ADMINISTRATIVE MEMORANDUM

COUNTY OF SAN MATEO

NUMBER: B-29

SUBJECT: Electronic and Facsimile Signatures

RESPONSIBLE DEPARTMENT: County Manager

APPROVED: _____ **DATE:** July 1, 2013
John L. Maltbie, County Manager

Purpose

This policy establishes when an electronic or facsimile signature may replace a hand-written (wet) signature, with the goal of encouraging the use of paperless, electronic documents whenever appropriate. This policy applies to all signatures used in processing independent contracts and requests for proposals as well as internal communications, routing slips, external correspondence, and other official activities. However, this policy does not require any department to use electronic signatures.

Background and Definitions

An electronic signature is defined as a signature entered into a computer by an authorized person with the intent to show authorship or to sign a record for approval, acceptance, or certification. Electronic signatures can be created through various means, and often a document with an electronic signature does not have a corresponding hardcopy "original" version—the electronic file with the signature is the "original" of the document. The creation of electronic signatures can be as simple as pasting a scanned image of a signature into a Microsoft Word document or can be as robust as affixing an electronic signature which includes certain security protections using a program like Adobe Acrobat in order to prevent any future changes to the electronically-signed document. Use and/or acceptance of electronic signatures for creating and processing documents expedites processing time, can facilitate document storage, and can have positive cost and environmental impacts.

A facsimile signature is defined as a signature that is copied or scanned from a document bearing an authorized original signature. Under California law, a document bearing a facsimile signature is equivalent to the original copy in most situations unless an original signature is required by law. A facsimile signature can be created when a document is copied on a copy machine, when it is scanned, or when it is transmitted via a facsimile (fax) machine.

Policy

This policy applies to any document requiring the signature of any employee where the signature is intended to show authorship, approval, authorization, or certification. It is the policy of the County to encourage the use of electronic signatures in all internal and external activities, documents, and transactions where it is operationally feasible to do so, where existing technology permits, and where it is otherwise appropriate based on the Department's preferences. In such situations, affixing an electronic signature to the document in a manner consistent with this policy and memorandum shall satisfy the County's requirements for signing a document. As used in this policy, the term "signature" includes using initials on a document instead of a signature.

It is also the policy of the County to accept use of a facsimile signature in lieu of an original (wet) signature. There is no longer a preference for obtaining original/wet signatures from vendors on signed copies of contracts, although each Department has discretion to require submission of an original/wet signature.

A. Department Discretion

Each Department has discretion to decide whether to permit use of electronic or facsimile signatures. In addition, each Department that opts to use electronic or facsimile signatures must adopt practices that satisfy the requirements of this memo.

B. Common Types of Documents

This memo is intended to broadly permit the use of electronic or facsimile signatures. The most common types of documents are listed in the following table, with notes on each type of document. For more information, please access the County's Intranet guidance regarding electronic signatures at: http://intranet.co.sanmateo.ca.us/

Document Type	Is Use of an Electronic Signature Acceptable?	Notes (if an electronic signature is used)
internal/external memos, Board memos, normal letters/ correspondence	Yes	The signature does not need to have added security features for these purposes, but the Department *may* use a Secure Electronic Signature as outlined by this memo.

Document Type	Is Use of an Electronic Signature Acceptable?	Notes (if an electronic signature is used)
Service contracts above $100,000	Yes	The County Manager, as Clerk of the Board, will set guidelines for the County's signatures. Signatures from vendors can be electronic, facsimile, or original/wet (if electronic, the vendor should be encouraged to create a document as secure as possible).
Board Resolutions, Ordinances, and other items	Yes	The County Manager, as Clerk of the Board, will set guidelines for the County's signatures.
Service contracts below $100,000	Yes	The Department Head or designee *must* use a Secure Electronic Signature as outlined by this memo in order to protect the Department Head's signature authority; the Contract Requestor may but is not required to use a Secure Electronic Signature to sign the agreement. Signatures from vendors can be electronic, facsimile, or original/wet (if electronic, the vendor should be encouraged to create a document as secure as possible, but no specific format is required unless the Department has a preference).
Financial Documents	Yes, if allowed by law	The Department should work with County Counsel to determine where applicable laws permit an electronic signature to be used.

Document Type	Is Use of an Electronic Signature Acceptable?	Notes (if an electronic signature is used)
HR-related Items, Employee Reviews	Yes	If an employee requests that an item be signed in hardcopy format, the Department should issue the item in that format. If an employee is required to sign something, a hardcopy signature is generally preferable, but the document may be scanned and then stored electronically.
Certificates, permits	Yes, if allowed by law	The Department should work with County Counsel to determine where applicable laws permit an electronic signature to be used.
Legal Items (Declarations, Court filings, items requiring notarization)	Yes, if allowed by law	The Department should work with County Counsel to determine where applicable laws permit an electronic signature to be used.

C. Documents Involving Other Parties

Where another party is involved as a recipient of a document, the Department should work with County Counsel to ensure that the document may be signed electronically.

In the case of contracts or transactions which must be signed by multiple parties, each party to the agreement must agree in advance to permit the use of an electronic signature by the County. The County Manager will be providing updated Contractor's Declaration for allowing the contractor to indicate whether it consents to the County's use of an electronic signature. No party to a contract or other document should be forced to accept an electronic signature from the County—they 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, although another party cannot withdraw consent for the use of an electronic signature that has already been provided pursuant to the party's original authorization.

Vendors may be encouraged to sign a contract or transaction electronically when the document is submitted to the County. When an electronic signature is transmitted to and received by the County from another party, the Department should ensure with a reasonable degree of certainty that the sender's signature has not been forged. For example, the Department can be in telephone or email communication with a trusted contact from the other side, and the signature can be compared against prior examples if one is available. The Department must also assure with a reasonable degree of certainty that a document and its signature have not been changed after it has been signed. Again, this can be done by having the Department communicate with the other side to ensure that the final version has been sent in a format that does not permit edits, as outlined below.

When a final document is electronically signed by all parties, the County should 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. The Department may also provide a hardcopy version of the final document if requested by the other parties.

D. Security Controls

As noted above, there are various methods by which a document may be signed in electronic format. Certain documents do not require added security, in which case they may be signed electronically in any format so long as the Department complies with the archiving requirements listed below.

In relation to documents which require added security, the term "Secure Electronic Signature" means an electronic signature that meets all of the following criteria:

1. The electronic signature must be **unique** to the person using it. The Department should maintain a copy of the signature to ensure that it is unique to the person using it. A copy of the signature should be kept on file using the Electronic Signature Documentation Form, available on the Intranet. These forms should be kept by the Department.

2. The electronic signature must be **capable of verification**. This means that the technology being used permits the signature's authenticity to be verified. Use of a program like Adobe Acrobat to add a digitally-encrypted signature meets this requirement. However, simply pasting a signature image into a Word or PDF file without other security does not meet this requirement since the image can be forged.

3. The electronic signature must be under the **sole control** of the person using it. This means that only the person whose signature

is being affixed *or* specific staff members authorized in writing by that person to affix the signature on their behalf (a "Signature Proxy") shall have the ability to affix the signature. Any password or private key used to create the electronic signature must be kept confidential by the person and any Signature Proxy. If a County employee wishes to permit another County employee to act as a Signature Proxy, the County employee and each person authorized to submit the signature must complete the Electronic Signature Proxy Authorization Form, available on the Intranet. In addition, the Department is encouraged to adopt its own policies making clear when a Signature Proxy is permitted to sign a document on someone's behalf. Some sample language for policies relating to use of a proxy is available on the electronic signature website listed at the end of this memo. These forms should be kept by the Department.

4. The electronic signature must be **linked to the data** in the document in such a manner that if the data are changed, the digital signature is invalidated. Again, use of a program like Adobe Acrobat to add a digitally-encrypted signature meets this requirement.

Any County employee that makes inappropriate, unauthorized, or illegal use of an electronic signature and/or records (regardless of whether the signature is a regular electronic signature or a Secure Electronic Signature) is subject to disciplinary action up to and including dismissal, suspension, and criminal prosecution.

E. Storage and Archiving of Electronically-Signed Documents

If a document exists only electronically, there is a risk that the document can be modified intentionally or inadvertently without keeping a record of the intended "final" version of the document. In addition, there is a risk that the final version of the document can be lost if it is not kept in a safe location. Accordingly, steps should be taken by each Department to ensure that a fixed version of the final document is stored in some manner, with preference given to electronic storage of a document. For example, the following methods of electronically securing the final version of a document are acceptable, starting with the more preferable (secure) methods: creating a final PDF that includes an encrypted signature which "breaks" if the document is modified; creating a PDF that is otherwise not editable; scanning in a hardcopy which is signed; or saving a native file (Word) that is locked to prevent future changes.

It is up to the Department to decide how to store these final electronic documents so long as it does so in a manner consistent with any applicable County document retention policies. Storage options include the following: saving the document on a network drive (preferably one that is automatically backed up);

saving the document in a County-provided electronic filing system (such as Autonomy); or emailing a copy of the final document to someone who will then retain the email and attached document (but email is not a preferred method for long-term storage). Departments should not rely on storing electronic documents on a local (C:) drive since the local drive may fail. In addition, use of portable media such as a memory stick/USB drive or CD is discouraged in general given the ease with which such items can become lost or damaged. If electronic storage is not possible, a copy of the final document should be kept and stored in hardcopy format.

For archiving of electronic documents beyond normal storage, Departments should ensure documents are archived in a manner that is consistent with any applicable County document retention policies.

F. Privacy Controls

Because it is possible to use an electronic signature to easily create a forged copy, caution should be used when posting an electronic signature on any public-facing Internet site or other medium. In such situations, the Department should consider redacting all signatures (whether representing the County or any other party) in order to minimize making the signature itself widely available. The redaction should generally include some kind of statement such as "redacted" or "redacted to maintain privacy" or "original signature on file" or "original signed by <<person name or title>>".

G. Acceptable Technologies & Additional Information

Given the complex nature and ongoing evolution of signature technologies, the County Manager will create an internal webpage with information about this memo and policy. That site will include a description of technologies that meet the requirements of this memo, instructions on how to use such technologies to create a Secure Electronic Signature, copies of the Electronic Signature Documentation Form and Electronic Signature Proxy Authorization Form, a list of frequently asked questions, and copies of sample documents.

For more information, go to:
http://intranet.co.sanmateo.ca.us