

MANAGEMENT DIRECTIVE

Commonwealth of Pennsylvania Governor's Office

Subject:

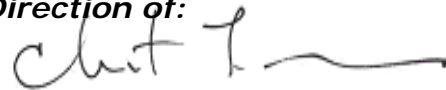
Electronic Commerce Initiatives
and Security

Number:

210.12 Amended

Date:

December 23, 2010

By Direction of:

Christian L. Soura, Secretary of Administration

Contact Agency:

PA Office of Administration, Office for Information Technology,
Telephone 717.787.5440

This directive establishes policy, responsibilities, and procedures for sending, accepting, storing, or using electronic signatures or electronic records and evaluating and reviewing electronic commerce initiatives and security. Marginal dots are excluded due to major changes.

- 1. PURPOSE.** To establish policy, responsibilities, and procedures for the implementation of the *Electronic Transactions Act (Act 69 of 1999)*, 73 Pa. C.S. § 2260.101, et seq.
- 2. SCOPE.** This directive applies to all department, boards, commissions, and councils (hereinafter referred to as "agencies") under the Governor's jurisdiction. Independent agencies are encouraged to adopt and follow similar procedures.
- 3. OBJECTIVES.**
 - a.** To ensure the consistent, reliable, and secure use of electronic records and electronic signatures.
 - b.** To provide standards for the secure transmission and storage of confidential information.
 - c.** To provide guidance for the use of electronic records and electronic signatures in providing services and conducting the business of government electronically.

4. DEFINITIONS

- a. **Act.** The *Electronic Transactions Act (Act 69 of 1999)*, 73 Pa. C.S. § 2260.101, et seq.
- b. **Electronic.** Relating to technology having electrical, digital, magnetic, wireless, optical, electromagnetic, or similar capabilities.
- c. **Electronic Record.** A record created, generated, sent, communicated, received, or stored by electronic means.
- d. **Electronic Signature.** 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.
- e. **Electronic Transaction.** The electronic sharing of information including:
 - (1) Electronic posting of sensitive data on a network, such as the World Wide Web.
 - (2) The exchange of an electronic record or electronic signature by an executive agency with a person to:
 - (a) facilitate access to restricted information;
 - (b) purchase, sell or lease goods, services, or construction;
 - (c) transfer funds;
 - (d) facilitate the submission of an electronic record or electronic signature required or accepted by the commonwealth; or
 - (e) create a record upon which the commonwealth or another person will reasonably rely.
- f. **Executive Agency.** A department, board, commission, council, authority, officer, or agency subject to the policy, supervision, and control of the Governor.
- g. **Information.** Data, text, images, sounds, codes, computer programs, software, data bases, or the like.
- h. **Person.** Any individual, corporation, business trust, estate, trust, partnership, limited liability company, association, joint venture, governmental agency, public corporation, or other legal or commercial entity.
- i. **Record.** Information which is inscribed on a tangible medium or is stored in an electronic or other medium and which is retrievable in perceivable form. The term includes permits, licenses, applications, and other documents required or issued by an executive agency.

- j. **Security Procedure.** 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. The term includes a procedure which requires the use of algorithms or other codes, identifying words or numbers, encryption or callback or other acknowledgment procedures.

5. POLICY.

- a. This directive shall be read in conjunction with:

- (1) *Management Directive 210.11, Acceptance of Imaged Documents.*
- (2) *Management Directive 205.34, Commonwealth of Pennsylvania Information Technology Acceptable Use Policy.*
- (3) *Management Directive 210.5, The Commonwealth of Pennsylvania State Records Management Program.*

- b. **Waivers.** An executive agency may apply for a waiver from the procedures established by this directive by providing the Office of Administration (OA) with adequate justification. Waivers must be approved, in writing, by OA, in consultation with the Office of General Counsel (OGC).

- c. **Notaries and Seals.**

- (1) Unless and until the laws of the commonwealth are amended to provide for electronic notarization, verification, or acknowledgment, executive agencies may not use or accept an electronic signature for these purposes.
- (2) Executive agencies may not use or accept electronically sealed records or documents except as specifically permitted by law. Executive agencies may accept electronic seals from "*Registered Professional Engineers,*" "*Registered Professional Land Surveyors,*" or "*Registered Professional Geologists,*" in accordance with *49 Pa. Code § 37.58.*

- d. **Review of Security Procedures.** Each executive agency shall review the manner in which it sends, accepts, uses, and stores electronic records and electronic signatures at least every 12 months to determine whether the security procedure being used is adequate or whether additional security is necessary.

6. RESPONSIBILITIES.

- a. **The Office of Administration** may require an agency to prepare or resubmit a completed Commonwealth Application Certification and Accreditation (CA)² application at any time.

- b. **The Office of the Budget** will audit electronic commerce initiatives by executive agencies and shall require compliance with the (CA)² process.

7. PROCEDURES.

- a. **Agency Risk Evaluation.** There are risks in conducting business using any medium, whether person-to-person, telephonic, paper-based, via fax, mail, or electronically. Prior to an executive agency participating in or initiating an electronic transaction, the executive agency shall evaluate the legal, financial, and other risks associated with the electronic transaction to the commonwealth and to other persons. Agencies shall take all reasonable steps to anticipate and eliminate any foreseen risks and shall obtain the approval of the Agency Chief Counsel prior to implementing a system for the acceptance of electronic records and electronic signatures. If the agency identifies risks inherent in the electronic transaction, the agency shall complete the (CA)² process required by subsection b.

- b. **Electronic Commerce Application Certification and Accreditation (CA)².**

- (1) Prior to participating in or initiating an electronic transaction involving the use, transmission, or storage of electronic records or electronic signatures, an executive agency is required to submit a (CA)² request to OA for review. This review consists of policy compliance assessments and risk assessments, which include source code analysis, host-based intrusion scans, and Web application risk assessments.
- (2) The (CA)² process identifies any inherent risks associated with an existing or proposed electronic commerce initiatives and enables OA, Office for Information Technology (OIT), Information Security Office to complete the security review for existing and proposed Web applications.
- (3) Applications that successfully go through the (CA)² process will be deemed accredited and will receive a seal from OA/OIT showing the application's accreditation status. Web applications that go through the process and have risks that cannot be remediated will be required to have a risk mitigation plan. The risk mitigation plan will identify the risks associated with the Web application and identify how the agency plans to mitigate these risks. This plan will be attached to the (CA)² submission and reviewed by OA/OIT/Information Security Office to determine if the application can go into production with a conditional accreditation.
- (4) The (CA)² process will evaluate the proposed use, transmission, or storage of the electronic record or electronic signature and recommend the electronic security procedure, if any, to be used by the agency based upon the:
 - (a) intended use of the electronic record or signature;

- (b) type of information being transmitted, received, or stored;
 - (c) network to be used;
 - (d) degree of risk to the commonwealth;
 - (e) degree of risk to the users of the system;
 - (f) projected volume of transactions;
 - (g) effectiveness of the security procedure;
 - (h) estimated cost; and
 - (i) potential legal liability.
- (5) OA will prepare and issue Information Technology Bulletins (ITBs), as appropriate, to provide agencies guidance on the technical aspects of the criteria listed in subsection b.(4). The ITBs will correspond with the (CA)² process and identify security procedures that may be used by executive agencies for sending, receiving, storing, and using electronic records and electronic signatures.

c. Use of Electronic Signatures and Records.

- (1) As provided in the *Act*, executive agencies may send, accept, store, and use electronic records and signatures in conducting their operations following the criteria listed in subsection b.(4) and any other criteria the agency determines appropriate.
- (2) Consistent with the (CA)² process, executive agencies are authorized to specify the format in which electronic records are to be created, stored, accepted, and sent.
- (3) Executive agencies shall, to the greatest extent possible, adopt formats that are consistent and interoperable with other federal, state, and local agencies.
- (4) Executive agencies may require that a record submitted electronically contain an electronic signature. If the agency determines that an electronic transaction requires an electronic signature, agencies shall specify the:
 - (a) manner and format in which the electronic signature must be affixed to the electronic record; and
 - (b) criteria that must be met by any third party used to facilitate the electronic signature process.

- (5) Executive agencies may specify record retention requirements for entities regulated by or under the agency's jurisdiction including the requirement that the record be retained and/or submitted in non-electronic form.
- d. Executive agencies that receive and use confidential information, as defined by applicable statute or regulation, shall take appropriate measures to maintain the confidentiality of the record.
- e. **Networks.**
 - (1) To the greatest extent possible, agencies should use open networks (i.e., the World Wide Web) when conducting business electronically.
 - (2) Executive agencies may use closed networks to send and accept electronic records and electronic signatures where, for security reasons, the agency determines the closed network is in the best interest of the commonwealth. Agencies may not create or participate in a closed network unless it is first approved by OA.
- f. **Monitoring.** After participating in or implementing a system for electronic transactions, executive agencies shall regularly examine their electronic commerce initiatives to evaluate the nature and extent of any risks to the user and to the commonwealth. Agencies shall evaluate their electronic commerce initiatives at least annually to make certain that the appropriate security procedures, electronic and otherwise, are being utilized to protect and preserve the integrity of the information being stored, sent, accepted, or used.
- g. **Electronic Record Retention and Conversion of Nonelectronic Records.**
 - (1) Executive agencies may determine whether, and the extent to which, they will create and retain electronic records and convert written records to electronic records.
 - (2) In retaining and storing electronic records and signatures, executive agencies shall comply with applicable law, ITBs issued by OA, and standards adopted by the Pennsylvania Historical and Museum Commission (PHMC). Executive agencies may prescribe additional processes and procedures to ensure the adequate preservation, disposition, integrity, security, confidentiality, and auditability of electronic records.
 - (3) Executive agencies that retain records electronically shall adopt procedures protecting the security and integrity of the information. Depending on the nature of the records, agencies shall consider adopting procedures limiting individual access to the electronic records.

h. Terms and Conditions for Electronic Transactions/Rebuttable Presumptions.

- (1) Executive agencies shall prepare and include on the network, available to users, the agencies' terms and conditions to participate in an electronic transaction with the agency. Prior to the network user's submission of any information as part of an electronic transaction, the user of the system must agree to the executive agency's electronic transaction terms and conditions.
- (2) In nonconsumer electronic transactions where the executive agency creates and uses a commercially reasonable security procedure on its network to verify the person from which an electronic signature or record is sent, the agency shall notify the person that the electronic signature and/or the electronic record will be attributed to the person identified by the security procedure. The electronic record or signature may not be attributed to the person if the person satisfies the burden of establishing one or more of the exceptions contained in *Section 701* of the *Act*.
- (3) In nonconsumer electronic transactions where the executive agency creates and uses a commercially reasonable security procedure on its network to detect errors or changes with respect to an electronic record or electronic signature, and the security procedure indicates that the electronic record or signature has not been changed or altered, the agency shall notify the user that the electronic record or electronic signature will be deemed to not have been altered.

This directive replaces, in its entirety, *Management Directive 210.12*, dated February 14, 2000.