

Document Code No.: INF-14-3-EP

Title: Using Electronic Signatures

Affected Agencies: All Executive Branch Departments and Agencies

Authorities: The Uniform Electronic Transaction Act (UETA)

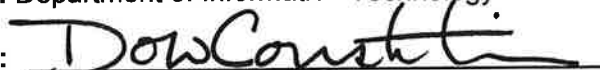
Keywords: electronic signature, e-signature

Sponsoring Agency: Department of Information Technology



King County

Executive signature:



Date signed and effective:

7.23.20

I. Purpose

This Policy establishes when electronic signature technology may replace a hand-written signature for internal and external business purposes. The Policy is intended to strongly encourage the use of paperless, electronic documents where appropriate, feasible, and allowed by law. The two-fold goal is to make electronic signature usage the norm of business practices countywide and to make the process of implementing electronic signature services as simple as possible. Minimizing barriers to implementation and standardizing the use of electronic signatures across the county promotes the county's efforts to achieve the "best-run government" by improving administrative efficiencies and supporting our long-term sustainability goals. This Policy provides specific guidance on how to implement, maintain, and establish internal controls for the use of electronic signature technology, and applies to signatures required for the processing of county documents.

II. Organizations Affected

This Policy applies to the Administrative Offices and Executive Departments supervised by the King County Executive and any non-Executive Branch King County departments adopting this Policy.

III. Definitions

"CIO" refers to King County's Chief Information Officer, director of King County's Department of Information Technology (KCIT).

"Agency" means any department or office managed by an elected official of any branch of King County government.

"Electronic Signature" or "e-signature" means an electronic sound, symbol, or process attached to or logically associated with a contract or other record and executed or adopted by a person with the intent to sign the record.

"KCIT" refers to King County's Department of Information Technology.

"Steering Committee" refers to the Electronic Business Steering Committee, formed to provide Electronic Signature program oversight and support.

IV. Policy

A. Acceptance of Electronic Signatures

1. Agencies may use Electronic Signatures to show approval, authorization and/or certification for electronic submissions, with the same force and effect as signatures affixed by hand. An Electronic Signature satisfies a signature requirement on a county document. Discretion is given to the Agency to determine which documents will be eligible for Electronic Signature, unless where required by statute.

2. An Agency that accepts Electronic Signatures must comply with KCIT's methods and processes for Electronic Signature as set forth in this Policy. Exceptions to the policy as stated herein must be approved by the Steering Committee as outlined in the Electronic Signature Procedures Manual.

3. Agencies electing to use Electronic Signatures will follow the following guidelines:

- a. For documents sent external to the county for signature, especially those that have a legally binding effect (including, but not limited to contracts, subpoenas and permits) and therefore require high-level authentication and security measures in a locked format, agencies are required to use the county's contracted Electronic Signature vendor.
- b. For documents used internal to a county agency, or between county agencies, that do not require high-level authentication and a locked format (for example, using a text box containing a signature that is inserted into the document), while use of the county's vendor is encouraged, agencies are given the discretion to use an alternative Electronic Signature vendor. In these cases, a request for an exception to policy is not required. However, for any other internal documents identified as needing signatures that have a legally binding effect, or require high-level authentication and security measures in a locked format, agencies are required to use the county's contracted Electronic Signature vendor.

4. Agencies that accept and use Electronic Signatures for documents that also require a notary certification are permitted to accept and use an electronic notary certification if the notarial act complies with state law as outlined in Chapter 42.45 RCW.

5. The county's contracted Electronic Signature vendor will manage all functions related to the affixing of e-signatures to, and access and storage of, designated county documents. KCIT will ensure that the electronic signature software is fully integrated into current KCIT approved software for document generation. The intent is to promote the standard use of Electronic Signature services and options among Agencies as a "best practice."

6. Documents sent to the county that originate at an external organization, requesting an e-signature using a method or process selected by the external organization, can be signed electronically by county staff as long as supervisors of both parties agree to the method or process beforehand.

B. Agency Business Applications

1. New Electronic Signature service implementations: Directors, managers, and supervisors (or their designees), of Agencies desiring to implement Electronic Signature services for the first time, or replace an existing vendor providing this service, should contact KCIT by submitting a Help Desk ticket for requirements, pricing, training, and scheduling. Departmental Information Technology Customer Success Managers (IT CSM) will be an alternate source of support in establishing e-signature services.

2. Existing Electronic Signature services. Agencies with Electronic Signature services provided under contract with another vendor prior to the effective date of these policies are expected to migrate to the county's contracted Electronic Signature Vendor when their current vendor contract expires (or is terminated) or when there is an option to renew or extend the contract. No Agency may enter into any vendor agreement for any Electronic Signature service that is not the county's contracted vendor without the prior written consent of the Steering Committee. Agencies may be permitted to maintain their use of a third-party management system that has an embedded Electronic Signature processes with the submission and approval of an Exception Request.

3. Process for Making an Exception Request: Agencies desiring to use another Electronic Signature vendor must request a waiver from the CIO or his/her designee in advance. The CIO or his/her designee will provide a recommendation to the Steering Committee for any exception to policy requested. The Steering Committee has ultimate authority to grant case-by-case exceptions for the use of an alternative solution instead of the county's approved Electronic Signature vendor. Due to an emphasis on standardizing best practices across the county, only in rare circumstance will requests for a waiver be approved.

C. Electronic Signature Security and Privacy

1. KCIT and its Electronic Signature vendor shall maintain and administer IT security requirements, ensuring the safeguarding of sensitive electronic documents and information stored by the vendor.

2. All Agencies accepting Electronic Signatures must be familiar with county policies and guidelines governing IT security, and required actions in the event of a security breach.

D. Internal Controls, and Documentation Preservation and Retention

1. Agencies that elect to use Electronic Signatures are responsible for determining, in conjunction with the Prosecuting Attorney's office, where applicable laws permit an Electronic Signature to be used. Agencies that opt to use Electronic Signatures must adopt/amend their business practices to support the requirements of this Policy.
2. Records of documents signed by Electronic Signature(s) must remain searchable and retrievable for the required retention period as established by policy and law.
3. The Electronic Signature vendor shall ensure that the documents signed electronically, once completed and stored electronically, cannot be changed or altered.
 - a) In cases where documents are initiated electronically and sufficient controls do not exist to ensure the integrity of the document's date, KCIT will notify the authorized user and the authorized individual must print, review, and sign the document. The printed records are considered the official source document and retained per the retention schedule.

E. Contracts

1. KCIT shall establish and administer countywide contracts with vendors for the providing of Electronic Signature solutions for county documents.
2. KCIT shall keep the Steering Committee apprised of all matters associated with the establishment and administration of contracts with vendors for the providing of Electronic Signature solutions for county documents.
3. No Agency may enter into any vendor agreement for any Electronic Signature service that is not the county's contracted vendor without the prior written consent of the Steering Committee.
4. KCIT, through the establishment of contracts with vendors and other related partners, shall assist Agencies in understanding contract requirements and the pricing structure options relative to Electronic Signature services.

F. Annual Reporting

The CIO or designee will work with Agencies each year to collect usage data to monitor the progress of e-signature usage across the county, including e-signature volume and document types.

V. Implementation Plan, Methods and Processes

- A. KCIT and the Steering Committee shall establish and maintain the methods and processes for management of Electronic Signature services, including, but not limited to, access to the Electronic Signature system, contracting for Electronic Signature services, monitoring the unit cost per signatures, and standard business processes and procedures.
- B. The Department of Information Technology is responsible for implementation of this Policy. Individual Agencies are responsible for setting up the use of electronic signature methods and processes within their Agency.
- C. The Department of Information Technology is responsible for communicating this Policy to the respective Agencies and other appropriate parties annually.

VI. Maintenance

- A. This Policy will be maintained by the King County Information Technology Department, or its successor agency.
- B. This Policy will automatically expire five (5) years after its effective date. A new, revised, or renewed policy will be initiated by the King County Information Technology Department, or its successor agency prior to the expiration date.

- VII. Consequences for Noncompliance.** Departments and Agencies that elect to use electronic signatures, and do not conform to this policy, may be in violation of County Code and State Law. Failure to comply with this policy may result in KCIT and the Steering Committee restricting or terminating the use of electronic signatures for the Agency's documents.

Appendices:

Electronic Signature Procedures Manual [available from KCIT]

Enterprise eSignature "How To's" documentation [available from KCIT]