MANAGEMENT MEMO

NUMBER:
MM 18-03

SUBJECT:

ELECTRONIC SIGNATURES, ELECTRONIC TRANSACTIONS AND ELECTRONIC RECORD MANAGEMENT POLICY

DATE ISSUED:
May 4, 2018

EXPIRES:
UPON INCORPORATION INTO SAM OR MAY 1, 2019

REFERENCES:
STATE ADMINISTRATIVE MANUAL: CHAPTER 1600 et seq; STATE CONTRACTING MANUALS VOLUMES 1 (Chs. 7.50, 9.09), 2 AND 3 (Ch.11) and FI$Cal (Ch. 9); CIV Secs.1633.1-1633.17, 1633.5); CCR Title 12, Sec 22003(a)(6) (B); AB 2296, CHAPTER 144, STATUTES of 2016

ISSUING AGENCY:
DEPARTMENT OF GENERAL SERVICES

Purpose

This policy identifies the permissible types of E-Signatures and requirements for the use of electronic signatures (hereafter "e-signatures" or e-sign), automatic or electronic transactions, and electronic records (hereafter "e-records") in conducting state business operations.

Policy

The Department of General Services permits the use of the following Electronic Signatures, Transactions and Record Management activities in conducting state business:

E-Signatures: State agencies may accept permissible types of e-signatures from all parties as legally binding and equivalent to handwritten signatures to signify an agreement. Each type of e-signature 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 e-signature unless otherwise prohibited by policies, laws or regulations. [1] Electronic documents must clearly and unambiguously show the chain of approval of all parties required to sign that document.

Electronic Transactions: Most purchase orders, contracts, and other contracting documents can now be executed electronically. State agencies may also accept bids, proposals, quotes, and offers with electronic signatures at their discretion.

In some cases, state agencies are required to use electronic signatures when transacting in the Fiscal Information System for California (FI$Cal). Conversely, some documents will still need to be submitted to DGS in paper format for the time being, due to technical limitations. These requirements will change over time as technology adoption improves.

DGS will maintain current guidance on transactions that must be conducted electronically, and on documents that must be submitted to DGS in paper format, in the State Contracting Manual.

Continued on next page

[1] Users are to remember that appropriate security policies must be followed.

Policy (Cont.)

Recordkeeping Requirements: An e-record may serve as the official copy of a procurement-related document. All relevant records, including e-records, shall be maintained in a reliable recordkeeping system. Business conducted by electronic means shall be fully documented to meet recordkeeping requirements, including procurement file documentation and information security requirements. Records shall be retained or disposed of in accordance with the approved records retention schedules stated in California State Records and Information Management (CalRIM) as supported by the State Contracting Manual (SCM) and the State Administrative Manual (SAM) 1600 et seq.

Scope

This policy applies to all transactions governed by the State Contracting Manual (all volumes) and/or conducted by the Department of General Services (DGS) Procurement Division. This policy enables state agency staff to conduct many transactions electronically, to accept e-signatures by other parties, and to sign agreements on the agency's behalf by using an e-signature. This policy does not waive or modify any requirement or limitation as to which officers and employees are authorized to bind their agency to a contract.

Use of E-Signatures is Generally Optional

Except in cases where DGS has specifically required a type of transaction or document to be executed electronically, accepting e-signatures or maintaining e-records is not mandatory under this policy. Each state agency may exercise at its discretion to conduct a transaction on paper or in non-electronic form. Furthermore, it does not affect a state agency's right or obligation to have documents be provided or made available on paper when required by applicable policies, laws or regulations.

Background

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

E-Signature Approvals

When an electronic document is emailed to DGS, the chain of approval of all those required to sign that document must be clear and unambiguous. All parties required to sign must have unequivocally approved the same document. For example: to demonstrate all approvers sign the same NCB Justification, a. PDF copy of that NCB must be emailed to DGS with a legally binding signature from each approver attached, and all approvers must be copied on the email.

There may be instances where the submission of an electronic document is unclear and more substantiation will be required by DGS.

A valid electronic document must include an email trail that includes all approvers. Each approval must be clear and unequivocal.

The following statement is an example of a clear and unequivocal approval:

> "I approve the attached document [specify document name, number or other specific document ID]."

The following statement is not an example of a clear and unequivocal approval:

> "I approve if specified revisions are made to #3 and #9."

History of Approvals and Corrections Required: A chain of approval demonstrates a history of approvals for the electronic document. If corrections are necessary, an email with the requisite "I approve the attached revised document [specify document name, number or other specific document ID]" is needed.

It must be clear that each approver has approved the same document and that document is attached. The chain of approval must be attached to the submission email and the approvers must also be copied on the email (with subject document attached) sent to DGS. By law or policy, some approvers are enabled to authorize others (designees) to sign on their behalf. An approval of a document by an authorized designee is acceptable; however both the requisite approver and his/her designee must be copied on the email sent to DGS.

Electronic approvals made through FI$Cal meet the approval chain requirements.

Types of E-Signatures Permitted for Use by State Agencies

Only the following types of e-signatures (further defined below) can be used by state agencies.

- A typed name
- FI$Cal approvals
- A recorded voice
- Personal Identification Number (PIN)
- Password (composed of numbers, symbols and/or alpha characters
- Digitized image of handwritten signature (e.g. PDF copy of Word document
- Identification number created using a number generator
- Digital Signature

Electronic Record Management

Each state agency will maintain a written policy that designates responsibilities and describes methodologies that accurately document the overall management of the recordkeeping system. The recordkeeping policy should be integrated into the state agency'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 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.

Recommendations for Implementation

Each state agency should work with its management, legal counsel, Information Security Officer (ISO), and Privacy Officer to implement e-signature policies including:

- Identify which transactions (if any) it does not want to execute with -signatures;
- Consider whether to adopt a uniform department-wide e-signature methodology, set parameters for using different methodologies, or establish different rules for various divisions;
- Determine what level(s) of authority can execute e-signatures;
- Decide what dollar levels will require e-signatures by which level(s) of authority;
- Implement requisite security and privacy protection procedures;
- Obtain an approval from ISO and AISO (Agency ISO) if applicable, on the security controls for signed documents.
- Create and periodically update a list of positions and/or personnel authorized to execute e-signatures;
- Designate backups in case of unavailability of authorized signatories;
- Maintain a database of e-signed transactions, which can be reviewed for transaction type, dollar amount, contract length, names of signatories, and level of authority of signatories;

Continued on next page

Recommendations for Implementation (Cont.)

- Document problems encountered with e-signatures (e.g., contractual disputes, unauthorized expenditures, missing transactions, unwilling vendors, overeager signatories, internal resistance, training problems, security issues, oversight concerns, etc.);
- Review database and documented problems after a trial run (e.g., six months of e-signatures) and adjust departmental e-signature practices as appropriate;
- Revise departmental records management policy as needed to ensure retention of e-signed transaction records for the required length of time.

Definition of Key Terms

E-signature involves a number of key terms which are defined in CIV Section 1633.2, including:

- **Automated transaction** means a transaction conducted or performed, in whole or in part, by electronic means or electronic records, in which the acts or records of one or both parties are not reviewed by an individual in the ordinary course in forming a contract, performing under an existing contract, or fulfilling an obligation required by the transaction.
- **Electronic** means relating to technology having electrical, digital, magnetic, wireless, optical, electromagnetic, or similar capabilities.
- **Electronic agent** means a computer program or an electronic or other automated means used independently to initiate an action or respond to electronic records or performances in whole or in part, without review by an individual.
- **Electronic record** means a record created, generated, sent, communicated, received, or stored by electronic means.
- **Electronic signature** means 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. For purposes of this title, a “digital signature” as defined in subdivision (d) of Section 16.5 of the Government Code is a type of electronic signature.
- **Information** means data, text, images, sounds, codes, computer programs, software, databases, or the like.
- **Record** means information that is inscribed on a tangible medium or that is stored in an electronic or other medium and is retrievable in perceivable form.
- **Security procedure** means a procedure employed for the purpose of verifying that an electronic signature, record, or performance is that of a specific person or for detecting changes or errors in the information in an electronic record. The term includes a procedure that requires the use of algorithms or other codes, identifying words or numbers, encryption, or callback or other acknowledgment procedures.
- **Transaction** means an action or set of actions occurring between two or more persons relating to the conduct of business, commercial, or governmental affairs.

Continued on next page

Additional Terms

In addition to the definitions provided by law, understanding what an e-signature requires understanding several other key terms:

- **Wet** or **original** signature is created when a person physically writes a name in a stylized, cursive format (or even a simple "X") on a piece of paper.
- **User Authentication** is the process of securely verifying the identity of an individual prior to allowing access to an electronic service.
- **User Authorization** involves verifying that an authenticated user has permission to access specific electronic services and/or perform certain operations.

Permissible Types of E-Signatures Explained

The permissible types of e-signatures are explained below.

- **Name Typed 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. Note: 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 Also: 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.

- **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.

- **Recorded Voice**: While a voice recording could be considered an electronic signature, simple voice recordings may not establish intent of agreement. Many voice systems include an additional step such as keypad verification to confirm agreement. To use a recorded voice as an e-signature, it must:
    - Be associated with the speaker;
    - Be associated with a specific document or record;
    - Show evidence of the speaker's intent to be bound to the terms and conditions in that specific document or record;
    - Be captured in electronic format.

Continued on next page

Permissible Types of E-Signatures Explained (Cont.)

- **Personal Identification Number (PIN) or password:** When using a PIN or password for an e-signature, 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.

- **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.

- **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.

Continued on next page

Permissible types of ESignatures Explained (Cont.)

- **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 has required that digital signatures can only be certified by entities that are on its approved list of Digital Signature Certification Authorities. See California Code of Regulations, Title 2, § 22003(a)(6)(B).
    - **Shared Private Key (Symmetric) Cryptography:** In this e-signature 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.
    - **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.

Contact

Questions concerning this policy may be directed to:

Matt Bender
Office of Legislative Affairs
Department of General Services
916-376-5008
Matt.Bender@dgs.ca.gov

Signature

Daniel C. Kim, Director
Department of General Services

05/04/2018

Date