ELECTRONIC OR DIGITAL SIGNATURE SYSTEM: Technical specifications

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 security levels, and the advantages of using the proposed technology
- **Hosting locations:** The only authorized hosting locations are Canada and USA.
- **Hosting locations:** 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 put in place.
    - 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.

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.

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**: The developer must describe the process and various security mechanisms available to allow the signatories to access the secure site containing forms for signing.
    - Details: At a minimum, the signature solution must allow the definition of a first security level to access the signing site.
        - *Password required to access the site – SMS, telephone*: This level of security will allow the user to configure a password that will be sent by phone or by SMS (or any form other than email) to the various signatories.
        - *Knowledge base, i.e. validation using questions by a third party*: This security level allows the user to delegate a third party, e.g. a credit reporting agency such as Equifax, to manage access to the secure site. In this case the signatory will have to answer a series of questions relating to his credit file over the phone. If the answers are correct, the signatory will gain access to the secure site.

- **Logging of transactions**: The developer must demonstrate the follow-up procedure for the transactions performed on the system. The log must indicate the person performing the transaction as well as the date and time. In addition, the developer must demonstrate that the following information is kept for all signatories: the IP address used by the signatory and the date and time at which the documents were received, the forms signed and the documents returned.
    - Details: The developer must provide a copy of the transaction log.

- **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.

- **Privacy protection**: 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.

- **Cancellation 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.

MANAGEMENT OF SIGNATORY FLOW

- **Expiration date/signing deadline for signatorie**s: 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.
- **Viewing of progress of signature process**: The system must allow for on-screen viewing of the progress of the signing process.

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.
    - o 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.
- **Procedure to prevent alteration of a signed document**: The developer must demonstrate that a signed document will be unalterable. He must describe the process that will be used to certify the PDF documents used in order to ensure their authenticity.

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 chosen by the client.
- 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 a agency/broker within the meaning of the Real Estate Brokerage Act and the regulations thereunder 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 is in possession of Confidential Information, including personal information, whose storage, use and destruction are subject to the regulations under the Real Estate Brokerage Act and the provisions of the Act respecting the protection of personal information in the private sector;
Preamble	**WHEREAS** the Client is obligated to notify the persons concerned of the location where their personal information is stored;
Preamble	**WHEREAS** the Provider recognizes the importance of maintaining the confidentiality of Confidential Information, including personal information, and that any unauthorized disclosure thereof could cause substantial harm to the Client and those persons to whom such information pertains;
Preamble	**WHEREAS** the Client and the Provider, in accordance with their legal obligations, wish to agree upon obligations and procedures designed to ensure the preservation of the confidentiality of Confidential Information and personal information communicated to them in connection with the performance of this Contract;
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. Notwithstanding the terms of the agreements entered into by the Provider with its subcontractors, the Provider is responsible for the performance of all obligations undertaken pursuant to the Contract regarding the provision of services and the preservation of the confidentiality of Confidential Information and personal information, and the Provider hereby warrants to the Client that all such obligations shall be fully performed.
Partitioning of Information Assets	The Provider shall provide the services and to store the Client's documents 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	*N.B. 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 applications and Information Assets, and shall use only such facilities and equipment that are located within the territorial boundaries of Canada or the United States of America.
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 other administrative demand for the communication of Confidential Information, the Provider shall so notify the Client within four (4) hours. The provider's obligations under this paragraph shall apply to any request resulting in client's documents or confidential information being accessed or communicated, regardless of whether or not the request or order is specifically focusing on these. The Provider shall, to the extent permitted by law, verify the legality of the procedure for the issuance or obtaining of the order or demand, and shall either contest same or request the postponement of its execution, in order to allow the Client to review the substance of the order or demand 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 the order or demand 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. In all circumstances the Provider undertakes not to voluntarily allow interception, and not to voluntarily disclose/communicate the Client's communications or documents in the absence of the appropriate warrant or subpoena, regardless of the possibility for the requesting party or any other interested party to grant the Provider legal immunity. The Provider shall, to the extent permitted by law, maintain a record of all orders or demands seeking access to the Information Assets. The Provider shall assist the Client in contesting the order or demand and, if asked to do so, shall provide information concerning the services provided at the Client's request.

MANDATORY OR EQUIVALENT INCLUSIONS IN THE CONTRACT BINDING THE PROVIDER TO CLIENTS (CONTINUED)

Confidentiality security	The Provider shall adopt and implement all appropriate security measures to maintain and protect the confidentiality, integrity and accessibility of the Information Assets, by an encryption mechanism of documents and information at the time of their transmission and preservation as well as reasonable measures to ensure controlled access thereto, authentication of users and operational continuity, which measures shall take into account the sensitivity of the information, 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 security incidents and breaches, errors, malfeasance, and unauthorized disclosure or destruction of information. The Provider shall also adopt an audit mechanism for verifying compliance with such rules and procedures.
Confidentiality security	The Provider acknowledges that Information Assets and documents containing confidential information, including personal information gathered and stored by the Client in the course of its operations ("**Confidential Information**") will be communicated to it and that it will have access to such documents. The Provider further acknowledges that all Confidential Information remains the exclusive property of the Client or that the Client is the holder thereof within the meaning of the A*ct respecting the protection of personal information in the private sector* (Québec), and that the Client may consequently reclaim documents containing Confidential Information, and that any unauthorized disclosure of Confidential Information could cause it substantial harm.
Confidentiality security	In performing the Contract, the Provider shall maintain the confidentiality of the Confidential Information and take all appropriate measures to that end at all stages of the performance of the Contract, including: o Maintaining the confidentiality of user IDs, passwords and encryption keys in accordance with industry best practices; o Have any person assigned by the Provider to handle or process Confidential Information sign beforehand a confidentiality undertaking and an undertaking regarding security measures whose terms are consistent with those set out in Schedules Confidentiality undertaking and Undertaking-Information security measures and limit access, communication and disclosure of Confidential Information to such persons alone; o Use Confidential Information solely for the purposes for which it was communicated; o Cooperate 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; o Cooperate with the Client for the purposes of erasing or destroying personal information and user profiles in accordance with the applicable retention schedule; o Cooperate with any investigation or audit concerning respect for the confidentiality of Confidential Information;
Right to verify	The Provider acknowledges the Client's right to ensure that the obligations stipulated above and in the *Act respecting the protection of personal information in the private sector* and the *Real Estate Brokerage Act* are respected at all times, including the right to have access to the Provider's facilities if necessary, and the Provider undertakes to cooperate, together with the Client, in any investigation or audit by the relevant authorities.
Notification and cooperation in the event that security is compromised	The Provider shall notify the Client within four (4) hours of any unauthorised access, attempted unauthorised access, or breach of the confidentiality of Confidential Information, and of any incident that could jeopardize the security or confidentiality of Confidential Information. The Provider shall in addition take all necessary action to mitigate the risk of an ongoing breach, conduct an investigation in order to identify any vulnerabilities and take the necessary remedial measures to avoid a repetition of such an incident. The parties shall jointly analyze and manage the situation in order to minimize the risks and identify the relevant responders in light of the nature of the risk.
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, 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 Information Assets of the Client, as well as the risk of an error or omission attributable to the Client, and the risk of destruction, corruption, loss and other similar risks in respect of the Client's data, information and documents.
Termination and destruction	Upon the expiration or earlier termination of the Contract, the Provider shall return all Information Assets and Confidential Information to the Client within 30 days of the expiration or termination date, regardless of the nature of the information or the medium on which it is stored.