Development Authority of the North Country Governance Policies

Subject: Electronic Signature Policy
Adopted: March 28, 2018 (Annual Meeting)
Resolution: 2018-03-35

Table of Contents

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 both electronic and digital signatures 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 and digital signature authorization process will be instituted for internal and external documentation and certification**.

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

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 Identity Assurance IT Policy No: NYS-P10-006 shall be utilized as a guideline for completing the evaluation.* https://its.ny.gov/sites/default/files/documents/nys-p10-006_identity_assurance_3.pdf

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

3.2. Determination of Electronic or Digital 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.

5. Definition of electronic and digital signatures

5.1. An electronic signature is any verifiable sound, symbol or process that is electronically associated with a contract or record indicating his or her intent to sign.

5.2. Digital signatures embed a unique digital "fingerprint" into documents and the signer is required to possess a certificate-based digital ID in order to link the signer and document. These certificates are issued by certification authorities (CAs) and these authorities provide users two digital keys for the certificate – a public key and a private key.

References:

i. NYS Office of Information Technology Services, Electronic Signatures and Records Act (ESRA) Guidelines: No: NYS-G04-001
https://its.ny.gov/sites/default/files/documents/nys-g04-001_electronic_signatures_and_records_act_ersa_guidelines.pdf

ii. NYS Office of Information Technology Services, Identity Assurance, No: NYS-P10-006
https://its.ny.gov/sites/default/files/documents/nys-p10-006_identity_assurance_3.pdf

Revision Date: March 28, 2018; Resolution No. 2018-03-35

EXHIBIT A

E-SIGNATURE – BUSINESS ANALYSIS AND RISK ASSESSMENT FORM

1. E-Signature Application:
    a. E-Signature Form Request:_____

    _____

    (Include document for which you are requesting to use e-signature for authentication)
    b. Document requires a notary and/or company seal? (Note: only the page requiring signature with notary and/or seal cannot be e-signed. All other pages needing signature are available for e-signature)
        i. If yes, unacceptable use of e-signature
        ii. If no, proceed to 1c
    c. Software Used:_____
2. Business Analysis:
    a. The Development Authority will be utilizing e-signatures for internal and external use. The use of e-signatures will be utilized for authorizing documents internally and externally in an effort to increase efficiency and to reduce paper consumption.
3. Risk Assessment:
    a. 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.
    b. To mitigate risk, Authority e-signatures shall be (check one):

    _____ authenticated through access to the Authority domain or

    _____ an approved e-signature software vendor

    Access to the Authority domain requires internal users follow a Computer Use and Password Policy which establishes a standard for the creation of strong passwords, the protection of those passwords and the frequency of change of such passwords. E-signatures requiring digital transaction management services outside the Authority domain must use an approved vendor established by IT and approved by the Executive Director.
    c. Given the requirement that all e-signatures must be managed by an approved vendor or have authentication through the Authority domain, the Authority determined that the likelihood a threat will occur would be unlikely.
    d. The Development Authority calculates its internal controls over the e-signature process to be effective.
    e. Comments:_____
    f. Overall Risk Assessment Per Exhibit B: Likelihood Rating: _____ Impact Rating: _____

    Negligible ☐ Low ☐ Medium ☐ High ☐

_____ _____

Manager Signature Executive Director Signature

_____

Director of Information Systems 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

High Risk =10-16 Medium Risk =7-9 Low Risk =4-6 Negligible Risk =1-3