

RESOLUTION NO. 2023-13

A RESOLUTION OF THE CITY COUNCIL OF THE CITY OF ELLENSBURG AUTHORIZING THE USE OF ELECTRONIC AND DIGITAL SIGNATURES IN THE CITY AND ADOPTING AN ELECTRONIC AND DIGITAL SIGNATURE POLICY.

WHEREAS, in Chapter 19.360 RCW, the Washington State Legislature authorized electronic dealings for governmental affairs and established the implementation framework for electronic governmental affairs and governmental transactions; and

WHEREAS, in March 2020, through Engrossed Substitute Senate Bill 602\$ (“ESSB 6028”), the Washington State Legislature repealed Chapter 19.360 RCW and adopted the Uniform Electronic Transactions Act (UETA), codified in Chapter 1.80 RCW, which is intended to facilitate use of electronic transactions consistent with other applicable law, and to bring consistency to reasonable practices concerning electronic transactions and with the continued expansion of those practices; and

WHEREAS, ESSB 6028 took effect on June 11, 2020; and

WHEREAS, ESSB 6028 defines an “electronic signature” as “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”; and

WHEREAS, ESSB 6028 defines an “electronic record” as “a record created, generated, sent, communicated, received, or stored by electronic means”; and

WHEREAS, ESSB 6028 provides that “[a] record or signature may not be denied legal effect or enforceability solely because it is in electronic form; a contract may not be denied legal effect or enforceability solely because an electronic record was used in its formation; if a law requires a record to be in writing, an electronic record satisfies the law; and if a law requires a signature, an electronic signature satisfies the law”; and

WHEREAS, the method and process for electronic submissions and the use of electronic signatures must be established by ordinance, resolution, policy, or rule; and

WHEREAS, to promote social distancing during the COVID-19 pandemic, and to increase the effectiveness and efficiency of the City of Ellensburg business processes, the City utilized technology solutions which are in compliance with the Uniform Electronic Transactions Act to apply authenticated electronic signatures to legally enforceable electronic records as allowed by ESSB 6028.

NOW, THEREFORE, BE IT RESOLVED, by the City Council of the City of Ellensburg, Washington, as follows:

Section 1. The foregoing recitals are incorporated and fully made a part of this Resolution.

Section 2. The City Council finds it to be in the public interest to allow the use of electronic records, electronic and digital signatures for City business to the fullest extent allowed by law.

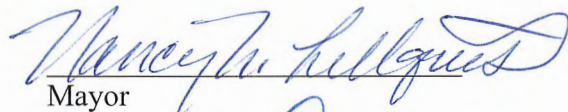
Section 3. The City Council hereby adopts the Electronic and Digital Signature Policy attached hereto as Exhibit "A".

Section 4. The City Council hereby authorizes the City Manager, or their designee, to establish any other policies, rules and/or regulations to implement the Electronic and Digital Signature Policy consistent with this Resolution and RCW 1.80., *et.seq.* (and as amended in the future).

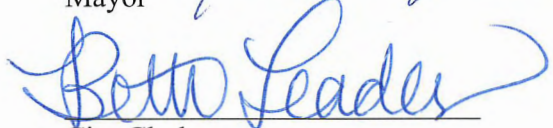
Section 4. This resolution and policy shall take effect immediately.

ADOPTED by the City Council of the City of Ellensburg this 5th day of June, 2023.

Attest:



Mayor



City Clerk

City of Ellensburg Electronic and Digital Signature Policy

1. Purpose

The purpose of this policy is to allow for the use of electronic and digital signatures that complies with the Uniform Electronic Transactions Act (UETA), chapter 1.80 RCW.

2. Definitions

Authentication: The assurance, using a security protocol appropriate for the purpose, that a given Electronic Signature is that of a person purporting to sign the record or conduct the Electronic Transaction so as to allow it to be properly attributed pursuant to RCW 1.80.080.

Authorized Signer: The Mayor, Mayor Pro Tempore, City Manager, Assistant City Manager, City Attorney, City Clerk, Department Directors, and their designees, and any other City employee or elected official who has been granted authority to sign certain records on behalf of the City either by the nature of their position in relation to the record or by direct authorization from City Council or Ellensburg City Code.

Certificate Authority or Certification Authority (CA): Is a trusted entity that issues digital certificates and assumes the role of trust center. The CA holds the Private Key that is used to validate the public key that was created by the Certificate Authority and the user's private keys.

Digital Signature: A digital signature is one type of Electronic Signature that uniquely links a user's identity information to a digital certificate issued by a licensed certificate authority, behind the signature, and offers validation that the document has not changed when added to a "signed" Electronic Record by the sole person in control of a certificate or password.

Digital Identification: Is an Identification validated by an electronic authorization process bonded to an electronic document that validates that the document has not been changed.

Digital Certificate: A digital certificate is a file or electronic password that proves the authenticity of a document, signature, or user through the use of cryptography and the standard Public Key Infrastructure. A private Digital Certificate is one that is issued by a Certificate Authority that is for internal use only, provides greater security, but should not be used for external signatures as the Internal Certificate Authority is not publicly accessible.

Electronic Signature: An electronic sound, symbol, or process, attached to or logically associated with an electronic record and executed or adopted by a person with the intent to sign the record.

Electronic Signature Vendor: The company with which the City contracts for electronic document and signature services. The company must use a valid public certificate authority for issuing digital certificates.

Facsimile Signature: One type of Electronic Signature that is a reproduction of a handwritten signature that has been saved electronically or by engraving, imprinting, or stamping.

Wet Signature: A signature created in person when the signer physically marks a document.

3. Responsibilities

It is the responsibility of all City employees, elected officials and volunteers to ensure that they adhere to the electronic signature policies outlined in this document to provide reasonable assurance of authenticity and accuracy when using electronic documents.

4. Electronic Signatures Authorized

A. This policy does not impact the use or legitimacy of wet signatures. However, the City recognizes electronic signatures as legally binding and equivalent in nature to wet signatures.

B. Electronic, digital or facsimile signatures may be used on City records requiring execution by a third party, consistent with the requirements of this policy.

C. The City Manager, City Department Directors, and all authorized representatives or designees thereunder, shall have authorization to use the Electronic Signature Vendor to affix electronic signatures to electronic records, including but not limited to ordinances, resolutions, contracts, applications, publications, and all other electronic documents through which the City conducts business.

D. The City authorizes the Finance Director to select a validation platform or process for electronic signature and/or digital identity for all financial transactions within the City, including but not limited to documentation or accounts payable records, payroll records (timesheets and leave requests), claim vouchers, purchase orders, or other similar documents.

E. Electronic Signatures may not be applied using another employee's name. Any employee or official applying an electronic signature shall use their own name.

5. Guidelines for Using Electronic Signatures

A. Security of Electronic Transactions and Electronic, Digital, and Facsimile Signatures.

1. A valid digital signature is a digital identification combined with a certificate issued by a certificate authority providing the following protections:

i. Verifies the Authorized Signer is who they represent themselves to be because the person had to prove their identity to a certificate authority to obtain the digital certificate.

ii. Confirms the document was not altered after the signature was applied to the document and not copied from another document because the certificate file and digital identification information is cryptographically bound to the document and depicted as a digital signature.

iii. Ensures the document was not altered after it was signed.

2. The certificate, password, and private key used to create a digital signature is the personal property of the subscriber and is exempt from public inspection and copying under Chapter 42.56 RCW.

3. Authorized Signers may sign City documents digitally if such an option is available, providing the following:

i. The digital signature utilized by the Authorized Signer in connection with the digital identification that is an electronic authentication process attached to or logically associated with an electronic document. The digital certificate is obtained from a certification authority in compliance with state law;

ii. When the authentication process depends on a digital certificate, then the digital certificate must not be expired when the Authorized Signer signs the document digitally with the validating certificate;

iii. The Authorized Signer does not provide information to the certification authority they know to be untrue; and

iv. The digital certificate must be;

- a. Unique to the licensee using the certificate;
- b. Capable of independent verification;
- c. Under the exclusive control of the licensee using it; and
- d. Linked to a document in such a manner that the digital identification is invalidated if any data in the document is changed.

v. The digital signature contains the following information:

- a. The date and time of the signature; and
- b. A hand-written representation of the Authorized Signer's signature; or
- c. A typed representation of the Authorized Signer's name and title.

4. Electronic or digital signatures cannot be applied using Authorized Signer's name. Records signed by an Authorized Signer shall use their own digital identification that is an electronic or digital signature.

5. Authorization to use or accept facsimile signatures shall be limited to instances where the authenticity of the signatures is deemed reliable and secure. In order to accept a facsimile signature in lieu of a wet signature, the authenticity of the facsimile signature must be verified by the receiving party. Such means of verification may include:

i. The receipt of a faxed signature from a facsimile number verified as belonging to or traceable to the party that did so sign and transmit the document.

ii. The receipt of an emailed signature from an email address verified as belonging to the party that did so sign and transmit the document.

B. For documents sent to the City from an external entity for signature, especially those that have a legally binding effect, such as contracts, subpoenas, permits, grants, etc., the documents may be signed electronically if there is reasonable assurance that the means and methods used in electronically signing or submitting the document ensure the integrity, authenticity and nonrepudiation of the signature or document received. Questions regarding whether a document meets this requirement should be directed to the IT Department and/or City Attorney's office prior to signature.

C. For documents used internally within the City that do not require high-level authentication and a certificated format, City staff may use alternative methods of electronic signature other than the Electronic Signature Vendor. However, for any internal documents identified as needing signatures that have a legally binding effect, or require high-level authentication and security measures in a locked format (e.g., certain financial documents), the City is required to use the Electronic Signature Vendor. The department with overall authority for the document type will determine whether an alternative method of electronic signature is appropriate for use.

D. If City staff does not know whether a document may be legally signed electronically, they should consult the City Attorney's Office for guidance.

6. Non-Electronic Signatures Required

There will be times where non-electronic or "wet" signatures will be required to be used by the City. Non-electronic signatures are required on all documents where they are required by law, real estate transfer documents (i.e., deeds, easements, covenants and other documents that may be recorded by the auditor as part of the transfer of title or possessory rights of real property), documents that must be notarized, and any other documents determined by the City Manager to be appropriate for non-electronic signature, regardless of state law.

7. Electronic Signature Security and Privacy

The IT Department and the Electronic Signature Vendor shall maintain and administer security requirements and ensure the safeguarding of sensitive electronic documents and information stored by the Electronic Signature Vendor. All City departments accepting electronic signatures must be familiar with this policy as well as all IT Security Policies, and the required actions to be taken in the event of a security breach.

8. Retention and Preservation

Records of documents signed by electronic signature must remain searchable and retrievable for the required retention period as established by law. The Electronic Signature Vendor will ensure that the documents signed electronically, once completed and stored electronically, cannot be changed or altered. If sufficient controls do not exist, IT will notify and/or work with staff and all documents must be printed, signed, and retained pursuant to City policy. The printed record will be considered the official source document for retention purposes. Upon receipt of a fully executed electronic document the Mayor, Mayor Pro Tempore, or City staff person signing the document shall process the document for proper retention and preservation.