BOC *Electronic & Digital Signature Policy*

Division: LEGISLATIVE
Scope: ALL PERSONNEL
Adopted: 04/12/2021 **Next Review**: 04/2025

CKFR Board Policy

1.0 INTRODUCTION

State law has codified the authority to execute documents remotely. Streamlining processes that require wet signatures and replacing them with electronic signatures, when practical, is consistent with the intent of State law to promote electronic transactions and remove barriers that might prevent the use of electronic transactions by governmental entities.

By transitioning to a policy of executing documents remotely, Central Kitsap Fire & Rescue (CKFR or "the District") will reduce its reliance on paper-based transactions and will further improve information security and sharing. Further, such transition will facilitate more efficient approval of and access to documents and reduce costs and environmental impact.

2.0 PURPOSE AND SCOPE

CKFR has established this Electronic & Digital Signature Policy to allow for the acceptance and submission of electronic and digital signatures and it applies to all authorized signers for Central Kitsap Fire & Rescue.

3.0 DEFINITIONS

Authorized Signer - The Board of Commissioners, The Fire Chief, Deputy Fire Chief, Assistant Chiefs, District Attorney, District Secretary, Department Directors and Managers, and their designees, and any other District employee who has been granted authority to sign certain records on behalf of the District either by the nature of their position in relation to the record or by direct authorization from the Fire Chief.

Digital Signature - One type of electronic signature that contains a digital certificate, issued by a licensed certificate authority, behind the signature and offers authentication when sending a "signed" electronic document.

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

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.

Facsimile Signature - A reproduction of a hand written signature that has been saved electronically or by engraving, imprinting or stamping.

4.0 POLICY

4.1 Pursuant to Resolution 21-14, the District authorizes electronic transactions and the use of electronic, digital, or facsimile signatures in accordance with this Policy.

4.2 A District document that is required by law to be signed in non-electronic media may not be electronically or digitally signed.

4.3 An electronic, digital or facsimile signature is an acceptable substitute for a wet signature on records requiring the signature of any record whenever the use of a wet signature is authorized or required, except as provided herein.

4.4 If an electronic or digital signature is used for interstate transactions or for documents required by the US Federal government, the signature shall comply with the requirements of the Electronic Signatures in Global and Electronic Commerce Act.

4.5 A document signed electronically, digitally or via facsimile shall be deemed the equivalent of an original signed document if the individual or entity signing the document has complied with the provisions of this Policy.

4.6 This Policy in no way affects the District's ability to conduct a transaction using a physical medium and shall not be construed as a prohibition on the use of wet signatures.

5.0 PROCEDURE

5.1 **Authorization for Use of Electronic Transactions and Electronic, Digital and Facsimile Signature:**

5.1.1 Authorized Signers are authorized to sign records using a facsimile signature or via an electronic signature platform to affix electronic or digital signature to District records as provided in the Policy.

5.1.2 Authorized Signers may affix electronic, digital or facsimile signatures to the following records: Minutes of all District Board meetings, retreats, and workshops, Resolutions and Ordinances adopted by the Board of Commissioners, Accounts Payable records (including but not limited to invoices, vouchers, and expenditure approvals), and any and all Contracts and Agreements to which the District is a party.

5.1.3 Electronic, digital or facsimile signatures may be used on District records requiring execution by a third party.

5.2 **Security of Electronic Transactions and Electronic, Digital and Facsimile Signature**

5.2.1 A valid digital signature that is issued by a certificate authority provides the following protections:

a. 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 signature.

b. Confirms the signature was applied to the document and not copied from another document because the signature file is cryptographically bound to the document.

c. Ensure the document was not altered after it was signed.

5.2.2 The 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.

5.2.3 Authorized Signers may sign District documents digitally if such an option is available, providing the following:

a. The digital certificate utilized by the Authorized Signer in connection with the digital signature is obtained from a certification authority in compliance with state law;

b. The digital certificate is not expired when the Authorized Signer signs the document digitally;

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

d. The digital signature contains the following information:

1. A hand-written representation of the Authorized Signer's signature;

2. A typed representation of the Authorized Signer's name and title; and;

3. The date and time of the signature.

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

5.2.5 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:

a. 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.

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

5.2.6 Information that is necessary to verify the authenticity of a facsimile signature should be retained and transmitted with the document. This retained information may include but it is not limited to an electronic file with metadata saved from an email to which facsimile signature was attached or a fax coversheet verifying who sent the record.

5.3 **Transmission and Storage of Electronic Transactions and Signatures**

5.3.1 Electronically or digitally signed electronic records shall be stored in such a way as to ensure their preservation, disposition, integrity, security, confidentiality, and auditability.

5.3.2 Electronic records shall only be transmitted via secure services including, but not limited to, email, drop box, and cloud-based digital signature platforms.

6.0 REFERENCES

6.1 Chapter 1.80 RCW – Uniform Electronic Transaction Act

6.2 SOP 03-03 – Purchasing Procedures