# INCORPORATED COUNTY OF LOS ALAMOS
# ADMINISTRATIVE PROCEDURE GUIDELINE

Index No. 1220 Effective: October 1, 2013

## E-SIGNATURE POLICY

I. Purpose

This policy is to allow for e-signature use at LAC by means of methods that are practical, secure, and balance risk and cost. It is not the intent of this policy to eliminate all risk but rather to provide a process that gives parties assurance that appropriate analysis was completed prior to implementation of e-signature, and that the level of user authentication used is reasonable for the type of transaction conducted.

A. Electronic Signatures Acts

Both federal and state law address electronic signatures and give electronic contracts the same weight as those executed on paper. The federal act is known as the "Electronic Signatures in Global and National Commerce Act," (Act) and is found at 15 U.S.C. Sections 7001-7006, 7021 & 7031. The New Mexico act is known as the "Uniform Electronic Transactions Act," and is found at Sections 14-16-1 through 14-16-19, N.M.S.A. (1978). Links to these statutes are provided below. All references herein are to the New Mexico act unless otherwise specified. The act has some specific exemptions or preemptions. *Although the act enables documents to be signed electronically, the ability to do so arises only when both parties agree to conduct transactions by electronic means. Any LAC department using E-signatures shall also provide methods for conducting transactions with its customers that do not require E-signatures in the event the customer declines to agree to such to conduct transactions by electronic means.* The act specifically avoids stipulating any 'approved' form of electronic signature, instead leaving the method open to interpretation by the marketplace. Any number of methods is acceptable under the act. Methods include simply pressing an *I Accept* button, digital certificates, smart cards and biometrics.

E-signatures may be implemented using various methodologies depending on the risks associated with the transaction. Examples of transaction risks include: fraud, repudiation, authentication, hacking, security and financial loss. The quality and security of the e-signature method shall be commensurate *with the risk and needed assurance of the authenticity of the signer. Authentication is a*

*way to ensure that the user who attempts to perform the function of an electronic signature is in fact who they say they are and is authorized to "sign".*

II. Policy

A. It is the policy of LAC that every user shall have unique identifying credentials. Authentication entails verifying the user's unique credentials, such as username and password, or a digital certificate.

B. Under this policy LAC departments may implement use of e-signatures, but shall also maintain alternative processes available for any consumer who declines to conduct transactions by electronic means. The LAC department is the organization conducting business by means of an e-signature. Implemented e-signatures will be reviewed periodically for appropriateness, and continued applicability.

C. An e-signature may be accepted in all situations if requirement of a signature/approval is stated or implied. This policy does not supersede situations where laws specifically require a written signature or where a party declines to conduct transactions by electronic means.

III. Responsibility

A. Security and access to LAC specific information is determined by the Access Control Authority (ACA) for the electronic system. ACA's shall have the ability to develop enabling procedures and are responsible for compliance with all legal obligations related to information, as well as determining the utilization, access, and release of data under their jurisdiction. ACA's are a representative from the requesting department or other designated representative (i.e., IT liaison, TAG representative). In some instances there are multiple ACA's for various systems. The ACA will ensure that appropriate controls and monitoring of required software/hardware required for implementation are in place.

B. LAC departments shall complete LAC risk assessment tool (E-Signature Authentication Request Process) and shall describe the reason for risk, identify the steps that will be taken to mitigate the risk and obtain the signed approval of the County Administrator. LAC departments shall conduct periodical reviews of every implementation, no less than every three years, which will include an evaluation of the e-signature use to determine whether any applicable legal, business, or data requirements have increased the risk of the e-signature implementation.

C. The Information Management Division (IMD) shall assist LAC department ACA's in preparation of their application and provide technological expertise (i.e., IT liaison).

D. III.4. The ACA may, after consultation with the County Attorney, reject any E-Signature application deemed in violation of or failing to meet statutory or regulatory requirements. The ACA, after consultation with the County Attorney, shall establish specifications for recording, documenting, and/or auditing the e-signature as required for non-repudiation and other legal requirements.

E. The County Administrator shall review and have final approval of each e-signature application.

F. Records Information Management (RIM) shall retain a formal record of the risk assessment evaluation, e-signature method selection, and justification.

IV. Procedure

The E-Signature Authentication Request Process tool outlines the process required by a department to apply for an e-signature implementation and shall address known identified risks.

A. An evaluation will be performed by the ACA to identify risks associated with using an e-signature and to determine the quality and security of the e-signature method required. An evaluation will be made using the E-Signature Authorization Request Process tool. The reports resulting from the assessment shall be included as part of the official record for this e-signature implementation and submitted with the proposal.
B. Requests for LAC e-signature transactions shall be evaluated by the ACA in conjunction with IMD, who will determine whether to recommend an e-signature method for approval, by understanding the systems and procedures associated with using that electronic signature, and whether the use of the electronic signature is at least as reliable as the existing method being used. The IMD review will include process, security and records review with a recommendation to the department on whether or not to proceed.
C. The ACA will request a review of the application from the County Attorney. Once that review has been completed and recommendation to proceed has been granted, the ACA will seek authorization to implement e-Signature from the County Administrator.
D. The signed document shall be included as part of the official record for this e-signature implementation.
E. Once approved, the implementation process will likely differ for each transaction and for each LAC department or affiliated body, as it is dependent on many factors such as records management requirements, technical environment, appropriate assurance level, and the nature of the transaction.
F. Software and/or hardware required for e-signatures, such as Public Key Infrastructure (PKI) certificates, "fobs", or "dongles", or other credential devices shall be purchased by the department or affiliated body.
G.

V. Resources and Links

A. Electronic Signatures in Global and National Commerce Act (ESIGN):

http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=106_cong_public_laws&docid=f:publ229.106.pdf

B. NIST Electronic Authentication Guidelines: 800-63;

http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf

C. Electronic Signatures in Global and National Commerce Act, 15 U.S.C. Sections 7001-7006, 7021 & 7031; http://uscode.house.gov/download/pls/15C96.txt

D. Uniform Electronic Transactions Act, Sections 14-16-1 through 14-16-19, N.M.S.A. (1978); http://www.conwaygreene.com/nmsu/lpext.dll?f=templates&fn=main-h.htm&2.0

## VI. Definitions

| | |
|---|---|
| **Access Control Authority (ACA)** | Department representative, or designee, who understands the data and manages the request for e-signature application process and implementation. |
| **Affiliated Body** | Board or Commission who act on behalf of a LAC Department. |
| **Authentication** | A method to ensure that the user who attempts to perform functions in a system is in fact the user who is authorized to do so in order to ascertain the identity of the originator, verify the integrity of the electronic data and establish the link between the data and the originator. |
| **Electronic Record** | Computer-generated information such as an e-mail message, document or image file created or received by the County in pursuance of law or in connection with the transactions of public business. |
| **Electronic Signature (E-Signature)** | The electronic signing of a document consisting of establishing a verifiable link between the originator and the document using an electronic sound, symbol, or process attached to or logically associated with a record and execute or adopted by a person with the intent to sign the record. |
| **Non-repudiation** | Specific identification of a user plus the need to specifically link the user to a transaction; i.e., to prove that the user intended to be bound by the transaction. |
| **Record** | Information that is inscribed on a tangible medium or that is stored in an electronic or other medium and is retrievable in a perceivable form. |
| **TAG (Technology Advisory Group)** | This group provides technological oversight to LAC and any member thereof may act as an ACA. |
| **Transaction** | Specific actions that users can perform to achieve a desirable result. A transaction is an actor, plus an action, resulting in a desired outcome. |

HARRY BURGESS — DATE
COUNTY ADMINISTRATOR