Board of Directors Agenda Report

MEETING DATE: APRIL 23, 2020 **ITEM NUMBER:** 10C

SUBJECT: **Consideration of and Vote on Policy for the Use of e-Signatures**

DATE: April 17, 2020

FROM: Michele Richards, CEO

PRESENTATION BY: Michele Richards, CEO

RECOMMENDATION

At the Board of Directors' discretion.

BACKGROUND

The use of electronic signatures for contracts and agreements is permitted by the California Department of General Service pursuant to the development and approval of a policy by the Board of Directors for a particular State agency.

The current remote work situation due to the COVID-19 pandemic has created the need for the use of e-Signatures for a variety of administrative forms, agreements and contracts. Use of e-Signatures would greatly streamline administrative processes and avoid the need for employees to go into the office for signatures.

The attached policy, developed through the Attorney General's Office, is presented for the Board's consideration.

32nd District Agricultural Association

eSignature Policy

A. Purpose

This eSignature Policy ("Policy") shall be used by the 32nd District Agricultural Association ("District") to increase productivity and ensure convenient, timely and appropriate access to District information by using electronic signature technology to collect and preserve signatures on documents quickly, securely, and efficiently.

This Policy identifies the permissible types of electronic signatures ("eSignatures") and requirements for the use of eSignatures, automatic or electronic transactions, and electronic records (collectively, "e-records") in conducting District business operations. This Policy also establishes when electronic signature technology may replace a hand-written signature, with the goal of encouraging the use of paperless, electronic documents whenever appropriate and allowed by law.

This Policy applies to all signatures used in processing various District documents and assumes the District signer has been given the authority to sign as determined by the District, and where appropriate, the District's Board of Directors.

While the District suggests and encourages the use of electronic signatures, this Policy does not require the District to use electronic signatures, nor can the District mandate that any third party signing a document use an electronic signature.

B. Policy

The District permits the use of the following eSignatures, transactions and other record management activities in conducting District business:

1. **eSignatures**: The District may accept permissible types of eSignatures from all parties as legally binding and equivalent to handwritten signatures to signify an agreement. Each type of eSignature will include the date the document was signed. Where state or federal laws, regulations, or rules require a handwritten signature, that requirement is met if the document contains an eSignature unless otherwise prohibited by District policies or state or federal laws or regulations. Electronic documents must clearly and unambiguously show the chain of approval of all parties required to sign that document.

2. **Electronic Transactions**: Most purchase orders, contracts, and other contracting documents can now be executed electronically. The District may also accept bids, proposals, quotes, and offers with eSignatures at its sole discretion. Where required by the Department of General Services (DGS) or the State Contracting

Manual, the District will use eSignatures when transacting in the Fiscal Information System for California (FI$Cal).

3. **Recordkeeping Requirements**: An e-record may serve as the official copy of a procurement-related document. The District will maintain all relevant records, including e-records, in a reliable recordkeeping system. The District will also fully document all business conducted by electronic means to meet recordkeeping requirements, including procurement file documentation and information security requirements. The District will retain or dispose of records in accordance with District policy and state law.

4. **No eSignature Requirement**: The District may exercise at its discretion to conduct a transaction on paper or in non-electronic form. Furthermore, it does not affect the District's right or obligation to provide or make available paper documents when required by applicable policies, laws or regulations.

C. Background

Federal legislation known as the Electronic Signatures in Global and National Commerce Act made both electronic contracts and electronic signatures as legal and enforceable (with some exceptions) as traditional paper contracts signed in person. California then adopted the Uniform Electronic Transactions Act (California Civil Code, §§ 1633.1-1633.17), which establishes the legal validity of eSignatures and contracts in a manner similar to federal law. California law was revised to make clear that the state is authorized to use any type of eSignature. (See AB 2296 (Chapter 144, Statutes of 2016), effective 1/1/17.)

D. eSignature Requirements

The use of eSignatures is permitted and shall have the same force and effect as the use of a "wet" or manual signature if all the following criteria are met:

1. The eSignature is unique to the person using it.
2. The eSignature is capable of verification.
3. The eSignature is under the sole control of the person or entity using it.
    a. Email notifications requesting electronic signatures must not be forwarded.
    b. These requirements prohibit the use of proxy signatures.
4. The eSignature is linked to the data in such a manner that if the data is changed after the eSignature is affixed, the electronic signature is invalidated.

E. Types of eSignatures

The District's Information Technology Department will be responsible to determine acceptable technologies and eSignature providers consistent with current state legal requirements and industry best practices to ensure the security and integrity of the data and the signature. For illustrative purposes only, below is a non-exhaustive list of types of eSignatures.

1. **Name Types into a Document**: When signing a document electronically online, a showing of intent to enter into an agreement is required to create a binding electronic record. A document needs to be tied to the signature itself with a statement (e.g., "I agree" or "I accept") before typing in one's name. Simply providing a signature or signature block at the end of an email or electronic record without an indication of agreement will not be considered a legal signature under this policy. Note that certain standard agreement and purchase order forms (i.e., STD. 210, STD. 213, STD. 213A, STD. 215 and STD. 65) already contain sufficient indications of agreement and may be signed as written.

2. **FI$Cal Approvals**: Electronic forms (such as "Requisition") available in FI$Cal and some uploaded documents/forms can be approved electronically. These are approved electronic business transactions.

3. **Personal Identification Number (PIN) or password**: When using a PIN or password for an eSignature, a person accessing an application is requested to enter identifying information, which may include an identification number, the person's name and a "shared secret" (called "shared" because it is known to both the user and the system), such as a PIN and/or password. The system checks that the PIN and/or password is indeed associated with the person accessing the system and "authenticates" the person. Sometimes the entry of some personal information (e.g., name, date of birth or gender) along with the PIN and password is also required.

   For low risk or low value transactions, the person may define a PIN and/or password after supplying minimal identifying information that may or may not be verified. The strength of the password can provide additional security. Medium and high risk transactions often require a password consisting of a combination of letters, numbers, and special symbols at least eight (8) characters in length. The user might be forced to authenticate using a security token, a digital certificate, and/or a secondary password.

4. **Digitized Image of Hand Written Signature**: A digitized signature is a graphical image of a handwritten signature. Some applications require a person to create a handwritten signature using a special computer input device, such as a digital pen and pad. Digitized signatures are most often used in face-to-face consumer transactions using credit cards. Some applications can compare the digitized representation of the entered signature with a stored copy of the graphical image of the signature. A digitized signature may be another form of shared secret known both to the person and to the system. Forging a digitized signature can be more difficult than forging a paper signature because the technology that compares the submitted signature image with the known signature image is more accurate than the human eye.

5. **Biometrics**: Individuals have unique physical characteristics that can be converted into digital form and then interpreted by a computer. Among these are voice patterns, fingerprints, face recognition, DNA, palm print, gait analysis, hand geometry, retinal scanning, and/or iris recognition. In this approach, the physical characteristic is measured (by optical reader, microphone, or some other device) and converted into a digital form or profile. These measurements are compared to a profile of the given biometric stored in the computer and authenticated beforehand as belonging to a particular person. If the measurements and the previously stored profile match, the software will accept the authentication and the transaction is allowed to proceed.

6. **Digital Signatures**: There are two main types of digital signatures, one using Symmetric Cryptography and the other using Asymmetric Cryptography. The California Secretary of State requires certification of digital signatures only by entities that are on its approved list of Digital Signature Certification Authorities. See California Code of Regulations, Title 2, § 22003(a)(6)(B).

    a. **Shared Private Key (Symmetric) Cryptography**: In this eSignature method, a person electronically signs using a single cryptographic key that is not publicly known, for authentication purposes. The same key is used to sign a document and verify the signer's identity, and is shared between the signer and the entity hosting the transaction requiring the signature.

    b. **Public/Private Key or (Asymmetric Cryptography)**: To produce a digital signature, two mathematically linked keys are generated— a private signing key that is kept private, and a public validation key that is publicly available. The two keys are mathematically linked, but the private key cannot be deduced from the public key. The public key is often made part

of a "digital certificate," which is a digitally signed electronic document binding the individual's identity to a private key in an unalterable fashion. Digital signatures are often used within the context of a Public Key Infrastructure (PKI) in which a trusted third party known as a Certification Authority binds individuals to private keys and issues and manages certificates.

F. Storage and Archiving of Electronically-Signed Documents

The District maintains a written policy that designates responsibilities and describes methodologies that accurately document the overall management of the recordkeeping system. The recordkeeping policy is integrated into the District's business processes so that all records are immediately captured and are secure so as to always be easily recoverable by authorized staff. Only authorized District personnel shall be permitted and enabled to create, capture, or purge e-records. E-records should be accessible and retrievable in a timely manner throughout their retention period.

If a document exists only electronically, the District will ensure that a fixed version of the final document is stored in some manner. The District will store these final electronic documents in a manner consistent with any applicable document retention policies and any applicable laws.

G. Common Types of Documents

This Policy is intended to broadly permit the use of eSignatures. Examples of common types of documents are listed in the following table, with notes on each type of document. The District should work with the Office of the Attorney General or, where applicable, the Department of General Services or the Department of Food & Agriculture, to determine where applicable laws permit an electronic signature to be used.

Document Type Examples	In Use of an Electronic Signature Acceptable?	Notes
Memos, Forms, Board Letters, and Other Correspondence	Yes	Electronic Signature is recommended
Contracts	Yes	Electronic Signature is recommended
Documents Requiring Notarization	No	
Document Requiring the Board President's Signature	No	

H. Documents Involving Other Parties

In the case of contracts or transactions which must be signed by outside parties, each party to the agreement must agree in advance to the use of an electronic signature. No party to a contract or other document may be forced to accept an electronic signature; that party must be permitted to decide either way. Such consent may be withdrawn by the other party at any time such that future documents must be signed in hardcopy format.

When a document is electronically signed by all parties, the District will provide a copy of the electronically-signed document to the other parties in an electronic format that is capable of being retained and printed by the other parties.

I. Setup and Use

To setup employees authorized to send out documents for eSignature, the District's management team should contact the District's Information Technology Manager.

J. Conclusion

The use of eSignature is intended to make District business practices more efficient. The process eliminates the need to print, file, and store paper copies of documents that can now be authenticated digitally and stored electronically.

K. Definitions

Electronic relates to technology having electrical, digital, magnetic, wireless, optical, electromagnetic, or similar capabilities.

Electronic Record is a record created, generated, sent, communicated, received, or stored by electronic means.

Electronic Signature, or eSignature, means an electronic identifier, created by computer, attached or affixed to or logically associated with an electronic record, executed or adopted by a person with the intention of using it to have the same force and effect as the use of a manual signature.

Electronic Transaction is a transaction conducted or performed, in whole or in part, by electronic means or electronic records.

eSignature Product means a software or service that provides a means of affixing an Electronic Signature to an electronic record.

Proxy Signatures are when Person-A authorizes Person-B to sign Person-A's signature on his/her behalf. (This is prohibited for eSignatures by this policy.)

Record is information that is inscribed on a tangible medium or that is stored in an electronic or other medium and is retrievable in perceivable form. Documents or forms are records.