Electronic Signature Policy

June 24, 2010

ELECTRONIC SIGNATURE POLICY

1. Introduction

1.1. Background

1.1.1. New York State adopted an Electronic Signatures and Records Act (ESRA) which provides guidance to NYS governmental entities, including Public Authorities. "The purpose of ESRA is to facilitate e-Commerce and e-Government in New York State by giving electronic signatures (e-signatures) …the same force and effect as signatures and records produced by non-electronic means".[i]

2. Policy Statement

2.1. This policy provides for the utilization of an electronic signature by the Development Authority of the North Country (Authority) by means of methods that are practical, secure, and balance risk and cost. **The Authority electronic signature authorization process will be instituted for internal documentation and certification only**.

2.2. The Authority's e-signature system will utilize user authentication by verifying the user's unique credentials; such as username and password, or a digital certificate.

2.3. This policy does not supersede situations where laws specifically require a written signature. This policy does not limit the option to conduct the transaction on paper or in non-electronic form and the right to have documents provided or made available on paper at no charge. The e-signature must be protected by reasonable security measures as applicable to established computer functions of the Authority.

3. Evaluation Process for Use of Electronic Signature

3.1. Evaluation of Risk

3.1.1. An evaluation will be performed by the Authority to determine risks associated with each e-signature application to determine the quality and security of the e-signature method required through the completion of the "E-SIGNATURE - BUSINESS ANALYSIS AND RISK ASSESSMENT FORM", attached as Exhibit A. The *New York State CIO's Best Practice Guidelines G07-001 Identity and Access Management: Trust Model (NYS Trust Model) shall be utilized as a guideline for completing the evaluation.* http://www.cio.ny.gov/policy/G07-001/G07-001.pdf

3.1.2. A copy of each E-SIGNATURE - BUSINESS ANALYSIS AND RISK ASSESSMENT shall be maintained on file.

3.2. Determination of Electronic Signature Methodology

3.2.1. The e-signature methodology should be commensurate to the assurances needed for the risks identified. In addition, specifications for recording, documenting, and/or auditing the e-signature as required for non-repudiation and other legal requirements shall also be determined by the Authority. The lowest cost, least complex method acceptable for the risk is generally preferable.

4. Maintenance and Review Requirements

4.1. Security. Software and/or hardware that are required for e-signatures will be provided by the Authority. The Authority will ensure that appropriate controls and monitoring of the software/hardware are in place.

4.2. Periodic Review

4.2.1. A review of each e-signature implementation will be conducted periodically by the Compliance Officer, but no less than annually. This will include an evaluation of the e-signature use to determine whether any applicable legal, business, or data requirements have changed. A determination will be made as to the continued appropriateness of the risk assessment and e-signature implementation method.

4.2.2. A record of this review will be documented and filed as part of the official record for this e-signature implementation maintained by the Authority. If as a result of the periodic review the risk level changes, a new risk assessment must be completed, including review and approval.

4.2.3. The results of the review shall be submitted to the Authority's Executive Director who shall evaluate and make recommendations to the Board for any changes deemed necessary and appropriate.

References:

i. CIO/OFT's ELECTRONIC SIGNATURES AND RECORDS ACT (ESRA) GUIDELINES, http://www.cio.ny.gov/Policy/G04-001/G04-001.pdf

ii. CIO/OFT New York State Information Technology Best Practice Guidelines, No.NYS-G07-001, Identity and Access Management: Trust Model, http://www.cio.ny.gov/policy/G07-001/G07-001.pdf

iii. CIO/OFT, New York State Information Technology Policy, No.NYS-G04-001, Electronic Signatures and Records Act (ESRA) Guidelines, http://www.oft.state.ny.us/Policy/G04-001/G04-001.pdf

EXHIBIT A
E-SIGNATURE - BUSINESS ANALYSIS AND RISK ASSESSMENT FORM
SAMPLE ANALYSIS

1. E-signature Application:
    a. E-Signature Form Request :_____
    (*Include document for which you are requesting to use e-signature for authentication*)
    b. Legal Requirements: Yes / No (Circle 1)
        i. If yes, unacceptable use of e-signature
        ii. If no, proceed to #1c
    c. Internal Use Only: Yes / No (Circle 1)
        i. If yes, proceed to #1D
        ii. If no, unacceptable use of e-signature.
    d. Software Used:_____
2. Business Analysis:
    a. The Development Authority will be utilizing e-signatures for internal use only and will not be utilizing e-signatures for the purposes of providing authorization to third parties. The use of e-signatures will be utilized for authorizing documents internally in an effort to increase efficiency and to reduce paper consumption.
3. Risk Assessment:
    b. Risk is a function of the likelihood that a given threat will exploit a potential vulnerability and have an adverse impact on an organization. A threat is a potential circumstance, entity or event capable of exploiting vulnerability and causing harm. Threats can come from natural causes, human actions, or environmental conditions. Vulnerability is a weakness that can be accidentally triggered or intentionally exploited. A threat does not present a risk when there is no vulnerability. Impact refers to the magnitude of harm that could be caused by a threat.
    c. To mitigate risk, Authority e-signatures shall be authenticated through access to the Authority domain. This requires users being granted access into the Authority domain and utilizing a username and password for authentication. The Authority has adopted a Computer Use and Password Policy which established a standard for the creation of strong passwords, the protection of those passwords and the frequency of change of such passwords. The internal controls included in such policy are deemed effective.
    d. To mitigate risk, the Authority will limit e-signatures to internal use only.
    e. Given the restricted use of e-signatures to include internal use only and the requirement that all users must be authenticated to the Authority domain for an e-signature to be deemed valid, the Authority determined the likelihood that a threat will occur to be unlikely.
    f. The Development Authority calculates its internal controls over the e-signature process to be effective.
    g. Overall Risk Assessment Per Exhibit B: (Circle 1)
        i. Negligible / Low / Medium / High

_____ _____
Manager Signature Executive Director Signature

_____
IT Signature

EXHIBIT B
RISK ASSESSMENT MATRIX

RISK = LIKELIHOOD x IMPACTS				
Likelihood	IMPACTS			
	High 4	Medium 3	Low 2	Negligible 1
High 4	High 16	High 12	Medium 8	Low 4
Medium 3	High 12	Medium 9	Low 6	Negligible 3
Low 2	Medium 8	Low 6	Low 4	Negligible 2
Unlikely 1	Low 4	Negligible 3	Negligible 2	Negligible 1