USE OF DIGITAL SIGNATURES

**POLICY**

Our Firm allows for the use of electronic signatures for SEC filings and other firm documents. Our firm's policy is to maintain files and records of all authentication documents in an appropriate, current, accurate, and well-organized manner. All manually signed attestations are retained for as long as the signatory may use an electronic signature to sign an authentication document and for a minimum period of seven years after the date of the most recent electronically signed authentication document.

may occur when the relationship between Advisor and client first begins and when a transaction occurs within the course of an existing relationship. Authentication refers to the process your firm uses to verify the identity of the client. This may vary from requiring your client to personally appear and present a physical ID and wet ink signature or your client providing a digital signature through a service like DocuSign. When authenticating via a digital signature, the client will receive an access or identification verification device, a “Credential”, which is used to streamline or automate identification in future transactions.   A Credential may be a username, password or pin, a number generated at random, a digital certificate, a biometric measurement (e.g., retina scan, fingerprint matching, or voice recognition) a digitized image of a handwritten signature, a typed name or a combination of these. The Credential may be used to authenticate an individual before an electronic signature is accepted.

If an Advisor chooses to implement a process for electronic signatures, the Advisor must update their procedures to document their process for accepting electronic signatures, which may include, but is not limited to the following:

1. Implementation of supervisory reviews and testing to ensure compliance with the above requirements.
2. Maintaining a record of all documents the Advisor allows to be executed by clients through electronic signature.
3. Maintaining a record of documents the Advisor allows to be delivered electronically, specifically those documents included in establishing and maintaining client relationships.
4. Maintaining a record of all client documents electronically signed and for each document signed, document:
   * Document Control Number or Unique Identifier;
   * Client Name(s);
   * Account Number(s);
   * Document Type or Name (i.e., account agreement, fund transfer request, etc.)
   * Authentication information for all parties that signed or created the document. Such information should include the client’s email address, username, or other means to authenticate the client’s identity;
   * IP Addresses used by all parties that signed or created the document;
   * Dates and times of all signatures on the document; and
   * Date and time that the document was created.

**Background**

The SEC adopted amendments to Rule 302(b) of Regulation S-T, which allows for the use of electronic signatures in SEC filings, and which went into effect on December 4, 2020. The rules permit a signatory to an electronic filing who follows certain procedures to sign an authentication document through an electronic signature that meets certain requirements specified in the EDGAR Filer Manual. These requirements are intended to be technologically neutral and allow for different types and forms of electronic signatures.

The signing process must incorporate a security procedure that requires the authentication of a signatory’s individual identity through a physical, logical, or digital credential, and the signing process must reasonably provide for the non-repudiation of the electronic signature. The signing process requirements also provide that the signature be logically associated with the signature page or document being signed, thereby providing the signatory with notice of the nature and substance of the document and an opportunity to review it before signing, and that the electronic signature be linked to the signature page or document in a manner that allows for later confirmation that the signatory signed the signature page or document. Finally, given that a signatory must execute an authentication document pursuant to Rule 302(b) before or at the time an electronic filing is made, the signing process must include a timestamp that records the date and time of the electronic signature.

The SEC also included a requirement in new Rule 302(b)(2) that, before a signatory initially uses an electronic signature to sign an authentication document, the signatory must manually sign a document attesting that the signatory agrees that the use of an electronic signature in any authentication document constitutes the legal equivalent of such individual’s manual signature for purposes of authenticating the signature to any filing for which it is. An electronic filer must retain this manually signed document for as long as the signatory may use an electronic signature to sign an authentication document and for a minimum period of seven years after the date of the most recent electronically signed authentication document.

**Responsibility**

The CCO has the overall responsibility for the implementation and monitoring of our e-signatures policy, practices, disclosures, and recordkeeping for the firm.

**Procedure**

The Firm has adopted procedures to implement the firm's policy and conducts reviews to monitor and ensure the firm's policy is observed, implemented properly and amended or updated, as appropriate, which include the following:

* Before a signatory initially uses an electronic signature to sign an authentication document, the signatory must manually sign a document attesting that the signatory agrees that the use of an electronic signature in any authentication document constitutes the legal equivalent of such individual’s manual signature for purposes of authenticating the signature to any filing for which it is provided;
* %firmName% will retain this manually signed document for as long as the signatory may use an electronic signature to sign an authentication document and for a minimum period of seven years after the date of the most recent electronically signed authentication document; and
* The signing process for signatories signing an authentication document must, at a minimum:
* Require the signatory to present a physical, logical, or digital credential that authenticates the signatory’s individual identity;
* Reasonably provide for non-repudiation of the signature;
* Provide that the signature be attached, affixed, or otherwise logically associated with the signature page or document being signed; and
* Include a timestamp to record the date and time of the signature.

The procedure described above is intended for compliance with SEC rules regarding the filing of regulatory documents with the SEC. The same procedures apply for the use of electronic signatures for customer documents with the exception of the requirement of a manual signature prior to signing electronically, so long as the document being signed electronically includes the provision that the customer agrees to the use of an electronic signature.

**Electronic Delivery And Signatures**

Federal securities law through the Electronic Signatures in Global and National Commerce Act of 2000 regulates the use of electronic media for transmitting documents and the recording and accepting of electronic signatures. This section outlines requirements when NTB uses electronic methods of delivery between NTB and its customers and the use of electronic signatures for internal purposes such as approval of new accounts.

**8.26.1 Electronic Delivery To Customers**

If NTB electronically transmits documents to customers and/or accepts signatures delivered electronically from customers, the following requirements will apply:

* The customer's consent will be obtained.
* Notice will be provided to customers that the information is available electronically.
* Customers who are provided electronic delivery have access to the information substantially equivalent to the access that would be provided if the information were delivered in paper form (*i.e.,* the electronically transmitted document will convey all material and required information). Customers will have ready access to the electronic document either through downloading or ongoing access online.
* NTB will evidence satisfactory delivery through the customer's informed consent agreeing to delivery of certain documents or obtaining actual confirmation the customer received the information.
* Electronic delivery is subject to NTB's policies and procedures to protect confidential customer information and ongoing review of NTB's security systems.

Electronic signatures may be used by designated supervisors to indicate approval/review of new accounts, orders, and other ongoing supervisory reviews. Supervisors will be assigned passwords which will be changed periodically to protect the security of the system.