eSign Policy of LivQuik Technology (India) Private Limited ("LivQuik")

Indian law has recognised electronic/digital signatures, or e-signatures,under the Information Technology Act, 2000 (IT Act). With its increased emphasis on improving the ease of doing business; streamlining the storage of records; and improving the safety, security, and cost-effectiveness of records, the Government of India has promoted the use of digital technologies by Indian citizens and corporations.

In consistency with the IT Act, LivQuik treats electronic signatures as equivalent to physical signatures, subject to a few exceptions. LivQuik shall allow the documents to be signed using any form of e-signatures. However, an e-signature must satisfy a numberof conditions, and certain checks must be done before it can be relied upon.

Below methods of electronic signatures shall be recognised as having the same legal status as handwritten signatures:

a. Electronic signatures that combine an Aadhaar identity number with an electronic Know-Your-Customer (eKYC) method (such as a one-time passcode). This method is known as the eSign online electronic signature service.

b. Digital signatures that are generated by an "asymmetric crypto-system and hash function." In this scenario, a signer is typically issued a long term (1- to 2-year) certificate-based digital ID stored on USB token, which is used—along with a personal PIN—to sign a document.

Reliability Conditions:

For the two types of e-signatures to be valid, they must satisfy the additional conditions as mentioned below:

a. E-signatures must be unique to the signatory (they must be uniquely linked to the person signing the document and no other person). This condition is met with a certificate-based digital ID.

b. At the time of signing, the signatory must have control over the data used to generate the e-signature (for example, by directly affixing the e-signature to the document).

c. Any alteration to the affixed e-signature, or the document to which the signature is affixed, must be detectable (for example, by encrypting the document with a tamper- evident seal).

d. There should be audit trail of steps taken during the signing process.

e. Signer certificates must be issued by a Certifying Authority(CA) recognised by the Controller of Certifying Authorities appointed under the IT Act. Only a CA licensed by the Controller of Certifying Authorities can issue e-signature or digital signature certificates.

If each of the Reliability Conditions is satisfied, then there is a legal presumption in favour of the validity of any document signed using an electronic signature.

If the validity of an electronic contract is disputed, the party claiming validity of the contract must be able to demonstrate that the essentials of a valid contract are fulfilled and that the parties in fact did execute the contract using a technology that followed the Reliability Conditions.

A contract executed using email as the first authentication method or that adds a second factor of authentication, such as a password or phone PIN, shall be considered as valid, provided it satisfies the requirements of the IT Act.

(Records signed using electronic means other than an e-signature as prescribed under the IT Act are not invalid. Contracts that are otherwise validly concluded shall not be rendered invalid merely because they were made in electronic form. Contractual liabilities" could arise by way of electronic means and that such contracts could be enforced to law. Section 10A of the IT act enables the use of electronic records and electronic means for the conclusion of agreements contracts and other purposes. Documents signed through other electronic modes other than Digital Signatures are valid and admissible before judicial bodies.)

Where electronic signatures cannot be used:

The following documents cannot be electronically signed and must be executed using traditional "wet" signatures in order to be legally enforceable:

- Negotiable instruments such as a promissory note or a bill ofexchange other than a cheque
- Powers of attorney
- Trust deeds
- Wills and any other testamentary disposition
- Real estate contracts such as leases or sale agreements

eSigning the documents with certain Government bodies:

Government authorities such as the Ministry of Corporate Affairs, Department of Revenue, and Ministry of Finance accept electronic records authenticated using digital signatures. In the case of e-filing with the Ministry of Corporate Affairs, income tax and GST (goods and service tax) filings, digital signatures shall be the preferred mode of execution.

Following of industry's best practices to help satisfy the requirements of the IT Act:

If email or another form of authentication is used to sign a document electronically, then the following industry best practices should be implemented to help satisfy the requirements of the IT Act:

- Sending a verification request to a unique email address, or sending an OTP to the signing party's mobile phone.
- Obtain the signing party's consent to do business electronically.
- Demonstrate clearly that the signing party intended to sign the document electronically by the particular method used.
- Track the process securely and keep an audit trail that logs each step.
- Secure the final document with a tamper-evident seal.

LivQuik hereby adopts the above wordings as its 'eSign Policy' in its Board Meeting dated 21st June, 2021.