LUCAS COUNTY, OHIO **BOARD OF COMMISSIONERS**	**NUMBER: 34**	**PAGE 1**
TITLE: ELECTRONIC SIGNATURE	**PERSONNEL** **ADMINISTRATIVE X**	**RESOLUTION** **NO:08-113**
EFFECTIVE **DATE: February 5, 2008**	**TYPE:** **POLICY X** **PROCEDURE**	**SUPERSEDES:** **POLICY #** **PROCEDURE #**

PURPOSE:

To authorize and provide procedures to verify 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 as required to facilitate secure authentication of electronic financial transactions and records.

SCOPE:

This policy applies to County Auditor data processing systems and processes that use electronic signature or other means to process financial transactions and other electronic records.

DEFINITIONS:

"Electronic record" means a record created, generated, sent, communicated, received, or stored by electronic means. An electronic record is not capable of retention by the recipient to print or store the electronic record. Electronic Signature systems should provide the signatory and recipient with the ability to print a copy of the document.

"Electronic signature" (E-Sign) means an electronic sound, symbol, or process attached to or logically associated with a record and executed or adopted by a person with the intent to sign the record. Electronic signatures have the equivalent level of legal protection that is given to paper-based signatures. All security procedures and technologies should provide a reasonable level of authentication and integrity based on risk and purpose.

"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. "Security procedure" includes a procedure that requires the use of algorithms or other codes, identifying word or numbers, encryption, or callback or other acknowledgment procedures.

"Digital Certificate" means an attachment to an electronic message used for security purposes. The most common use of a digital certificate is to verify that a user sending a message is who he or she claims to be and to provide the receiver with the means to encode a reply.

"Identification and Authentication" means the verification of the identity of a requesting entity (a person, computer, system or process). Once it is determined who may have access to a system, the identification and authentication (I&A) process helps to enforce access control to the system by verifying the identity of the entity. Systems may use a variety of techniques or combinations of techniques such as user-ID, password, personal identification number, and digital certificates, to enforce I&A depending upon the level of access control required to protect the system.

"Integrity" means the assurance that information is not changed accidentally or through a malicious or otherwise improper act. Any changes occurring through the transmission or processing of an E-Sign record should either invalidate the signature or clearly show the change and create a security log identifying the user or system that produced the change and the time that it occurred. Comparative record audits and internal control procedures should also be considered to ensure the integrity of the information. These control procedures should be recorded in the system documentation along with any changes to the application, system environment, and operating procedures during the lifetime of the system.

"Risk Assessment" means a process concerned with identifying, analyzing and responding to Information Technology (IT) security risks. Risk assessment attempts to maximize the results of positive events and minimize the results of negative events.

"Interface Requirements" means that the Auditor must require a separate and distinct action on the part of the person for each signature action. The separate and distinct action must be clearly marked as indicating the user's intent to electronically sign a record. The separate and distinct action may include a series of keystrokes, a click of a mouse or other similar action.

"Nonrepudiation" procedures are designed to ensure that the signatory adopted or assented to the record or electronic transaction. An example would be add a statement as follows: **"By pressing the "Submit" button you are certifying that you are the authorized user of this system and agree that you are submitting an Electronic Signature which is comparable to your written signature for the purposes of this document."**

Per the Ohio Revised Code § 304.01:
(B) "County Office" means any officer, department, board, commission, agency, court, or other instrumentality of a county.

(E) "Electronic signature" means an electronic sound, symbol, or process attached to or logically associated with a record and executed or adopted by a person with the intent to sign the record.

➢ Note: The signature can be by a County employee **or** a citizen transacting with the County.

Ohio Revised Code § 304.02:

Prior to a county office using electronic records and electronic signatures, a county office shall adopt, in writing, a security procedure to verify 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. A security procedure includes, but is not limited to, a procedure requiring algorithms or other codes, identifying words or numbers, encryption, or callback or other acknowledgment procedures.

All E-Sign projects will be managed according to the Lucas County Auditor Management Policies and may require approval of the Lucas County Data Processing Board (LCDP Board).

The Security Procedures relating to E-Sign Systems developed or procured under authority of the LCDP Board will be managed by the Lucas County Auditor's LCIS representative and coordinated with agency staff and their Business Account Representative. All E-Sign Project Plans must contain a Security Assessment, which identifies and documents the level and type of technology used to provide security for the system. This assessment will become a permanent component of the Project File and associated System Documentation.

PROCEDURES:

As part of the Information Technology project planning process, the Auditor's LCIS Representative will complete an assessment of the risk for the use of the application by completing an "Electronic Transaction Security Assessment." The risk assessment identifies the appropriate security level by analyzing the impact of a security breach and the probability of an attempt to breach security. The agency risk assessment shall consider the nature of the information and the systems, the business purpose, the operating environment, the existing protections, the impact of a security breach, and the likelihood of a breach occurring. This process is initiated by each agency completing an "Electronic Transaction Security Assessment Request."

E-Sign systems shall receive a comprehensive Security Assessment to verify that an electronic signature created by the system is that of a specific person and for detecting changes or errors in the information in an electronic record. This Security Assessment must include, but is not limited to, a procedure requiring algorithms or other

codes, identifying words or numbers, encryption, or callback or other acknowledgment procedures. The system **documentation must include the specific security procedures and processes automatically employed by the system or conducted by security administrators, to ensure the identity of the signatory and the integrity of the electronic records stored within the system.**

RISK ASSESSMENT BY EACH COUNTY AGENCY:

(1) A representative of LCIS will assist Agencies in completing an assessment of the transaction risk for the use of the set of similar electronic transactions. The transaction risk assessment identifies the appropriate security level by analyzing the impact of a security breach and the probability of an attempt to breach security

(2) In determining the potential impact of a security breach, county agencies shall consider the:

(a) intended use of the electronic record or signature;
(b) type of information being transmitted, received or stored;
(C) network used;
(d) degree of risk to the state;
(e) degree of risk to the users of the system;
(f) degree of risk to third parties;
(g) projected volume of transactions;
(h) estimated cost;
(I) potential legal liability; and
(j) appropriate requirements for authentication of identity.

(3) Impact of a Security Breach. The potential impact of a security breach falls into one of four categories: low-impact, medium-impact, high-impact and very high-impact.

(a) Low-impact: A security breach is considered low-impact if: (I) there is no impact of a breach of security or (ii) the impact is slight or so insignificant that there would be no or only a slight and negligible financial loss, loss of the public's trust or adverse legal consequences.

(b) Medium-impact: A security breach is considered medium-impact if the impact is limited in nature. Limited in nature means that: (I) the financial loss when averaged for the electronic transaction set is less than ten thousand dollars to the business, citizen, state or other entity involved, or (ii) there are no major adverse legal implications, or (iii) the breach would cause at least some but not significant public distrust of the county.

(C) High-impact: A security breach is considered high-impact if: (I) compromised security would have a significant impact so that the financial harm when averaged for the electronic transaction set ranges from ten thousand dollars to five hundred thousand dollars, or (ii) the breach would result in media scrutiny and significant public distrust, or (iii) the breach would have adverse legal consequences.

(d) Very High-impact: The result of a security breach that has a very high impact would be extremely serious. This type of breach results in: (I) financial loss when averaged for the electronic transaction set exceeding five hundred thousand dollars, or (ii) considerable legal violations, or (iii) intense media scrutiny and widespread, deep public distrust.

(4) Probability of an Attempt to Breach Security. The primary consideration is the value of a security breach to a person attempting a breach. Value includes financial gain, unauthorized access to confidential information, and the ability to harass, embarrass or shock. The probability is characterized as low, medium or high.

(a) Low-probability: A low-probability electronic transaction is one that would have little value to someone attempting a breach, and therefore, the likelihood of breach attempts is small with any attempts likely to be none or few and limited in effort.

(b) Medium-probability: A medium-probability electronic transaction is one which would provide value to someone seeking to breach security.

(C) High-probability: A high-probability electronic transaction would provide great value to someone should he or she breach security.

SECURITY LEVELS:

In general, there are four levels of security that apply to internal E-Sign applications. Security Level "A" provides the minimum level of security for E-Sign systems. Security Level "D" provides the highest level of security:

Security Level A: Applications must use, at a minimum, a unique user-ID and an alphanumeric password consisting of at least eight characters, or other security procedures or features as approved by the Auditor. In cases where a user password is used for Electronic Signature authentication, a statement notifying the User should be provided at the point where the User logs into the system. An example would be: **"This Password acts as an Electronic Signature and is comparable to the authorized user's written legal signature. Passwords must never be shared or revealed to anyone else. Revealing a password exposes the authorized user to responsibility for actions that another party takes with password."**

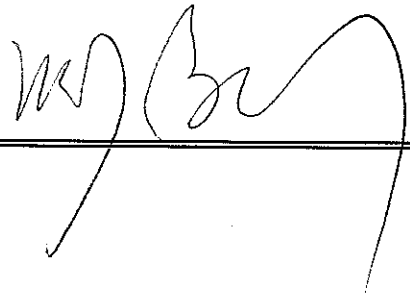
Security Level B: The addition of a smartcard or other physical device with a unique proprietary password combined with the password requirements described in Level A.

Security Level C: Under Level C security, agencies must use either digital certificates for authentication or a combination of a unique user-ID, password (described above), and a physical device such as a smartcard. The transmission of user-IDs and passwords must be encrypted using secure sockets layer or equivalent encryption when transmitted over the Internet or wireless transmission. Digital certificates used for electronic signatures require a significant infrastructure known as public key infrastructure (PKI). Therefore, Auditor employees may use a PKI only with the approval of the Auditor.

Security Level D: Security Level D requires a unique user-ID and password, a digital certificate issued under PKI, and a physical device such as a smartcard **or** biometric.

The above Security Levels are provided as guidelines. There may be cases where additional levels or types of security technology may be required. Each proposed E-Sign system and project will have its own set of variables which must be reviewed in the Security Analysis. These include the intended use of the signature; type of documents or information stored on the system; audit requirements; potential liability or cost of a security breech; network used, and degree of risk to the County or users of the system. Therefore, it's important that the business and functional requirements, and operating environment for each proposed E-Sign system are fully identified, analyzed, and documented before a Project Plan for development or purchase is approved.

References:
Rule 123:3-1-01 of the Ohio Administrative Code: Use of Electronic Signatures and Records.
Ohio Revised Code §304.02: Adoption of Security Procedures for Use of Electronic Records and Signatures.

APPROVED BY: 

DATE: 2/14/08