Policy 14.00: Electronic and Digital Signatures

The manner and format by which electronic and digital signatures will be used in state government will be reviewed and approved by the Office for Information Resources.

Definitions:

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. Examples of an electronic signature are: a name at the end of an email, clicking a button or downloading content to indicate acceptance of a transaction or certain terms and conditions.

Digital signature – a specific type of electronic signature that relies on the technology of cryptography to authenticate the signer's identity and ensure the integrity of the signed document. A digital signature is bound to the document being signed using a mathematical algorithm such that any modification of the document after it is signed can be detected. (Note: The term document as applied in this policy is used interchangeably with terms such as electronic document, record or transaction.)

REFERENCE:

Tennessee Code Annotated, Section 4-3-5501, effective May 10, 1994.
Tennessee Code Annotated, Section 47-10-118, effective April 11, 2001
Uniform Electronic Transactions Act (UETA).

OBJECTIVES:

1. Ensure that digital signatures are implemented using a standard information technology architecture for interoperability of documents across government.
2. Ensure that documents and/or transactions signed using a digital signature can be reproduced over time to meet statutory requirements.
3. Facilitate online business processes that require a high degree of "trust" (identity authentication) between the parties and the "integrity" of the transaction.
4. Promote the cost effective use of electronic and digital signature technologies to provide business solutions commensurate with the value and risk to the business process.
5. Define the responsibilities of information systems management and users in the use of electronic and digital signature technologies.

SCOPE:

This policy applies to the use of all electronic and digital signatures regardless of computing platform, type of software utilized (custom developed or commercial off the shelf product), procured, acquired or hosted by a third party.

IMPLEMENTATION:

Office for Information Resources (OIR)

1. Develop statewide standards, procedures and guidelines necessary for the implementation of electronic and digital signatures in state government.
2. Provide management and technical consulting to state agencies in planning for and utilizing electronic and digital signature technologies.
3. Provide for the ongoing technical review of electronic and digital signature technologies and legislation in order to forecast changes needed in state policy.
4. Provide for administrative review of the policies, standards, procedures and guidelines in light of technical, procedural, or statutory changes that may occur in the use of electronic and digital signatures.
5. Define the responsibilities of information systems management and users in the use of electronic and digital signature technologies.

Agency

1. Establish agency policies, standards, procedures and guidelines pertaining to the implementation of electronic and digital signatures consistent with statewide policies and standards.
2. Educate users on the policies, standards, procedures and guidelines related to the use of electronic and digital signatures.
3. Provide for agency administrative review of the policies, standards, procedures and guidelines in light of technical, procedural, or statutory changes that may occur in the use of electronic and digital signatures.

Individual Users/Clients

1. Adhere to statewide and agency policies, standards, procedures and guidelines pertaining to the implementation of electronic and digital signatures in state government.
2. Refrain from behaviors that would expose the confidential nature of authentication and/or integrity components of electronic and digital signature technology to unnecessary or unauthorized risks.

Date Last Revised – 3/6/2007 – Approved by Information Systems Council