



**POLICY 1060**

**Digital and Electronic Signature Policy**

**VERSION 2**

**APPROVED BY BOARD** 12/11/2025

**APPLIES TO**

Division	Districtwide
Sub-Division	Administration

<b>VERSION</b>	<b>REVISION DATE</b>	<b>DESCRIPTION OF CHANGE/SUPERSEDE</b>	<b>AUTHOR</b>
1	8/11/2020	Creation of digital signature policy to align with the CSDA digital signature policy	Unknown
2	10/2/2025	Updated to reflect current digital signature practices per the CSDA digital signature policy	Administrative Coordinator

**TERMS AND DEFINITIONS**

<b>TERM</b>	<b>DEFINITION</b>
Digital Signature	An electronic identifier and type of "electronic signature," created by computer, intended by the party using it to have the same force and effect as the use of a manual signature.
Digital Signature Certification Authority	An entity authorized by the Secretary of State to issue digital certificates that are required for a digital signature under California law.
Digital Signature Provider	An entity that provides document signing services using digital technology.
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 electronic record.

**RATIONALE**

The Chico Area Recreation and Park District ("District") supports the use of digital signatures to improve efficiency and flexibility in its operations. When signatures are required, the District may accept digital signatures that comply with California Government Code Section 16.5 and are created using technologies authorized by the California Secretary of State. Use of digital signatures is voluntary for both the District and the signer, and acceptance remains at the District's discretion. This policy does not obligate the District to accept any digitally signed documents.

## **PROCEDURE**

### **Electronic Signatures**

The use of electronic signatures is authorized by two California statutes, the Uniform Electronic Transactions Act (“UETA”), codified at Civil Code Section 1633.1 et seq., and Government Code Section 16.5.

The UETA provides that a signature may not be denied legal effect or enforceability solely because it is in electronic form. The UETA applies to a transaction only when the parties have agreed to conduct the transaction by electronic means, which is determined based on the “context and surrounding circumstances, including the parties’ conduct.”

Government Code Section 16.5 applies to public entities such as the District, and authorizes any party to a written communication with a public entity, in which a signature is required or used, to affix a signature by use of a digital signature that complies with the requirements of Section 16.5.7 Digital signature transactions involving public entities that are subject to the UETA are also subject to the more particular requirements of Government Code Section 16.5.8 The use of a digital signature will have the same force and effect as the use of a manual signature if, and only if, the digital signature embodies the five attributes outlined below.

### **Digital Signatures**

Government Code Section 16.5 and State regulations require that a digital signature (i) be created by a technology deemed acceptable for use by the State of California and (ii) embody the following five attributes:

- 1) It is unique to the person using it;
- 2) It is capable of verification;
- 3) It is under the sole control of the person using it;
- 4) It is linked to data in such a manner that if the data are changed, the digital signature is invalidated; and
- 5) It conforms to regulations adopted by the Secretary of State, codified at Chapter 10 of Division 7 of Title 2 (commencing with Section 22000) of the California Code of Regulations.

### **Digital Signature Technologies**

The Secretary of State allows public entities to utilize digital signatures that are created using either “Public Key Cryptography” or “Signature Dynamics” technologies, provided that the digital signatures are also created consistent with the provisions of Section 22003 of the California Code of Regulations.

Public key cryptography (“PKC”) is a form of cryptography that generally allows users to communicate securely. PKC signatures are affixed to documents using software enhancements to existing applications and web browsers and are capable of immediate third-party verification.

## Policy 1060– Digital and Electronic Signature Policy

Signature dynamics use the individual's handwritten signature. Unlike PKC signatures, signature dynamics signatures require additional hardware to create the signatures. An electronic drawing tablet and stylus are used to record the direction, speed, and coordinates of a handwritten signature – essentially, taking a snapshot of a person's signature.

The District shall only contract with digital signature providers that offer their digital signature services with a certificate issued by a Digital Signature Certification Authority. District staff shall only accept digital signatures created by PKC or signature dynamics technologies. As advised by the Secretary of State, District staff shall consider the following issues and other issues when identifying the appropriate technology to use for each document that includes a digital signature component:

- Are the documents containing signatures going to be transmitted over an "open" or "closed" network?
- Does the signature on the document need to be verified?
- How much time and resources can be allocated to verification?
- Does the signature need to be compared to a manual signature on paper, or can a digital certificate adequately provide one-stop verification?
- Will immediate verifiability reduce the potential of fraud?
- Will the documents containing digital signatures need to be reproduced for public access to the records?
- Will the documents containing digital signatures need to be utilized by another local, state or federal agency? If so, is the technology compatible with the other agency's needs?

However, whenever a document requires immediate absolute verification of a signature, District staff shall only use and accept digital signatures by PKC technology.

---

---

**Authority:** General Manager; Board of Directors

---

---

Approved by the Board of Directors on: **12/11/2025**