

F-2 ELECTRONIC SIGNATURE USE POLICY



Inception Date: 06/25/2019

Revision Date: NEW

By: CAO/ACO/DoIT/County Counsel

Page: 1 of 5

2.1.0 PURPOSE

- 2.1.1 The Countywide Electronic Signature Use Policy shall be used by Solano County to increase productivity and ensure convenient, timely and appropriate access to County information by using electronic signature (eSignature) technology to collect and preserve signatures on documents quickly, securely, and efficiently. In addition to increasing productivity and efficiency, this Policy furthers the County's paperless initiative goal by reducing the consumption and storage of paper documents and the maintenance and supply of printers.
- 2.1.2 This Policy establishes when eSignature 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 County documents and assumes the County signer has been given the authority to sign as determined by Department business process.
- 2.1.3 While the use of eSignatures is suggested and encouraged, this Policy does not require any Department to use eSignatures, nor can the County mandate that any third party signing a document use eSignature.

2.2.0 LEGAL AUTHORITY

- 2.2.1 Electronic Signature is the broad umbrella category under which all eSignatures fall.
- 2.2.2 The legality and use of eSignatures are governed by federal and State law. (See 15 United States Code, section 7001, *et seq.* [U.S. Federal Electronic Signatures in Global and National Commerce Act]; California Government Code, section 16.5; California Civil Code, section 1633.1, *et seq.*)

2.3.0 INTENDED GOALS FOR ESIGNATURE

- 2.3.1 Security and Legal Compliance: The use of eForms and eSignatures provides a secure method of signing and transferring documents electronically. Any alterations to an electronically signed document invalidate the signature. Therefore, an electronically signed document can be considered more secure and verifiable than a traditionally signed document. Additionally, a history of any changes made to the document prior to the signature is kept with the document and cannot be changed or deleted. When eSignatures are used, hash values are attached to the document to verify the authenticity of a document during any transfer for added security.
- 2.3.2 Integration into Business Processes: The eSignature process may fit into pre-existing business practices, provide automated processes, retrieve documents, use standard Application Program Interfaces (API), generate reminders and expiration settings, and allow multiple people to view a document and track its progress.

F-2 ELECTRONIC SIGNATURE USE POLICY



Inception Date: 06/25/2019

Revision Date: NEW

By: CAO/ACO/DoIT/County Counsel

Page: 2 of 5

2.3.3 Simplified Workflow: eSignatures eliminate resource-intensive processes that require agencies, the public, and staff to manually sign documents. Features of the eSignature process include automation of simple forms, ability to track and review changes, vary the recipient roles, tag signatures, etc.

2.3.4 Cost Benefits: There is a potential cost-savings from not having to print, file, scan, and store paper copies. The County will also save on certified mail, postage, printing, ink, envelopes, and paper.

2.4.0 POLICY

2.4.1 This Policy applies to any document requiring a signature of any person where the signature is intended to show authorship, approval, authorization, or certification, as allowed by law. It is the Policy of the County to encourage the use of eSignatures 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 eSignature to the document in a manner consistent with this Policy 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 as well as any auditable system transaction that requires user authentication and records a date stamp.

2.5.0 DEPARTMENT DISCRETION

2.5.1 Each Department has discretion to decide whether to permit the use of eSignatures. Departments should work with County Counsel to determine where applicable laws permit an eSignature to be used. In addition, each Department that opts to use eSignatures must adopt/amend their business practices to support the requirements of this Policy.

2.6.0 REQUIREMENTS OF ESIGNATURE

2.6.1 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:

- A. The eSignature is unique to the person using it.
- B. The eSignature is capable of verification.
- C. The eSignature is under the sole control of the person using it.
 - 1. Email notifications requesting eSignatures must not be forwarded.
 - 2. These requirements prohibit the use of proxy signatures.

F-2 ELECTRONIC SIGNATURE USE POLICY



Inception Date: 06/25/2019

Revision Date: NEW

By: CAO/ACO/DoIT/County Counsel

Page: 3 of 5

- D. The eSignature is linked to the data in such a manner that if the data is changed after the eSignature is affixed, the eSignature is invalidated.

2.7.0 COMMON TYPES OF DOCUMENTS

- 2.7.1 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 examples are provided for illustration purposes only. Departments should work with County Counsel to determine where applicable laws permit an eSignature to be used.

Document Type Examples	Is Use of an Electronic Signature Acceptable?	Notes
Memos, Forms, and Other Correspondence	Yes	Electronic Signature is recommended.
Contracts	Yes	Electronic Signature is recommended.
Certificates, Permits	Yes, if allowed by law	Departments should work with County Counsel to determine where applicable laws permit an eSignature to be used.
Documents Requiring Notarization	No	
Document Requiring the Board Chair's Signature	No	

2.8.0 DOCUMENTS INVOLVING OTHER PARTIES

- 2.8.1 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 eSignature. No party to a contract or other document may be forced to accept an eSignature; 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.
- 2.8.2 When a document is electronically signed by all parties, the County 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.

F-2 ELECTRONIC SIGNATURE USE POLICY



Inception Date: 06/25/2019

Revision Date: NEW

By: CAO/ACO/DoIT/County Counsel

Page: 4 of 5

2.9.0 SETUP & USE

2.9.1 To setup employees authorized to send out documents for eSignature, authorized department staff shall initiate a service request through the Department of Information Technology's help desk.

2.9.2 All County users of eSignature technology shall conform to the rules set forth in the *Solano County Information Technology Acceptable Use Policy*.

2.10.0 STORAGE AND ARCHIVING OF ELECTRONICALLY-SIGNED DOCUMENTS

2.10.1 If a document exists only electronically, steps should be taken by each Department to ensure that a fixed version of the final document is stored in some manner. 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 and any applicable laws.

2.11.0 ESIGNATURE SOLUTION PROVIDERS

2.11.1 The Solano County Department of Information Technology 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.

2.12.0 CONCLUSION

2.12.1 The use of eSignature is intended to make Solano County 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. This Policy is intended to be broadly interpreted to allow for the use of eSignatures whenever legally applicable to County business needs.

2.13.0 DEFINITIONS

2.13.1 "Application Program Interface (API)" is a set of clearly defined methods of communication between various software components. API's allow applications to interact with each other, allowing integration of one system with another.

2.13.2 "Digital Signature" is a specific signature technology implementation of eSignature that uses cryptography to provide additional proof of the identity of a signer and integrity of a document. This cryptography uses Public Key Infrastructure (PKI) technology to issue digital certificates. PKI technology is accepted by the California Secretary of State for digital signatures created by a public entity.

F-2 ELECTRONIC SIGNATURE USE POLICY



Inception Date: 06/25/2019

Revision Date: NEW

By: CAO/ACO/DoIT/County Counsel

Page: 5 of 5

- 2.13.3 “Electronic” relates to technology having electrical, digital, magnetic, wireless, optical, electromagnetic, or similar capabilities.
- 2.13.4 “Electronic Record” is a record created, generated, sent, communicated, received, or stored by electronic means.
- 2.13.5 “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.
- 2.13.6 “Electronic Transaction” is a transaction conducted or performed, in whole or in part, by electronic means or electronic records.
- 2.13.7 “eSignature Product” means a software or service that provides a means of affixing an eSignature to an electronic record.
- 2.13.8 “Hash Value” is a unique numerical identifier that can be assigned to a file, a group of files, or a portion of a file, based on a standard mathematical algorithm applied to the characteristics of the data set. The numerical identifier is so distinctive that the chance that any two files will have the same hash value, no matter how similar they appear, is less than one in one billion. ‘Hashing’ is used to guarantee the authenticity of an original file.
- 2.13.9 “Permitted Transactions and Notices” means electronic transactions and notices for which the use of eSignatures is not prohibited under applicable law.
- 2.13.10 “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.)
- 2.13.11 “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.