

Rule 123:3-1-01 of the Ohio Administrative Code Use Of Electronic Signatures And Records

Effective Date: June 2, 2007

- (A) Definitions. In addition to the definitions in section 1306.01 of the Revised Code, the following definitions are also applicable to this rule:
- (1) "Authentication" is the assurance that the electronic signature is that of the person purporting to sign a record or otherwise conducting an electronic transaction.
 - (2) "Domain" means category of persons based on the nature of the identity of the person.
 - (3) "Electronic transaction" means the exchange of an electronic record and electronic signature between a state agency and a person to:
 - (a) consent to release information;
 - (b) purchase, sell or lease goods, services or construction;
 - (c) transfer funds;
 - (d) facilitate the submission of an electronic record with an electronic signature required or accepted by a state agency; or
 - (e) create records upon which the State of Ohio or any other person will reasonably rely including but not limited to formal communication, letters, notices, directives, policies, guidelines and any other record. This subsection does not include informational publications and informal communications.
 - (4) "Integrity" is the assurance that the electronic record is not modified from what the signatory adopted.
 - (5) "Nonrepudiation" is the proof that the signatory adopted or assented to the electronic record or electronic transaction.
 - (6) "Office of Information Technology" (OIT) is the entity housed within the Department of Administrative Services under section 125.18 of the Revised Code to provide state governance and direction for information technology.
- (B) Scope.
- (1) This rule applies only to electronic transactions involving a state agency. In accordance with section 1306.20 of the Revised Code, for the purposes of this section, "state agency" means every organized body, office, or agency established by the laws of the state for the exercise of any function of state government, but does not include the general assembly, any legislative agency, the supreme court, the other courts of record in this state, or any judicial agency.

- (2) This rule applies to electronic transactions that include electronically signed records or electronic transactions involving a monetary transfer between a state agency and an individual, a corporation or another entity.

(C) General Rule.

- (1) Electronic transactions have the equivalent level of legal protection that is given to paper-based transactions. All security procedures and technologies should provide authentication, nonrepudiation and integrity to the extent that is reasonable for each electronic transaction.
- (2) This rule establishes an overarching security procedure that requires state agencies to:
 - (a) document uses of electronic transactions;
 - (b) conduct a transaction risk assessment of each set of similar electronic transactions;
 - (c) use, as a minimum, technology standards and security procedures that are appropriate for the level of security as determined by the transaction risk assessment;
 - (d) establish and maintain documented security policies and procedures; and
 - (e) seek a waiver from OIT if the state agency determines that the security technologies or procedures do not conform to the minimum technology standards as established by this rule for the level of security identified in the transaction risk assessment.

(D) Documenting Uses of Electronic Transactions.

- (1) For each set of similar electronic transactions, state agencies must complete an electronic transaction report before acquiring or implementing electronic signatures, transactions or related technology. Agencies must complete and update electronic transaction reports on forms provided by OIT at <http://www.ohio.gov/itp>. Agencies must maintain electronic transaction reports for as long as the electronic records of the electronic transaction are retained in accordance with that agency's record retention schedule.
- (2) Each electronic transaction report must include:
 - (a) The identification and description of the set of similar electronic transactions;
 - (b) The domain under which the electronic transaction set falls;
 - (c) A transaction risk assessment that identifies the potential impact of a security breach and the probability of attempts to breach security;
 - (d) A determination of the security level required for the electronic transaction set per the transaction risk assessment;
 - (e) The security procedure used for the electronic transaction set; and
 - (f) A list of documented agency security policies for physical, network and computer security. These documents must be clearly referenced and maintained on file and available for audit.

- (3) State agencies must update electronic transaction reports to accurately reflect changes in the electronic transaction's associated risk, technology or security procedures. If the state agency determines that due to these changes in risk, technology or security procedures, the electronic transaction does not conform to the minimum technology standard for the level of security identified in the transaction risk assessment, the state agency must modify the risk, technologies or procedures to bring the electronic transaction into compliance with this rule or the state agency shall seek a waiver from OIT.
- (E) Electronic Transaction Domains. Persons using electronic transactions in the course of government affairs fall in one of three domains – the citizen domain, the business domain or the state internal domain.
- (1) Citizen Domain: The citizen domain consists of individuals acting on their own behalf or on the behalf of any other individual under a power of attorney. The citizen domain includes only those individuals who choose to interact electronically with the State of Ohio. The citizen domain also includes state Web and application servers that interact with citizens.
 - (2) Business Domain: The business domain consists of corporations, business trusts, partnerships, limited liability companies, associations, joint ventures or any other commercial, charitable or legal entity that interacts electronically with state agencies. This domain also includes Web and application servers that interact with businesses.
 - (3) State Internal Domain: The state internal domain consists of state employees acting on behalf of the state, and any other agent of the state; network components; and web and application servers that use electronic transaction-enabled applications to conduct internal state business. The state internal domain also applies to local government representatives for electronic transactions with state government agencies.
- (F) Transaction Risk Assessment.
- (1) As part of the agency report, agencies must complete 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, state 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 state.
 - (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.
- (5) Transaction Risk Assessment. The transaction risk assessment results in a determination that the electronic transaction falls within one of four minimum security levels – low (Level A), medium (Level B), high (Level C) or very high (Level D). The minimum security level is determined by the combination of the level of the impact of a security breach and the level of probability of a security breach as identified in the following table:

Transaction Risk Assessment as Determined by the Impact of a Security Breach and the Probability of a Security Breach

	Low-Probability	Medium-Probability	High-Probability
Low-Impact	Level A	Level A	Level B
Medium-Impact	Level B	Level B	Level B
High-Impact	Level B	Level C	Level C
Very High-Impact	Level C	Level C	Level D

(G) Security Procedures Appropriate for Security Levels. Each electronic transaction set must conform to the minimum security procedures including technology standards for the level of security identified in the transaction risk assessment. State agencies may choose to meet the requirements of higher security levels with Level A being least secure and Level D being the most secure.

- (1) For any transaction used at Levels B, C or D or any Level A transaction involving confidential data or a monetary transfer, the transmission of user-IDs and passwords must be encrypted using secure sockets layer or equivalent encryption when transmitted over the Internet.
- (2) Level A: Under this level of security, state agencies may use any technological means for processing these sets of electronic transactions and providing assurance of authentication, nonrepudiation and integrity. State agencies shall document Level A electronic transaction sets per paragraph (D)(1) of this rule.
- (3) Level B: Level B electronic transactions must use at a minimum one of the following two security procedures for authentication: (a) a unique user-ID and an alphanumeric password consisting of at least eight characters, or (b) a smartcard or physical device with a unique proprietary password as an alternative. State agencies documenting Level B electronic transaction sets per paragraph (D)(1) of this rule must describe in the electronic transaction report the authentication process including information on the initial registration process and the means used to prove the identity of persons registering to use electronic transactions in the report.
- (4) Level C: Under Level C security, state agencies must submit the electronic transaction report to OIT and shall not use the electronic transaction until OIT approves the electronic transaction as being in compliance with this rule. State agencies must use digital certificates subject to paragraph (G)(4)(a) of this rule for these electronic transaction sets or the alternative in paragraph (G)(4)(b) of this rule.
 - (a) Digital certificates used for electronic signatures require a significant infrastructure known as public key infrastructure (PKI). Therefore, state agencies may use a PKI only with the approval of OIT. Pursuant to section 1306.21 of the Revised Code, when OIT determines that a PKI implementation is feasible, OIT may require the use of a common PKI by state agencies.
 - (i) OIT may make a state PKI available for use by the general assembly, any legislative agency, local governments, the supreme court, the other courts of record in this state or any judicial agency. These agencies are not required to use a state PKI.

- (ii) In establishing a PKI, OIT has the authority to review, approve and mandate components of a PKI including the registration process and authorities; certificate policies and certificate practices statements, certificate management including issuance, continued participation, certificate revocation and certificate suspension; and any other PKI policy, practice, management or operation. OIT may delegate any or all components of a PKI to state agencies or to vendors. OIT may revoke delegation of PKI components to a state agency or a vendor in the event that the state agency or vendor is in noncompliance with this rule, a certificate policy, or any other PKI policy or agreement.
 - (iii) OIT or its delegatee may revoke the digital certificate of any person whose use of the digital certificate is not in conformance with this rule, a certificate policy, or any other PKI policy or agreement.
 - (b) As an alternative to paragraph (a) of this section, agencies may meet Level C security by combining the use of a unique user-ID and an alphanumeric password consisting of at least eight characters with a smartcard or physical device. State agencies seeking approval of electronic transaction sets using this alternative must provide a description of the authentication process including information on the initial registration process and the means used to prove the identity of persons registering to use electronic transactions. Pursuant to section 1306.21 of the Revised Code and Executive Order 2004-02T, which may be found at <http://www.ohio.gov/itp>, OIT may require that state agencies use a common multi-agency smartcard or physical device infrastructure.
- (5) Level D: For Level D electronic transactions, state agencies must submit the electronic transaction report to OIT and shall not use the electronic transaction until OIT approves the electronic transaction as being in compliance with this rule. State agencies must use a digital certificate issued under a PKI approved by OIT in combination with a unique user-ID and password consisting of at least eight characters and a smartcard or physical device or biometric. Like Level C security, OIT may require state agencies use a common multi-agency infrastructure. Any state agency using a biometric must establish security policies to provide a high degree of assurance of the integrity and, if applicable, confidentiality of the biometric information. Agencies subject to policies issued under section 125.18 of the Revised Code shall conform with any OIT policies and standards published at <http://www.ohio.gov/itp> for security, interoperability and need. While state agencies may use higher levels of security than required by the transaction risk assessment, for biometrics, a state agency seeking to implement the use of biometrics must provide a justification to OIT.
- (H) Required Policies. State agencies must establish documented policies and procedures that provide reasonable assurance of the authenticity of the electronic signatures, the nonrepudiation of the electronic records by the signatories and the integrity of the electronically signed records. This includes but is not limited to policies and procedures on access, control, monitoring, maintenance and any other actions necessary for physical, network and computer security. Nothing in this rule permits state agencies to supersede or establish security policies in conflict with any other policy, which may be found at <http://www.ohio.gov/itp>, established by OIT.

- (I) Interface Requirements. When at any time during an electronic transaction a state agency requires a signature or is conducting a financial transaction, the state agency must require a separate and distinct action on the part of the person conducting the transaction for financial transactions and each signature. The separate and distinct action must be clearly marked as indicating an intent to complete a financial transaction or electronically sign a record. The separate and distinct action may include a series of keystrokes, a click of a mouse or other similar action.
- (J) Records Retention Requirements. State agencies' records retention practices must assure nonrepudiation, integrity and continued access to the electronic record.
- (K) Waiver Provisions. State agencies may request a waiver of this rule by OIT.
 - (1) Upon a state agency request for a waiver pursuant to paragraph (D) of this rule, the director of the OIT or the director's designee may waive the requirements of this rule for an electronic transaction set upon a showing by the state agency that the alternative security technology and procedures governing the set of similar electronic transactions do not compromise the level of security as determined by paragraphs (F) and (G) of this rule. Upon finding that the alternative security technologies or procedures are no longer appropriate for the level of risk, the OIT director may revoke the waiver.
 - (2) The waiver request is a letter to OIT identifying the electronic transaction set, stating that the state agency is seeking a waiver and providing a justification for the waiver. The request for waiver includes the electronic transaction report. The justification must show that the proposed alternative security technology and procedures provide authentication, nonrepudiation and integrity and do not compromise the level of security as determined by paragraphs (F) and (G) of this rule.
- (L) Electronic Transactions with Agencies of Other States and the Federal Government. This rule applies to electronic transactions between state agencies and federal agencies to the extent that it is consistent with federal law. OIT may coordinate the use of electronic signatures between state agencies and the federal government. OIT may coordinate the use of electronic signatures with agencies of another state.

Effective: June 2, 2007

R.C. 119.032 review dates: April 3, 2011

Promulgated under: R.C. 111.15
Statutory authority: R.C. 1306.21
Rule amplifies: R.C. 1306.21