristics that can be converted into digital form and then interpreted by a computer (i.e., a fingerprint, facial recognition, etc.).

(vi) Signature Dynamics: A signature digest consisting of handwriting measurements of the person signing the message, such as a supermarket's credit card signature pad.

(b) Cryptographic technologies for Digital Signatures can be either symmetric (shared private key) cryptography, or asymmetric (public key/private key) cryptography. The latter is used in producing Digital Signatures.

(i) Shared Symmetric Key Cryptography: In shared symmetric key cryptography, the user signs a document and verifies the signature using a single, encrypted binary key.

(ii) Public/Private Key (Asymmetric) Cryptography - Digital Signatures: The term Digital Signature is now a generally accepted term that refers to a particular type of electronic signature that is created by cryptographic means involving the use of two mathematically related keys (i.e., a public and private key pair, often referred to as Public Key Infrastructure or PKI).

3.5. Document: Any signed communication which, in the course of an official transaction, becomes a government record. This includes records created or formatted electronically. Thus, all records and signatures must remain trustworthy and accessible for later reference as required by law.

3.6. Electronic: Relating to technology having electrical, digital, magnetic, wireless, optical, electromagnetic, or similar capabilities.

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

3.8. 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. Digital Signatures are a subset of Electronic Signatures.

3.9. Facsimile Signature: A reproduction of the manual signature of an authorized official that is made by any method, including engraving, imprinting, lithographing, and stamping.

3.10. 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.

3.11. Transaction: An action or set of actions occurring between two or more persons relating to the conduct of business, commercial, or governmental affairs.

3.12. Verification: The process of ensuring that a given Digital Signature is valid and positively identifies the originator of a message or record.

4. Exceptions

4.1. This policy does not apply to the following exceptions:

(a) Any federal law applicable to the record;

(b) A law governing the creation and execution of wills, codicils, or testamentary trusts;

(c) For the receipt of electronically filed documents pursuant to the Texas Business and Commerce Code or other applicable statutory law where the purpose of the written electronic communication is to comply with statutory filing requirements and the County is not a party to the underlying transaction which is the subject of the communication;

(d) This chapter does not apply to the transmission, preparation, completion, enforceability, or admissibility of a document in any form that is:

(i) produced by a court reporter appointed under Chapter 52, Government Code, or a court reporter certified under or a shorthand reporting firm registered under Chapter 154, Government Code, for use in the state or federal judicial system; or

(ii) governed by rules adopted by the supreme court, including rules governing the electronic filing system established by the supreme court.

(e) For the electronic approval of payment vouchers under rules adopted by the comptroller of public accounts pursuant to applicable law; or

(f) A law prohibits a transaction from occurring electronically, the transaction must occur in the manner otherwise allowed by law.

5. Use of Electronic Signatures

5.1. A department may use Electronic Signatures to conduct County business transactions and approvals in accordance with this policy and the UETA.

5.2. Where policies, laws, regulations, and rules require a signature, that requirement is met if the document contains an Electronic Signature.

5.3. Each party to a transaction must agree to conduct the transaction electronically in order for the electronic transaction to be valid. Consent may be implied from the context and surrounding circumstances.

5.4. If a law requires an Electronic Signature to contain specific elements, the Electronic Signature must contain the elements specified by law.

5.5. The manner and circumstances in which Electronic Signatures are acceptable is enumerated in the UETA.

5.6. This policy does not require a specific method for executing an Electronic Signature. The department signing the agreement is responsible for taking steps, in consultation with the Fort Bend County Attorney's Office, Information Technology, and Fort Bend County Purchasing to ensure that the method chosen is appropriate for the size and type of the transaction. Consideration must, at a minimum, be given to confidentiality, authentication of signatures, and verification that the document signed is, in all respects, identical to the one to which the signer intends to bind the company.

5.7. During the certification process, the County Attorney's Office, IT, Purchasing, and the department will consider the following issues:

(a) Legal Compliance – The electronic records and signatures must be maintained in a manner that efficiently and reliably preserves and protects the information over time so that it may be used for recognized governmental and legal purposes. The County Attorney's Office should be consulted if the Electronic Signature system will involve procurement, contracts, real estate, or matters governed by specific statutes or regulations not routinely handled by the department.

(b) The Value of the Transaction – Electronic signature systems for transactions involving the

transfer of funds or committing the County to actions or contracts should account for and minimize the County's financial and legal liability.

(c) Security – Electronic signature systems for secured transactions or transactions involving sensitive information should protect the County and users in terms of legal liability (civil or criminal), privacy, and confidentiality.

(d) Obsolescence – Both the record and the signature must be capable of long-term preservation in a format that will be supported for a duration consistent with retention laws.

(e) Documentation – The technology must ensure that the signatory cannot reasonably deny signing or sending a document, and each party must be capable of storing the final record.

(f) Interoperability – The Electronic Signature technology must be reasonably compatible with relevant software applications.

(g) Cost Benefit Analysis – The cost and use of the Electronic Signature method must comport with the degree of transactional and systemic risk.

5.8. Prior to accepting an Electronic Signature, the department shall ensure that the level of security used to identify the signer of a message and to transmit the signature is sufficient for the transaction being conducted. A department that accepts Electronic Signatures may not effectively discourage the use of Electronic Signatures by imposing unreasonable or burdensome requirements on persons wishing to use Electronic Signatures to authenticate written electronic communications sent to the department.

5.9. The department shall ensure that all written electronic communications received by the department and authenticated by means of an Electronic Signature in accordance with this Policy, as well as any information resources necessary to permit access to the written electronic communications, are retained by the department as necessary to comply with applicable law pertaining to audit and records retention requirements.

5.10. Use of Electronic Signatures is permitted, without further authorization, if all of the following requirements are met:

(a) The signing employee would be authorized to manually sign the agreement/document on behalf of their department Fort Bend County pursuant to;

(b) The other party/parties to the agreement are US entities and the transaction covered by the agreement will take place in the US; and

(c) The transaction does not involve a transfer of interests in real property.

5.11. Use of Electronic Signatures on any contract not meeting these requirements requires the prior review and approval by Purchasing, the County Attorney's Office and any other County Office with applicable authority to bind the County to contract.

5.12. Training on This Policy – All employees who have signing authority on any County contracts, have approval responsibilities for County commitments, or otherwise are involved in the contracting process must have knowledge and understanding of this Policy. The County Attorney's Office in conjunction with Purchasing, is responsible for providing the necessary training on this Policy.

6. Administration of This Policy

6.1. Fort Bend County Information Technology, with assistance from the County Attorney's Office and Purchasing, is responsible for the administration of this Policy. All employees are responsible for consulting and complying with the most current version of this Policy. If you have any questions regarding this Policy, please contact the Fort Bend County Information Technology or the Fort Bend County Attorney's Office.

7. Compliance with Related Policies.

7.1. All other policies that apply to the execution of contracts on behalf of the County remain in full force and effect.

8. Authorities & References

8.1. Guidelines for the Management of Electronic Transactions and Signed Records.Uniform Electronic Transactions Act ("UETA"), Tex. Bus. & Comm. Code Ann. §§ 322.001, *et. seq.*, (West 2009 as amended).

8.2. Tex. Gov't Code Ann. § 618.002 (West 2011).

8.3. Tex. Gov't Code Ann. § 2054.060(e)(1) (West 2011)

8.4. Uniform Federal Lien Registration Act, Tex. Prop. Code § 15.001, et. seq., (West 2009).

8.5. Uniform Real Property Electronic Recording Act, Tex. Prop. Code § 15.001, et. seq., (West 2009)