1. GENERAL INFORMATION

- **Signature technology:** The developer must describe the type of signature technology provided to the end user, i.e. digital or electronic.
  - Details: Provide a brief description of the signing process and the advantages of using the proposed technology
- **Technology security:** The designer must also provide information on the security mechanisms applied to prevent internal and external IT security threats (such as policies, procedures, security tools, etc.).
  - Details: Does the designer meet the various security requirements needed to comply with applicable laws such as *Act respecting the protection of personal information in the private sector* of Québec, the federal *Personal Information Protection and Electronic Documents Act* (PIPEDA), and security standards such as ISO 3200, ISO 27001 and others?
- **Hosting locations**: The OACIQ prefers hosting locations in Québec and Canada, where privacy standards are recognized and secure. Note that the law requires that a privacy impact assessment (PIA) be carried out by the company in the event of the communication and storage of information, including personal information, outside Québec.
- **Hosting of the solution**: The developer must indicate the location(s) where the solution is hosted, as well as those of backup sites.
- **Hosting of signed forms**: The developer must indicate the location(s) where the data is stored (i.e. forms) and of the backup sites. In the case of a signature technology integrator, the place of incorporation of the signature technology provider must be specified.
- **Redundancy system**: The developer must indicate the redundancy strategy implemented to ensure high availability.
  - Details: If no redundancy strategy/system is in place, the developer must indicate:
    - The maximum period during which information could be lost based on the backup strategy.
    - The process the developer intends to put in place to guard against the loss of data in case of equipment failure between two backups.

2. MANAGEMENT OF OACIQ FORMS

- **File formats to upload forms for signing**: The developer must indicate the various authorized file formats on which the user will be able to sign.
- **Customization of signature areas**: The developer must indicate the type of user authorized to customize the various signature areas and specify the maximum number of signatures per form.
- **Saving signature areas as a template**: The developer must indicate if the solution allows the saving of form templates with pre-established signature areas and the creation of a library of forms for signing.
  - Details: This way, when the user wishes to have an existing form signed, he will not need to define the signature areas as these will already have been saved.

- **Storing of predefined forms on the provider's site**: The developer must indicate if it is possible to have a library of predefined forms and specify the maximum number and the file format of forms that can be stored.
- **Automatic matching of uploaded form with a predefined template**: The developer must indicate if the system allows the automatic matching of a form uploaded by the user with a predefined form contained in the forms library.
- **Multilingual interface – English and French:** The developer must provide a copy of the forms management interfaces for quality validation.
- **Interface customization**: The developer must indicate if the forms management interface can be customized with a broker's colours/logos.
    - Details: A sample customization must be provided.

3. SIGNATORIES MANAGEMENT, SECURITY OF ACCESS

- **Management of multiple signatories**: The developer must indicate if the system allows the management of multiple signatories for both the buyer and the seller and specify the maximum number of signatories.
- **Management of signatory flow/sequence**: The developer must describe the signatory management process.
    - Details: The developer must describe how the user can control the signature flow of signatories according to one of these options:
        - ✓ *Series/sequence process*: Implies that a set of forms for signing can only be sent to the next signatory when the first signatory has successfully completed the signing process of all the forms.
        - ✓ *Parallel process*: Implies that a set of forms for signing can be sent to all signatories simultaneously, regardless of completion status.
    - Should the signatories be represented by various stakeholders, the electronic or digital signature system must allow a business process.
- **Customization of emails to all signatories**: The developer must provide an example of the customization of emails sent to signatories.
    - Details: If customization is not possible, the developer must provide a sample message that will be sent to signatories.
- **Customization of email according to signatory language**: The developer must indicate if it is possible to customize the language of the email sent to each signatory.
- **Security levels (Signatory identity verification):** The developer must describe the process and the various methods for verifying the signatory's digital identity before accessing the site containing the forms to be signed.
  Details: The signatory's identity must be verified by a combination of at least (2) two of the methods detailed below:
        - ✓ **Proof of identity** validated by official documents such as health insurance card, passport, driver's license, etc.

- ✓ A **knowledge-based confirmation**, which can be static (using personal information collected previously or established at a specific point in time) or dynamic (using personal information collected or generated over time).
- ✓ A **confirmation of biological or behavioural features** (facial features comparison, iris comparison, fingerprint comparison, voice comparison, data analysis, etc.).
- ✓ A **confirmation by a trusted arbitrator** (Respondent, notary, certified agent)
- ✓ A **confirmation by an element known to the user** (e.g. stored secret tokens or pre-recorded intelligence tokens), by an **element that the user possesses** (e.g. matrix secret token, out-of-band token, single-factor one-time password feature or single-factor cryptographic device) or by an **element that the user produces or that characterizes the user** (such as biometric data such as fingerprint, retinal scan and facial recognition).

Confirmation may involve a secure interaction with a physical or electronic validation process such as a push notification on an out-of-band device like a smartphone.

The identity verification method (with a valid photo document issued by a government) should be preferred as it represents a lower risk compared to other methods.

- **Security of transactions:** The developer must provide guarantees on the security of electronic signatures.
  To do this, he must:
  - ✓ **Guaranteeing the integrity of signed documents**

  The developer must demonstrate that a signed document cannot be altered. He must describe the certification process of PDF documents used to ensure their authenticity.
    - Details: Once the signing process is complete, the documents must be electronically sealed using a tamper-proof digital seal generated from a Public Key Infrastructure (PKI). This seal confirms the validity of the signature and guarantees that the electronic document has not been altered or modified since its signature date.
      If the developer does not use a digital signature, he must demonstrate that the process used guarantees the authenticity of signed documents.
  - ✓ **Issuing a certificate of completion**

  This electronic certificate strengthens the security of digital signatures by providing detailed information on each signatory. This information must include the consumer's declaration confirming the signatory's agreement to use the electronic signature, the image of that signature, the timestamps associated with key events, the signatory's IP address and other identification data. These elements help validate and authenticate the signatory's electronic signature.
- **Logging of transactions:** The developer must demonstrate the follow-up procedure for the transactions performed on the system. To do this, he must provide an audit trail for each transaction, which will act as an electronic record of all the actions carried out on the digital

document. This audit trail must detail the history and timestamp (which links the date and time to the data in such a way as to reasonably exclude the possibility of undetectable modification to the data and which must be based on an accurate clock linked to Coordinated Universal Time), including when the document was opened, viewed and signed. In the event of a dispute or doubt about an electronic signature, this audit trail, which is accessible to all participants in the transaction, can be used to provide evidence and resolve objections.

- Details: The developer must provide a copy of the transaction log.

- **Considerations for a long-term validation:** The developer must demonstrate that all information required to validate the electronic signature will be available for as long as the record needs to be kept. The electronic signature must be able to be verified and confirmed over time.

- **Allocation of access rights:** The developer must describe the tools used for access management. He must indicate which individual(s) authorize(s) which individuals and the mechanisms guaranteeing these individuals' privacy of access (password changes).
  - Details: Since the user may use the signature system without being a member of a real estate board, it will be important to know if the developer requires the OACIQ to be solely responsible for allocating access rights, as this solution would not be desirable or viable.

- **User groups:** The developer must identify the user groups that have access to the system. This description must define what users are part of these groups, their rights and privileges – administrators, users, signatories, etc. This access management must abide by the "least privilege" principle (a security concept in which a user is granted the minimum level of access [or permissions] required to perform their job) and the "need-to-know" principle (whereby access to a file must only be given to duly authorized and authenticated users) to minimize the risk of data exposure.

- **Maintenance of privacy of access:** The developer must indicate the mechanisms used to preserve user privacy, especially in cases where the application is accessible to clients and electronic authentication is required. Mechanisms such as multiple authentication are expected.

- **Termination of access rights:**

The developer must describe the processes used to remove access rights to the system from users who no longer have such privileges, regardless of reason: change of agency, end of subscription to the service, etc. The process must allow for timely recognition and immediate implementation of access termination.

4. MANAGEMENT OF SIGNATORY FLOW

- **Expiration date/signing deadline for signatories:** The developer must indicate if the system allows for the application of a signing deadline, either an end date or a period of hours or days.
- **Management of reminders to signatories**: The system must include a follow-up and reminder mechanism to let signatories know that a document or series of documents are ready to be signed. The developer must provide an example of this reminder and ensure that it is available in French.
- **Automatic email alert to process manager**: The system must allow for an automatic email notice to be sent to the user/manager to follow-up on the progress of the signature process. All signatories must receive confirmation that the process is complete. Each can then download and save the document.
- **Viewing of progress of signature process**: The system must allow for on-screen viewing of the progress of the signing process.

5. FORMS SIGNING PROCESS

- **Multilingual interface – English and French**: The developer must make sure that all interfaces displayed for the signatories are available in English and French.
- **Browser access – IE, Safari, Firefox, Chrome**: The developer must provide a list of all authorized browsers and their versions.
- **Android, iPhone, iPad app**: The developer must indicate if the signature solution has a specific app for Smart Phones and/or Tablets and provide a list of authorized platforms.
- **Consent display/acceptance before signature process is initiated**: The developer must allow for consent wording to be displayed and accepted by the signatory before the signature process is launched.
    - Details: The developer must provide for the consent wording to be available in English or French.
- **Platform accepted for the signature process**: The developer must specify the types of platforms that signatories can use during the signing process.
- **Signing option**: The developer must describe the various signing options available to signatories. The use of the keyboard with selection of calligraphy type would be a minimum basic option.

- **Assisted navigation in signature areas**: The developer must allow signatories to navigate quickly from one signature area to another and inform the signatory about the percentage or level of completion of the signing process.
- **Clearly identified signature areas**: The system must clearly indicate the precise areas where signatories must enter either their initials or their signatures.
- **Saving of signed forms**: The system must allow for signed forms to be saved on the signatory's platform and for forms to be hosted and stored on the developer/solution provider's server(s).
- **Exporting a set of signed documents**: The developer must allow the signing process manager to be able to select and export a set of signed documents in PDF format.

6. MANDATORY OR EQUIVALENT INCLUSIONS IN THE CONTRACT BINDING THE PROVIDER TO CLIENTS

- The contractual clauses listed below or equivalent clauses shall be included in any contract binding the provider to a client, in English or French, depending on the language of the contract.
- The provider shall provide, in view of his certification by the OACIQ, a copy of the contract he intends to use in his business relationship with clients.
- In the event the clauses listed below are not fully reproduced in the contract, additional fees will be required for approval of equivalency.

Preamble	WHEREAS the Client is an agency/broker within the meaning of the *Real Estate Brokerage Act* and its regulations and is subject to the supervision and control of the Organisme d'autoréglementation du courtage immobilier du Québec (the "OACIQ"), and its agencies and brokers are subject to the powers of the Syndic of the OACIQ;
Preamble	WHEREAS the Client holds data, applications, documents and confidential information, including personal information (hereinafter referred to as the "information assets"), whose collection, storage, use, communication and destruction are subject to the regulations under the *Real Estate Brokerage Act* (c. C-73.2) and the provisions of the *Act respecting the protection of personal information in the private sector* (c. P-39.1) (hereinafter referred to as the "Private Sector Act");
Preamble	WHEREAS, in accordance with its legal obligations, the Client is required to protect the personal information it collects, uses, stores, discloses and destroys and is required, among other things, to notify the persons concerned of the name of the third party for whom the personal information is collected, the name of the third party to whom personal information collected must be disclosed and the possibility that personal information may be disclosed outside Québec;

Preamble	WHEREAS, in accordance with its legal obligations, the Client must carry out a Privacy Impact Assessment (PIA) in the event of the communication and storage of personal information it holds outside Québec;
Preamble	WHEREAS the Client must, if it has reasonable grounds to believe that a *confidentiality incident* within the meaning of the *Private Sector Act* has occurred and that this incident involves personal information that it holds, take reasonable measures to reduce the risk of harm being caused and to prevent further incidents of the same nature from occurring and must also, if the incident presents a serious risk of harm, notify the persons concerned and the competent authorities;
Preamble	WHEREAS the Client and the Provider, in accordance with their legal obligations, wish to agree upon obligations and procedures designed to ensure the confidentiality of the Client's information assets at all times, including the personal information received, used, stored or disclosed in connection with the performance of this contract;
Protection of information assets	The Provider acknowledges that it is responsible at all times for ensuring the protection and confidentiality of the information assets, including personal information, that it receives as part of this contract, during their communication, use, possession, conservation and destruction.
Subcontractors	The Provider shall supervise the activities and obtain contractual undertakings from its subcontractors so as to ensure that the latter comply with the obligations stipulated in this contract, including those relating to the communication, use, retention, destruction and protection of personal information. **The Provider warrants to the Client that all such obligations shall be fully performed.** Notwithstanding the terms of the agreements entered into by the Provider with its subcontractors, the Provider is responsible for the performance of all obligations set forth in this contract regarding the provision of services and the preservation of the confidentiality of the information assets, **and the Provider warrants to the Client that all such obligations shall be fully performed**.
Partitioning of Information Assets	The Provider undertakes to provide the services and to store the Client's information assets in such a way as to ensure the logical partitioning thereof. The parties acknowledge that this does not exclude using the storage facilities of a third party acting as a subcontractor of the Provider.
Dedicated equipment	*Note: To the extent that the sensitivity of the information warrants and justifies higher costs, some providers offer dedicated equipment. If that option is selected, the following clause may be used*: The Provider shall use dedicated equipment for the purposes of providing the services, in order to ensure the partitioning

	of the information assets of the client. The parties acknowledge that this does not exclude using the storage facilities of a third party acting as a subcontractor of the Provider.
Limitation of geographical location	The Provider shall notify the Client of the geographic location of the facilities, equipment and systems used for the performance of the contract and on which are stored the client's information assets, and shall use only such facilities and equipment that are located within the territorial boundaries of Canada, preferably Québec. The Provider undertakes to notify the Client immediately and each time the Provider or a subcontractor under this contract uses hosting facilities located outside Québec.
Notification and cooperation in the event of an official order or demand to have access to confidential information	In the event that the Provider or one of its subcontractors receives a court order, subpoena or any other demand from a competent authority for the communication of information assets, the Provider undertakes to notify the Client within four (4) hours. The Provider's obligations under this paragraph shall apply to any request resulting in client's information assets being accessed or communicated, regardless of whether or not the order, subpoena or any other demand from a competent authority is specifically focusing on such assets. The Provider undertakes, to the extent permitted by Québec laws, verify the legality of the procedure for the issuance or obtaining of the order, subpoena or any other demand from a competent authority. Unless it is a request of any kind from the OACIQ, the Provider undertakes to either contest the order, subpoena or any other demand from a competent authority or request the postponement of its execution, in order to allow the Client to review their substance and, if appropriate, to assert its rights or those of its clients. In the event that the Provider is unable to notify the Client of competent authority or summon in a timely manner, or cannot legally inform the Client thereof contemporaneously, the Provider shall so notify the Client as soon as it is legally allowed to do so. The Provider shall, to the extent permitted by Québec laws, maintain a record of all orders or demands.

Confidentiality security	The Provider shall adopt and implement all appropriate security measures to maintain and protect the confidentiality, integrity and accessibility of the client's information assets, by an encryption mechanism of documents and information at the time of their transmission and preservation, but also at the centres where these information assets are stored. The Provider shall also adopt and implement reasonable measures to ensure controlled access thereto, authentication of users and operational continuity, which measures shall take into account the sensitivity of the information assets received and/or disclosed under this contract, the purpose for which it is being used, the quantity thereof and the medium on which it is stored. The rules and procedures so adopted must also seek to prevent confidentiality incidents and within the meaning of the *Private Sector Act*, breaches, errors (such as unsupervised system changes), malfeasance, and unauthorized disclosure or destruction of information assets. The Provider shall also adopt an audit mechanism for identifying and managing the risks faced by the Provider, for verifying compliance with such rules and procedures.
Confidentiality security	The Provider acknowledges that the confidential information assets gathered and stored by the Client in the course of its operations shall be disclosed to it and that it shall have access thereto. The Provider further acknowledges that the information assets remain the exclusive property of the Client or that the Client is the holder thereof within the meaning of the *Private Sector Act*, and that the Client may consequently reclaim the information assets, and that any unauthorized disclosure of the information assets, including personal information, could cause it substantial harm.
Confidentiality security	In performing this contract, the Provider shall maintain the confidentiality of the information assets and take all appropriate measures to that end at all stages of the performance of the contract, including: • Maintaining the confidentiality of user IDs, passwords and encryption keys in accordance with industry best practices; • Having any person assigned by the Provider to handle or process the information assets sign beforehand a confidentiality undertaking and an undertaking to comply with security measures, restrict access, communication and disclosure of the information assets to such persons alone, and carry out background checks prior to their recruitment. • Using information assets, including personal information, solely for the purposes for which they were communicated; • Not to disclose the Client's information assets, including personal information received and/or disclosed under this contract, to third parties, except insofar as this is necessary for the performance of this contract. Cooperating

	with the Client and its clients, as the case may be, in order to allow those persons concerned to exercise their right to have access to and correct their personal information; • Cooperating with the Client for the purposes of erasing or destroying personal information and user profiles in accordance with the applicable retention schedule; • Not to reproduce the Client's information assets, including personal information received and/or disclosed under this contract, unless such reproduction is required for the performance of this contract. • Cooperating with any investigation or audit concerning compliance with the confidentiality of information assets, including personal information.
Right to verify	The Provider acknowledges the Client's right to ensure that the obligations stipulated above, the *compliance with the Private Sector Act* and the *Real Estate Brokerage Act*, are respected at all times, including the right to have access to the Provider's facilities if necessary. The Provider undertakes to cooperate, together with the Client, in any investigation or audit by the relevant authorities, including the OACIQ.
Notification and cooperation in the event of a breach of confidentiality of personal information and/or a breach of security	The Provider shall immediately notify the Client, within four (4) hours, of any breach or attempted breach by any person of the obligations relating to the confidentiality of personal information disclosed under this contract, of any confidentiality incident within the meaning of the *Private Sector Act*, of any unauthorized access or attempted access or of any breach of the confidentiality of the Client's information assets. The Provider shall in addition take all necessary action to mitigate the risk of an ongoing breach, conduct an investigation to identify any vulnerabilities and take the necessary remedial measures to avoid a repetition of such an incident. The Provider shall allow the Client or any person designated by the Client to carry out any audit relating to the confidentiality of personal information. To this effect, the Provider will allow the Client or any person designated by the Client to have access to any place, material, document or equipment in connection with any breach or attempted breach of the obligations relating to the confidentiality of personal information. The parties shall jointly analyze and manage the situation to minimize the risks and identify the relevant responders in light of the nature of the risk. The Provider shall take any measures requested by the Client to reduce the risk of harm being caused.

Insurance	The Provider shall take out and maintain in effect for the duration of the contract, at its sole expense, with a recognized insurer, a professional liability insurance policy providing coverage of at least five hundred thousand ($500,000) Canadian dollars per occurrence of the risk, with a deductible not exceeding $10,000) covering without limitation loss and damage resulting from errors or omissions in the performance of the Contract. Such policy must also include equivalent coverage against the risk of hackers who may illicitly gain access to the Client's information assets, as well as the risk of an error or omission attributable to the Client, and shall include a rider against destruction, corruption, loss and other similar risks in respect of the Client's data, information, including personal information, and documents.
Expiration, Termination, cancellation	The Provider shall return all information assets received and/or disclosed under this contract to the Client within 30 days of the date of expiration, termination or cancellation of the contract, regardless of the nature of the information, documents or the medium on which they are stored. As of the date of expiration, termination, or cancellation of the contract, the Provider undertakes not to keep a copy of or make any further use of the information assets, including the personal information received and/or disclosed under this contract. At the Client's express written request, the Provider undertakes to provide the Client with proof thereof that is acceptable by the Client. The Provider's obligations relating to the confidentiality of personal information received and/or disclosed under this contract shall survive its expiration, termination or cancellation.