FNSB NO. 40.06
DATE: 09/05/19

APPROVED James O. Williams

ELECTRONIC SIGNATURE POLICY

I. GENERAL

Information technology now provides for the creation, processing, and maintenance of documents in electronic form without requiring creation of corresponding paper media. Electronic information processing is becoming the preferred mode for management and transfer of contracts and other documents.

II. PURPOSE

The purpose of this policy is to establish and identify the criteria and requirements for the use and validation of electronic signatures when conducting the Borough's business operations both internally and externally. The policy is intended to ensure that, as departments implement this technology, they do so in a manner that is consistent Borough wide.

III. RESPONSIBILITY

A. Department directors shall ensure that their department staff follows the procedure set forth in this policy.

B. Digital Services shall enforce this policy.

C. Human Resources shall maintain this policy.

IV. POLICY

A. This policy applies to signatures both internal and external to the Borough but excludes all international agreements.

B. Consistent with applicable Federal and State laws and Borough policies regarding electronic recordkeeping and security, the Borough is committed to supporting the implementation of integrated electronic processing applications which expedite the workflow and reduce duplication of effort.

C. This policy specifically applies to any electronic transaction that is a replacement for, or complement to, a paper form or document originated by the Borough or a contractor, grantor/grantee, or lessor/lessee.

D. Documents that by law must be notarized are excluded from this policy and must be signed in a non-electronic form.

E. This policy does not limit the Borough's right or option to conduct a Borough transaction on paper or in non-electronic form, nor affect the Borough's right or obligation to require that documents be provided or made available on paper when required by applicable policies, laws, or regulations.

F. This policy applies only to transactions between parties who have each agreed to conduct transactions by electronic means.

G. When a document containing an electronic signature is signed, transmitted, and received the following requirements must be met:

1. Signature Authentication:

   a. The electronic signature must establish sender/user authenticity;

   b. It must be possible to ensure, with a reasonable degree of certainty, that the sender's signature has not been forged;

   c. Sufficient audit trails must be provided to resolve disputes, with a reasonable degree of certainty, when an individual disavows signing the document.

   d. The signing of a contract using an approved electronic signature method does not ensure that the record has been signed by a person authorized to sign or approve that record. Thus, appropriate documentation showing that the signer has authority to bind the entity entering into an agreement with the Borough may be required.

   e. If approved electronic signature methods require the use of encryption technology that uses public key infrastructure and/or certificates, the Digital Services Department will be responsible for the administration of such public or private keys and/or certificates, as applicable.

2. Message Authentication:

   a. It must be possible to ensure, with a reasonable degree of certainty, that a document and its signature have not been changed after it is signed. If a document has been modified or changed, the signature is invalid.

   b. Electronic information and forms processing applications using electronic signatures may incorporate the following additional considerations when applicable:

      i. The need for the signature on a document to be obscured from disclosure during transmission (i.e., data encryption);

      ii. The need for only a few individuals to have access to signing, processing, or viewing capabilities (i.e., access control).

V. PROCEDURE

The Digital Services Director, with the assistance and advice of the Chief Financial Officer, the Chief Procurement Officer, and the Borough Clerk, is responsible for:

A. Approval of Electronic Signature Methods

1. The Director of Digital Services, or their designee, shall issue final approval of any electronic signature method. In determining whether to approve an electronic signature method, consideration will be given to the systems and procedures associated with using that electronic signature and whether the use of the electronic signature is at least as reliable as the method currently used.

2. If an approved electronic signature method requires the use of encryption

technology that uses public key infrastructure and/or certificates, the Digital Services Department will be responsible for the administration of such public or private keys and certificates as applicable.

3. The approval of an electronic signature method can limit the use of that method to particular records, classes of records, or particular departments. An electronic signature used outside of its limitations will not be considered valid by the Borough.
4. All approved electronic signature methods will be available to Borough departments and the public and will be deemed appendices to this policy as they are approved.
5. In the event that the Director of Digital Services determines that an approved electronic signature method is no longer trustworthy, they shall inform the affected Department Director that the approval of that electronic signature method is revoked. If there is continued significance for an agreement electronically signed using the revoked method, the affected Department Director will take steps to ensure that the documents are re-signed using an approved signature method.

B. Reviewing all automated systems within the Borough to determine applicability of this policy and establishing specific procedures to ensure current and future systems comply with the requirements of this policy.

C. Identifying a specific technical approach for all required technology areas that cost-effectively addresses the risks of the application.

D. Determining the level of security required for any proposed electronic signature solution.

E. Providing training and awareness about electronic signatures and this policy.

F. Providing guidance and assistance in implementing this policy.

G. Ensuring that information security and privacy issues are met.

H. Periodically reviewing electronic signature solutions to ensure that electronic records are maintained in accordance with Federal, State and Borough laws, policies, and procedures.

I. Developing and maintaining procedures for the acceptable use of specific electronic signature software and hardware components, including documentation of transactions for auditing purposes.

J. Developing and maintaining procedures for the issuance and discontinuance of assignment of signatory privileges to individual employees.

K. Discontinuing or amending employee defined privileges when employees change positions or leave Borough employment.

L. Maintaining methods for tracking and auditing documents using electronic signatures.

VI. SUPPLEMENTAL INFORMATION

A. References –

1. Electronic Records and Signatures in Commerce (15 USCS 7001 et seq.

PL106-229)

2. Uniform Electronic Transactions Act (AS 09.80.010 et seq.)

B. Definitions –

1. "Certificate" is an electronic document used to identify an individual, server, a company, or some other entity and provides generally recognized proof of a person's identity.
2. "Electronic" relates to technology having electrical, digital, magnetic, wireless, optical, electromagnetic, or similar capabilities.
3. "Electronic record" is a record created, generated, sent, communicated, received, or stored by electronic means.
4. "Electronic signature" means an electronic sound, symbol, or process that is attached to or logically associated with a record and that is executed or adopted with the intent to sign the record.
5. "Electronic transaction" is a transaction conducted or performed, in whole or in part, by electronic means or electronic records.
6. "Private key" means code that is paired with a public key to set off algorithms for text encryption and decryption. It is created as part of public key cryptography during asymmetric-key encryption and used to decrypt and transform a message to a readable format.
7. "Public key" means encryption cryptography that uses asymmetric encryption algorithms. Public keys are used to convert a message into an unreadable format. Decryption is carried out using a different, but matching, private key. Public and private keys are paired to enable secure communication.
8. "Record" means information that is inscribed on a tangible medium or that is stored in an electronic or other medium and that is retrievable in perceivable form.

C. Revision History

Supersedes Policy No.
(None - New)