Fund Industry Guidelines for Electronic Signatures

These Guidelines were developed by Fundserv Inc. in consultation with an industry working group, including The Investment Funds Institute of Canada. They are intended as guidance for the fund industry in order to facilitate a standardized approach to electronic signature (or e-signature) use and acceptability for Fundserv members.

Members should seek legal advice as to the applicable laws if they have any questions or require further information about electronic commerce and e-signatures and how they apply to their business. Fundserv believes that the following requirements are in compliance with applicable law, but takes no responsibility for reliance on the Guidelines by its members and is not providing legal advice to its members. The purpose of an e-signature is to establish a lasting and reliable record of intent to execute a document. Implemented correctly, and where applicable, an e-signature is functionally equivalent to a manual/ink signature on a paper document. When referring to e-signatures, this can be any electronic method that a person adopts in order to sign a document and that is in, attached to, or associated with the document. This could be an electronic depiction of a handwritten signature, or any other type of digital representation of the person's identification.

These Guidelines are for obtaining e-signatures from clients of Distributors for documents delivered to Manufacturers, Intermediaries, or other Distributors, by implementing a specific cryptographic technology called electronic signatures. These Guidelines are intended to be technology-neutral. There are many different and evolving ways to obtain electronic signatures. When an organization chooses to institute an electronic signature solution to implement e-signatures, then the following are the minimum requirements needed in order to adhere to these Guidelines. These Guidelines are in supplement to, and do not supersede, any applicable regulatory and legal requirements, as amended from time to time.

For the purposes of this Guideline:

- "**deliverer**" means a Distributor, including an Intermediary.
- "**e-sign service**" means an electronic signature solution to implement an e-signature.
- "**recipient**" means a Manufacturer, Intermediary or a Distributor, who has received from a deliverer a document signed with an e-signature or an instruction to take action, where the signer has authorized the instruction by signing with a e-signature.
- "**signer**" means the client of a Distributor.
- An "**electronic signature**", or "**e-signature**" refers to electronic information that a person creates or adopts in order to sign a document and that is in, attached to or associated with the document. These Guidelines do not prescribe the specific form that the electronic signature must take, as long as they comply with the functional requirement set out in the following document. For the purpose of these guidelines, "**e-signing**" a document refers to the act of applying an electronic/e-signature to a document.

1. **Document & Signature Security**
   Secure encryption must be applied for data in transit between the signer, the device used to capture the e-signature, the esign service, and the recipient.

   1.1 Document and Electronic Signature Protection
   - **i)** The process used by the deliverer must clearly indicate to the recipient when the signer has used an esign service.
   - **ii)** The document and e-signatures must be protected using electronic signature technology so that any attempt to alter the document's contents will render it invalid. The technology must also ensure that esignatures cannot be copied and pasted.
   - **iii)** The electronic signature mechanism shall be applied to e-signatures added to the document in order to build a comprehensive audit trail with the date and time that each e-signature was applied.
   - **iv)** The electronic signature must include satisfactory evidence that the signer is the true signer and not someone else.
   - **v)** The deliverer must establish that the document has not been modified or corrupted during delivery to the recipient.

   1.2 Ability to easily verify an e-signed record, ensuring long term reliability, independent of the e-sign service.
   - **i)** All e-signatures, time stamping, IP addresses, and audit trails should be directly associated with the document, so that:
     - document authenticity can be verified;
     - the record can securely travel through any email, storage, or archiving system approved by the recipient without being compromised or requiring additional programming; and
     - all information necessary to validate the e-signature contained within any PDF file complies with Long-Term Validation (LTV) principles.

2. **Signer Identity, Authentication & Attribution**

   2.1 Access to the documents must be provided in a secure manner, such that each signer is authenticated, and the correct documents will be presented, before allowing the signer access to the documents. Signer authentication options include:
   - **i)** user ID and password;
   - **ii)** ii. knowledge-based authentication;
   - **iii)** iii. leveraging existing credentials; or
   - **iv)** iv. third-party trusted identification services.

   2.2 Evidence of who actually clicked or otherwise applied an e-signature as the signer must apply to both remote and face-to-face transactions.

3. Signer Experience

3.1 Where required under electronic commerce rules pertaining to the financial industry, the signer must consent to executing a document in electronic form by acknowledging an appropriate Disclosure and Consent document, which may be obtained earlier as part of regulatory requirements. Other types of signers may not be required to provide specific consent (such as advisors, branch managers, compliance officers, etc.) where consent may be implied as part of the approved distributor policies for employees or independent advisors of such distributors (such as financial planners, etc.).

3.2 The signer must receive notice that the document has been, or will be, delivered electronically.

3.3 The recipient and the signer must have easy access to the document and should have the ability to download, print, and/or save the document for future reference. The document must be organized (including with formatting) in substantially the same manner as the non-electronic version of the document.

3.4 The document that is received by the signer and the recipient must be the same as the document sent by the deliverer.

3.5 The signer must be provided with a signature-verified copy of the signed documents once all signatures have been obtained and the signer must be provided with a reasonable amount of time within which to download and save the documents before the documents are archived.

3.6 The deliverer must have the ability to create an end-to-end trusted experience through white-labeling and integration with an existing identity. Subject to any other regulatory disclosure requirements, the deliverer brand and only their brand should appear across the transaction.

4. Delivery & Retention

4.1 The deliverer must deliver a document that is completely e-signed and in good order to each required recipient using a delivery method satisfactory to the recipient.

4.2 Digitized documents which have been e-signed must be backed up and included in disaster recovery programs in accordance with existing applicable document retention policies and requirements.

5. Data Security

5.1 Sufficient protection of company and customer data, both at rest and in transit, must be in place to meet compliance and local data privacy law requirements, in accordance with existing regulatory requirements.

5.2 The solution must satisfy any applicable Canadian data residency and disclosure requirements, if any.

6. Enforceability of the e-Signature (Best Practices)

6.1. The key to ensuring an enforceable e-signed record is to capture and reproduce as much relevant electronic evidence as possible.

- **i)** Create an audit trail of the entire electronic process from the steps to verify the identity of the persons signing the document all the way through to sealing electronically the document, securely archiving it, and making it retrievable.
- **ii)** Record and reproduce the exact records to build the person's understanding of what they were agreeing to and signing.
- **iii)** The exact order and appearance of all web screens, documents, and legal disclosures presented to signers.

6.2 When an e-sign service is used for any part of the solution, contractually and regularly verify the e-sign service's ability to meet the security and business continuity requirements.

6.3 Where applicable, an electronic signature is functionally equivalent to a wet/ink signature, however, not all documents may be electronically signed. Each of the deliverer and the recipient must satisfy itself whether, under 3 applicable law, an e-signature may not be effective for certain documentation, such as testamentary dispositions and beneficiary designations, trusts created by wills, powers of attorney regarding an individual's financial affairs or personal care, documents that create or transfer interests in land and that require registration to be effective against third parties, and negotiable instruments and documents of title.