1. POLICY STATEMENT

The City of Houston 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.

Under this policy, an electronic signature may be used by City departments and divisions to conduct transactions both internal and external to the City.

2. POLICY PURPOSE & SCOPE

To increase efficiency by adopting electronic signatures as an alternative to manual signatures on paper documents and to provide a process by which departments can be certified to incorporate electronic signature technology into their electronic workflow processes. The City recognizes electronic signatures are becoming a routine way of conducting business and that formal rules governing the use of electronic signatures by the City are necessary. This policy applies to all City departments and divisions that desire to use electronic signatures to conduct transactions both internal and external to the City.

3. DEFINITIONS

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

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:

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

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 Texas 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.

- Non-cryptographic technologies are the most commonly used for digital signatures and include the following:
  - 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.

- 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.
- Digitized Signature (not to be confused with digital signature): A digitized signature is a graphical image of a handwritten signature.
- A 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.
- Biometrics: Individuals have unique physical characteristics that can be converted into digital form and then interpreted by a computer (i.e., a fingerprint).
- Signature Dynamics: A signature digest consisting of handwriting measurements of the person signing the message, such as a supermarket's credit card signature pad.

○ 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.

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

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.

Electronic: Has the meaning ascribed in the Texas Uniform Electronic Transactions Act, Tex. Bus. & Com. Code Ann. § 322.002(5) (West 2009), as amended from time to time, which as of the date of issuance of this policy, reads as follows: Technology having electrical, digital, magnetic, wireless, optical or electromagnetic, or similar capabilities.

Electronic Record: A record of information that is created, generated, sent, communicated, received or stored by electronic means and that is retrievable in perceivable form.

Electronic Signature (e-signature): Has the meaning ascribed in the Texas Uniform Electronic Transactions Act, Tex. Bus. & Com. Code Ann. § 322.002(8) (West 2009), as amended from time to time, which as of the date of issuance of this policy, reads as follows: 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.

Facsimile Signature: Has the meaning ascribed in the Texas Government Code, Tex. Gov't Code Ann. § 618.002 (West 2011), as amended from time to time, which as of the date of issuance of this policy, reads as follows: A reproduction of the manual signature of an authorized officer that is made by any method, including engraving, imprinting, lithographing, and stamping; and which is further defined, referenced to, and governed by other laws, including Section 2-27 of the City of Houston Code of Ordinances.

Law: Refers collectively to all laws, statutes, ordinances, rules, regulations, policies, and other types of local, state, national and foreign government authority, including the City Charter, the City of Houston Code of Ordinances, and laws relating to electronic signatures, fraud, and computer crimes.

Record: Has the meaning ascribed in the Texas Uniform Electronic Transactions Act, Tex. Bus. & Com. Code Ann. § 322.002(12) (West 2009), as amended from time to time, which as of the date of issuance of this policy, reads as follows: Information that is inscribed on a tangible medium or that is stored in an electronic or other medium and that is retrievable in perceivable form.

SOC report: Refers to the Service Organization Control auditing reports that are issued in compliance with the SSAE18 standard.

SSAE18 standard: Refers to the Statement on Standards for Attestation Engagements No. 18 auditing standard set by the American Institute of Certified Public Accountants.

Texas Uniform Electronic Transactions Act (Texas UETA): Refers to Texas Business and Commerce Code, Chapter 322 et seq., as amended from time to time.

Transactions: Has the meaning ascribed in the Texas Uniform Electronic Transactions Act, Tex. Bus. & Com. Code Ann. § 322.002(15) (West 2009), as amended from time to time, which as of the date of issuance of this policy, reads as follows: An action or set of actions occurring between two or more persons relating to the conduct of business, commercial, or governmental affairs.

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

Unless otherwise defined in this policy, terms having specific meaning shall have the meaning defined in the Texas UETA.

4. POLICY DETAILS

4.1 A department may use electronic signatures to conduct City business transactions and approvals in accordance with the following guidelines and the Texas Uniform Electronic Transactions Act, Tex. Bus. & Com. Code Ann. Section 322 et seq. (West 2009).

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

4.1.2 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.

4.1.3 If a law prohibits a transaction from occurring electronically, the transaction must occur in the manner otherwise allowed by law.

4.1.4 If a law requires an electronic signature to contain specific elements, the electronic signature must contain the elements specified by law.

4.1.5 The manner and circumstances in which electronic signatures are acceptable is enumerated in the Texas Uniform Electronic Transactions Act, Tex. Bus. & Com. Code Ann. Section 322 et seq. (West 2009).

4.2 A department seeking or converting to an electronic signature system must first receive certification approval from the Records Management Division of ARA, followed by authorization through the City's IT Governance Board. Records Management shall route these requests through the appropriate individuals.

4.3 During the certification process, HITS, ARA, and the department will consider the following issues:

4.3.1 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 City 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, ARA, or HITS.

4.3.2 The Value of the Transaction – Electronic signature systems for transactions involving the

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

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

4.3.4 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 AP 8- 5.

4.3.5 Documentation – The technology must ensure that the signatory cannot reasonably deny signing or sending a document.

4.3.6 Interoperability – The electronic signature technology must be reasonably compatible with relevant software applications.

4.3.7 Cost Benefit Analysis – The cost and use of the electronic signature method must comport with the degree of transactional and systemic risk.

4.3.7.1 HITS, ARA, and the department will evaluate the risks of the transaction in terms of dollar value, consequences of failure, damage to credibility, etc.

4.3.7.2 HITS, ARA, and the department will evaluate the effectiveness of the electronic signature method in terms of verification and system security. An ID and password may not provide the same level of assurance of authenticity compared to a method that involves encryption or biometrics (e.g., fingerprints or voice prints).

4.3.7.3 HITS, ARA, and the department will evaluate the cost of the available alternatives in terms of capital and operational costs to implement and maintain a particular signature method. Using an ID and password is less expensive and easier to implement compared to a more expensive biometric or encryption-based signature method.

4.3.8 The City's IT Operating Committee or the IT Governance Board reviews each proposed electronic signature system for compliance with previously approved standards, technologies, vendors, and contracts. Exceptions to these standards will be approved on a case by case basis by the IT Governance Board. Electronic signature systems or electronic recordkeeping systems used to store electronic signatures that that have been used but not already approved pursuant to this policy will be certified based on sections 6.2.1 – 6.2.4, not by vendor or technology. See section 6 for recertification procedures.

5. ROLES AND RESPONSIBILITIES

5.1 Houston Information Technology Service (HITS) shall:

5.1.1 Provide assistance and support to City departments seeking or converting to process transactions through electronic signature systems by conveying standards approved by the IT Governance Board, analyzing requirements and providing technology recommendations, assisting with procurement via City-wide IT contracts, etc.;

5.1.2 Within 60 days of receipt of an application for a new electronic signature system, review departmental electronic signature system applications before presentation to the IT Governance Board;

5.1.3 Support implementation of electronic signature systems approved by the IT Governance Board;

5.1.4 Keep logistical information regarding what electronic signature software is currently approved,

what City departments are using this software, and annual SOC report submissions from approved electronic signature system providers; and

5.1.5 Maintain general oversight of the City's Certification Authorities through third-party vendors or HITS-maintained security and authentication services. Departments, if requested, will have control over day to day administration of certificates including creation and revocation procedures.

5.2 Records Management Division (Records Management) of Administration and Regulatory Affairs Department (ARA) shall:

5.2.1 Provide assistance and support to departments requesting certification;

5.2.2 Confer with HITS and other intra-governmental bodies to establish minimum security requirements and citywide standardization, and to address any concerns relevant to electronic system acquisition;

5.2.3 Process approved certification requests; and

5.2.4 Provide documentation of compliance when certification requirements have been met.

5.3 Departments electing to use an electronic signature system shall:

5.3.1 Certify any electronic recordkeeping systems (e.g.; SAP, SharePoint, Shared Drive, etc.) used to store electronic signatures in accordance with AP 8-5 and this policy. To start the certification process, contact ARA's Records Management Section at 832-393-8543.

5.3.2 Collaborate with HITS to select an appropriate electronic signature system;

5.3.3 Seek certification of the electronic signature system; and

5.3.4 Obtain authorization and certification for any electronic signature systems or electronic recordkeeping systems used to store electronic signatures that were currently in use on the date policy was effective. See section 6 for recertification procedures.

6. USE AND RENEWAL OF CERTIFICATIONS

6.1 Once an electronic signature system has been approved by the IT Governance Board and the appropriate certification requirements are met and verified by Records Management, a department may use electronic signatures in lieu of manual signatures.

6.2 Authorization and Certification Timelines:

6.2.1 Electronic signature systems that have been used but not already approved pursuant to this policy shall be authorized and certified by the process described herein. These authorizations and certifications shall be completed within three (3) years of the effective date of this policy. Initial certification of existing systems shall be conducted primarily in regards to legal and security compliance of the system's electronic signature methodology rather than compliance to approved standards for specific technologies or vendors.

6.2.2 HITS may prioritize electronic signature systems' authorization reviews when considering operational needs and risks.

6.2.3 Authorizations and certifications must be renewed in accordance with the term specified in the digital certificate, which term shall not exceed five (5) years. Renewals are reviewed based on all the considerations described in section 6.2.

6.2.4 ARA, in collaboration with HITS and the Legal Department, may revoke an electronic signature system's authorization if it is later deemed unsuitable for the task it is assigned.

6.3 To ensure that all electronic signature systems used by the City conform with physical, technical, operational, and administrative measures and protocols regarding data security, HITS shall request that all authorized and certified electronic signature system providers, on an annual basis, submit to HITS a copy of its SOC report received from its third-party independent auditors.

7. AUTHORITY AND EFFECT OF ELECTRONIC SIGNATURES

7.1 In accordance with Sections 322.005(b) and 322.007(d), Tex. Bus & Com. Code Ann. (West 2009), where policies, laws, regulations, and rules require a written document or signature, that requirement is met if the document or signature is, respectively, an electronic record or contains an electronic signature, subject to certain exceptions stated in this policy or as otherwise required by law.

7.2 Electronic signatures shall not be used, and shall have no binding authority or effect on City records, where electronic signatures are prohibited by law or other City policies or where a law prohibits a transaction from occurring electronically.

7.3 This policy shall not preclude the use of any other types of signatures, including without limitation, manual signatures or Facsimile Signatures. This policy shall not limit, alter, modify, or otherwise affect any requirement imposed by law relating to (a) authority, obligations, or procedures required for Facsimile Signatures, including Section 2-27 of the City of Houston Code of Ordinances; (b) the proper procedures and authorization necessary to execute City records; (c) requirements to legally bind or obligate the City under any contract or agreement; and (d) the legal effectiveness, validity, or enforceability of any City record, including any contract or agreement, signed electronically in violation of any such laws. All laws regarding signing City records shall apply to electronic signatures and electronic records, including Article II, Section 19 of the City Charter, Chapter 15 of the City of Houston Code of Ordinances, and all laws regarding signing, adopting, entering in, or executing contracts, agreements, purchase orders, statements of work, ordinances, leases, licenses, and any other document purporting to be legally binding upon or otherwise obligating the City.

7.4 In the event that any electronic signature is found by the City Attorney to have been used or applied to a City record or certified in violation of this policy or any other law, the electronic signature shall be null and void and the City record signed electronically using the unlawful, fraudulent, unauthorized or otherwise improper electronic signature shall also be (a) null and void, (b) discontinued, and (c) unenforceable against the City.

8. POLICY SPONSOR

Department: Administration and Regulatory Affairs

9. CONFLICT AND REPEAL

This Administrative Policy supersedes Administrative Procedure 8-6, Electronic Signatures, dated April 23, 2014, which shall be of no further force or effect.

If the provisions of this policy conflict with any law, that law shall prevail.