**Policy # BRD-46-00**
**Effective Date 4/9/2020**

# Digital Signatures Policy

## 1.0 PURPOSE

The purpose of the Santa Clara Valley Open Space Authority's (Authority) Digital Signatures Policy (Policy) is to enable the use of digital signatures in compliance with applicable law.

## 2.0 APPLICABILITY

This Policy supplements the Authority's Cash Management Policy by authorizing staff to execute documents with a digital signature. This Policy does not create any new authorization for signing documents on behalf of the Authority, and only those authorized by Authority policies, including but not limited to the Cash Management Policy, may execute documents with a digital signature.

A digital signature satisfying the criteria below may be used for documents generated for official use by the Authority which require a signature. However, digital signatures may not be used if there is a specific federal or state statute or regulation, or Authority policy, that requires a document to be signed in non-electronic form.

The Authority will accept digital signatures from another party if such signatures satisfy the criteria below. However, the Authority retains the discretion to reject a digital signature and require a physical signature from another party when it deems appropriate or necessary.

## 3.0 CRITERIA FOR DIGITAL SIGNATURES

For a digital signature to be valid for use by the Authority, it must be created by DocuSign.

The Authority may recognize a digital signature from another party as having the same force and effect as a physical signature if all of the following requirements are met:

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 California Secretary of State.

## 4.0 RECORDKEEPING

The Authority shall maintain an electronic recordkeeping system that can receive, store, and reproduce digital signatures related to communications and transactions in their original form consistent with state law and the Authority's Record Management Policy. This recordkeeping system shall include security procedures whereby the Authority can achieve the following:

1. Verify the attribution of a signature to a specific individual;
2. Detect changes or errors in the information contained in the record that was submitted electronically;
3. Protect and prevent access, alternation, manipulation or use by an unauthorized person, and;
4. Accurately and completely reproduce digitally signed documents for later reference and retain such documents until such time as all legally mandated retention requirements are satisfied.
5. Provide for nonrepudiation through strong and substantial evidence that will make it difficult for the signer to claim that the electronic representation is not valid.

| | |
|---|---|
| **ID #** | BRD-046 |
| **Rev** | 00 |
| **Date** | April 9, 2020 |
| **Reso** | 20-16 |