IMPLEMENTATION OF AN ELECTRONIC DOCUMENT MANAGEMENT SYSTEM: TECHNICAL SPECIFICATIONS FOR AGENCIES AND BROKERS ACTING ON THEIR ACCOUNT

IMPORTANT

The OACIQ reserves the right to change its requirements based on technological and legal developments.

1. DATA PRESERVATION

EXPLANATORY NOTES:

The preservation of information refers particularly to two aspects that should be distinguished:

- **Storage**: Recording information for future re-use. Storage must make information available to the persons authorized to re-use it.
- **Backup:** Backup is the action of duplicating system data and keeping it in a safe place so that the system data can be restored following an equipment breakdown (hard drive system failure) or an undesired or accidental modification of the data.

1.1. Content of the backup

The designer should describe:

- ☐ The files that are included in the backup procedure; and these files must be grouped according to their level of sensitivity (high, medium and low)
- ☐ The full content that is backed up
- ☐ The data storage system (a file system, a database or both)

Examples:

- ☐ System data is backed up in a database. The whole database used for the solution is backed up, including system management data
- ☐ System data is backed up in files and not in a database. Only the files of active brokers are backed up

1.2. Storage unit

The designer should indicate the type of storage units that are used for file backup.

Examples:

- ☐ Local external hard drive
- ☐ Network Attached Storage (NAS)
- ☐ Backup sent to an enterprise specialized in data backup
- ☐ Magnetic tape

1.3. Procedure

The designer should describe the backup procedure by indicating

- ☐ The backup strategy that ensures a document's integrity throughout its life cycle: use of full backup, incremental backup, differential backup

- ☐ The frequency and the period of retention of different types of backup
- ☐ The daily, weekly, monthly and annual backup techniques, if applicable

Examples:

- ☐ A full backup of database is carried out every night. This copy is then sent to an enterprise specialized in backup and is kept for two months
- ☐ A full back up is made every week on Monday at midnight (kept for 2 weeks) and a differential backup is done every day at midnight (kept for 2 weeks)
- ☐ A full backup is made every day at midnight (kept for one month on an external local hard drive and sent on a daily basis to the external backup department for conservation for a week). An incremental backup is performed every hour (kept for two days on a network hard drive)

1.4. Storage location

The designer must indicate the storage location of the backup copies. The OACIQ prefers storage 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.

These copies must be stored offsite of the residence location of the source information, in a secure location protected from bad weather and damage.

Examples:

- ☐ The backup is made on a network hard drive located outside of the system operation site; the servers' location containing these hard drives is secured and its access is possible only for persons responsible for backups

As the backup is made on magnetic tapes in the system operation premises, this necessitates bringing these tapes, on a daily basis, in a fireproof safe to an external location to […]

1.5. Retrieval

The designer must explain the procedure for file retrieval in the event of a major breakdown as well as the estimated time of retrieval.

1.6. System Redundancy

The designer must indicate the redundancy strategy in place. If there is no strategy or a system redundancy in place, the designer must indicate:

- ✓ The maximum period during which a data loss may occur as a result of the data backup strategy.
- ✓ The process that he intends to put in place to guard against data losses, should an equipment breakdown occur between two data backups.

1.7. Backup log

The designer must be able to present a backup log (or an execution log) indicating the various parameters of performing backups. The backup log must contain at least the following elements:

- ☐ The backup date
- ☐ The backup type; and
- ☐ Anomalies, if any.

2. INFORMATION CAPTURE, STORAGE AND ARCHIVING

EXPLANATORY NOTE:
The role of archiving is different from that of backup.

- While the aim of a backup is to restore the previous data state, archiving is the set of actions put in place to collect, classify and preserve documents until their final disposal, while ensuring that their integrity, availability and confidentiality are preserved.

The two approaches complement each other in the information management plan.

2.1. System content types

Management of registers and records prescribed by the *Regulation respecting records, books and registers, trust accounting and inspection of brokers and agencies*

The system must allow the management of all registers and records prescribed by the *Regulation* or some of them. The designer must identify the type of registers or records assumed by the system and describe the mechanisms that ensure the inclusion of documents according to the record evolution context and dependency between documents:

- Depending on the record type (brokerage contract record or transaction record), this cannot be completed without including in it the mandatory documents and information
- The system must allow attaching to a record any type of document required for its completion
- During the record evolution, some documents become mandatory. Therefore, they must be mandatory at certain times, depending on the record status

Examples:

- A listing record must include a brokerage contract.
- The sale of a co-ownership must contain an agreement of co-ownership.
- When submitting an accepted promise to purchase with a down payment, the copy of the cheque and the trust receipt must be added to the record.
- Etc.

2.2. Content of the archive

The designer must describe:

- ✓ The method(s) of integrating the documents listed above into the EDM system.
- ✓ Permitted digital document formats (e.g. pdf, jpg, msg)

Examples:

- ✓ Documents can be created electronically or digitized from paper documents.
- ✓ Integration can include scanning paper documents and importing electronic files.
- ✓ The system allows the integration of PDF files only.

2.3. Digitization of documents

2.3.1. Digitization software integrated into the system

The designer shall describe the digitization procedure and present:

- The digitization procedure specifying, in particular, the steps to be performed by users, the devices used and the settings to be applied
- The transfer mechanisms through which the files are integrated into the EDM solution

The designer must ensure that digitization abides by the requirements of the *Legal framework for information technology Act*. For more details, read the following articles "Document before you destroy!", "Electronic document management: Digitization, give it more importance", "Electronic document management: some pitfalls to be avoided" and "Quality control: a step that should not be overlooked" as well as the guide "Digitization: Go for quality and document your process! " available on the OACIQ website.

The OACIQ recognizes the digitization settings recommended by the Bibliothèque et Archives nationales du Québec (BANQ) i.e., an image resolution of **300 dpi (ppp)**.

2.3.2. Digitization software non-integrated into the system

The designer must specify:

- How documents will be added to the solution
- The nature of the relationship between the digitization system and the EDM system, if applicable
- How he or she intends to disseminate sound digitization practices to clients, for example by providing a digitization procedure or a procedure model

2.4. Classification and indexing

The designer must describe:

- ✓ Classifying documents by specifying the basic criteria.
- ✓ The metadata profile for indexing documents and thus improving their search and retrieval.

Examples:

- ✓ Documents can be organized into appropriate categories (e.g. according to their level of sensitivity) to make their management and retrieval easier.
- ✓ The system allows the following metadata to be entered: type of document, signature date.

2.5. Conservation and sustainability of media

The designer must describe:

- ✓ The conservation procedure for archived documents
- ✓ The validation and migration procedure for documents and data

Examples:

- ✓ The retention policy he intends to implement, which will determine the period during which documents and data must be kept according to their categories. This includes managing modification versions and histories.
- ✓ The procedure he intends to implement to migrate documents to new formats or systems as technologies evolve to ensure information sustainability.
- ✓ The procedure he will implement to periodically verify that archived documents are still accessible and intact, and that the way they are stored meets regulatory and organizational requirements.

2.6. Destruction or elimination

The designer must describe how documents will be securely deleted once their retention period has expired. This may include the permanent deletion of files, deletion of back-up copies and secure disposal of physical media, where appropriate.

3. DATA INTEGRITY AND SECURITY

EXPLANATORY NOTE:

The integrity of a document refers to its accuracy and completeness and results from two elements:

- When there is a possibility to verify that data is not altered or destroyed erroneously or without authorization and is fully maintained.
- When the medium carrying this data provides it with the stability and durability required.

Confidentiality consists in ensuring that data is used only by authorized persons and for the purpose for which it was intended.

3.1. Proof of integrity

The designer must describe the mechanisms that ensure data integrity. The designer must prove beyond all reasonable doubt that the data cannot be altered fraudulently or inadvertently throughout the life cycle of a document.

3.2. Handwritten Signature

The designer must prove that all documents that have been hand signed cannot be altered from the time they are filed in the EDM system.

Example: The documents signed must be in PDF format. Thus, these documents cannot be altered accidentally. In addition, it is impossible for a broker (or any other user) to change a document that is already in the system.

3.3. Recording of transactions

The designer must demonstrate the procedure for tracking transactions made in the system and:

- ☐ List all actions (at least cover the following actions: creation, modification, consultation, downloading, sharing and deletion) and the user groups that made them and triggered an entry in the transactions' log.
- ☐ Provide a copy of the transactions' log and the details of a log entry.

The transactions' log must:

- ☐ Indicate the name of the person carrying out the transaction, the time and date of the transaction, and the data that was affected
- ☐ Not be altered
- ☐ Be kept as long as the documents
- ☐ Be accessible by the agency

3.4. Confidentiality of information

The designer must describe the mechanisms that ensure data confidentiality so that this data can only be used for performing the contract and that it is not kept after the expiry of the contract. These mechanisms must prove that the documents will remain inaccessible and protected even in the event of a security breach.

Example: Once created, the encryption of documents and data ensures that they can only be read by

users with the appropriate keys.

3.5. System protection

The designer must describe the security features implemented to ensure the security of the EDM system.

Examples:

- ✓ Are the servers periodically tested for vulnerabilities?
- ✓ Are there any procedures for handling security incidents? These procedures enable security incidents to be detected, analyzed and handled. These may include procedures for alerting, analyzing and notifying the authorities and individuals concerned.
- ✓ Is there any regular patching cycle to keep the tool up to date and protect it against vulnerabilities?

These features must prove that the documents will remain inaccessible and protected even in the event of a security breach. The designer must also describe how he manages any breach or attempted breach of privacy obligations and how he notifies his contractor of such an event and cooperates with him to carry out any privacy verifications.

4. SECURITY OF ACCESS

EXPLANATORY NOTE:

- Confidentiality: Only the legitimate recipient (or owner) of a document may have an intelligible vision of it.
- Authentication: When sending a document or when connecting to a system, we surely know the identity of the sender or the identity of the user who logged in.
- Non-repudiation: The author of an action on a document cannot deny his work.

The criteria below aim at ensuring that these four concepts are respected.

4.1. Allocation of access

The designer must indicate the access management tools:

- ☐ The name of the user group or of the user who grants authorizations to other users
- ☐ The mechanisms that guarantee individual access privacy (password modification)

4.2. User groups

The designer must indicate:

- ☐ The user groups that have access to the system, including the system administrator (provider)
- ☐ The users who are part of these groups
- ☐ Access profiles, i.e. the permissions and accesses of these groups:
  - The functionalities to which each group has access (e.g. consultation, edition, deletion, transmission, etc.)
  - The data these groups may consult, modify, add, delete, and transmit.
    - The profile details established for OACIQ inspectors, i.e. access to all read-only data and, where appropriate, access to registers, trust accounting and general accounting, as set out in the *Regulation*

respecting records, books and registers, trust accounting and inspection of brokers and agencies in the case where the system offers these components electronically. The OACIQ should be able to print and download these documents.

4.3. Maintenance of privacy of access

The designer must indicate the mechanisms that ensure the maintenance of the users' privacy of access, particularly in the case where the application is accessible to clients and an online authentication is required.

N.B. We strongly encourage the use of two-factor authentication for an additional layer of security.

4.4. Termination of access rights

The designer must describe the process for interrupting user access to the system, whatever the reason is: agency change, end of the subscription to the service, etc. The process must allow timely recognition of access termination and immediate interruption of access.

4.5. System access management

4.5.1. System through Internet

The designer must demonstrate system authentication mechanisms that meet the minimal class 2 standard. This level requires allocating a user ID and password after presentation of supporting documents, either in person or otherwise.

4.5.2. Network system

The agency must demonstrate that the access control mechanisms to the physical location from which the solution is accessible have been implemented.

5. RAISING EMPLOYEE AWARENESS

The designer must describe his strategy for regularly training employees and raising their awareness of good security practices.

Examples:

- ✓ Organizing training sessions on the secure use of the EDM, the risks associated with cybercrime and the measures to be taken in the event of a security breach.
- ✓ Encouraging employees to report any suspicious activity or abnormal behaviour.

6. INFORMATION SHARING

6.1. Description of information-sharing tool

The designer shall present the information-sharing tool that is included in the solution:

- ✓ Type of information that can be shared
- ✓ Method of information-sharing
- ✓ Information-sharing automation level

The designer must provide a screen shot to illustrate the information-sharing functionality.

N. B. Due to the nature of documents, which may contain personal, confidential, commercial or financial information, the OACIQ promotes a secure communication method, including secure email, a secure FTP site or other.

Example:

- ✓ The tool enables brokers to send, by email only, a document or all the documents contained in a record.

6.2. Management of access to information-sharing tool

The designer must detail the process of security and restriction of access to the information-sharing system:

- ✓ The name of user groups that can use the information-sharing tool
- ✓ Type of information these users can share
- ✓ How the roles and responsibilities of the users of the information-sharing application are defined

Examples:

- ✓ Only users of "Brokers" group can use the information-sharing tool, and they can send only their own records or the documents contained in their records.
- ✓ Users of "Administrative assistant" group can only send the records (or documents of a record) belonging to "Brokers" users' group with which they are associated

6.3. History

The designer must describe the mechanisms for recording information-sharing transactions and:

- ✓ List all sending actions and the user groups that made them and triggered an entry in the information-sharing transactions log
- ✓ Provide a copy of information-sharing transactions log as well as details of an entry in the information-sharing transactions log.

The log must at least include the date, the time the sharing began and the recipient.

7. RECORDS TRANSFER

EXPLANATORY NOTE:
The record transfer function manages the exchange of real estate brokerage records during movements of real estate brokers (broker change of agency, termination of broker's employment, or an agency shutdown, etc.).

The designer must give details of a transfer of the records of an agency (or of a broker acting on his own account) that uses the system described below, **according to three scenarios:**

- To an agency that uses the same system
- To another EDM system
- To paper (no EDM system)

7.1. Definition of the records transfer tool

The designer must describe the record transfer process.

7.2. Access management to the record transfer tool:

The designer must define the access security mechanisms to the record transfer tool.

This criterion is related to *3. Access security* section, particularly to *3.1. User groups* and *3.2. Allocation of access* criteria.

Example:

✓ Only users of the "Agency administrator" group can access the transfer functionalities of the solution

7.3. Transfer mechanisms:

The designer must indicate the transfer mechanisms depending on the case where the recipient uses the same system, uses another EDM system or does not use any system.

7.4. Information security

The designer must indicate the methods of respect of information privacy and integrity when transferring records.

Example:

✓ Transfer of records from system X to another system Y is carried out by a secured (SFTP) transfer FTP, which crypts the data sent and, therefore, guarantees the privacy of information transmitted.

✓ Data is transferred via a secure SSL channel. Once connected, exchanges between the user's computer and the servers are encrypted within an SSL tunnel provided by the HTTPS protocol.

7.5. History

The designer must describe logging mechanisms of record transfers and:

✓ List all transfer actions and user groups that made them and triggered an entry in the information-sharing log

✓ Provide a copy of the transfer transactions log or the acknowledgment of receipt of the transfer transaction

Example:

- ✓ This history can be generated automatically by the system if the latter allows the automatic transfer of broker or agency records. The history must include the date and time of the transfer, the requester, the files impacted, the recipient, and the acknowledgment of receipt.
- ✓ It can also be done in writing, in the form of acknowledgment of receipt signed by the EDM system designer and the broker or agency. This acknowledgment of receipt must include the date and time of the transfer, the requester, the files impacted, and the recipient.

7.6. Sending a notification to the OACIQ

The designer or the agency must inform the OACIQ when an agency using the EDM system ceases its activities, by indicating the date the records were sent, the name of the applicant, the affected files and the name of the recipient.

7.7. Data preservation

Data must have a secured residence location at all times. In the case where the agency ceases its activity and that no recipient agency is assigned, the agency or the broker working on his account must inform the OACIQ of the storage location of documents for the next six years.

8. SEARCH FOR RECORDS AND DOCUMENTS

EXPLANATORY NOTE:
Search criteria of an application are the representation of the system designer of the needs of users. In this case, the OACIQ constitutes a group of users. Therefore, the designer must take into consideration the research needs of the OACIQ inspection and syndic groups. These consultation methods must be protected and reserved for the OACIQ inspection and investigation purposes in order to preserve the information privacy.

8.1. OACIQ search methods

The designer must describe the search mechanisms of records and documents reserved for the Organization. If possible, he must provide a screen shot to illustrate the search functionality reserved for the OACIQ.

8.2. OACIQ search tools security

The designer must demonstrate that the search tools reserved for the OACIQ are secure and that only the OACIQ recognized authorities have access to this functionality.

This criterion is related to *3. Access security* section, particularly to *3.1. Allocation of access* criteria and *3.2. User groups*.

8.3. Search method:

The designer must demonstrate that the search mechanisms reserved for users allow retrieving only the documents to which the user is authorized.

This criterion is related to *3. Access security* section, particularly to *3.1. Allocation of access* criteria and *3.2.* User groups.

RECOMMENDATIONS MADE TO USERS AND USE PROCEDURES

A system designed in full conformity with the rules of confidentiality, integrity and preservation of information may be used inappropriately. This would cause a contravention of the ethical and professional requirements, established by the *Real Estate Brokerage Act* (R.S.Q., c. C-73.2) and its different application regulations. Therefore, it is important that the designers of an EDM system provide with their solution a user guide and recommendations so that all users should be informed of the measures to take to ensure that these requirements are met and that the integrity, confidentiality and the preservation of information are not compromised.

To complete his accreditation, the designer must provide to the OACIQ the relevant documentation that was given to their system users. These documents must provide all necessary information to all user groups (agency managers, brokers, office staff, etc.) so that the system is used in a way that does not contravene the ethical and professional requirements, established by the *Real Estate Brokerage Act* (R.S.Q., c. C-73.2) and its different regulations.

The recommendations should focus, among others, on the following points: system access allocation, access withdrawal, management of access given to external third parties (clients, etc.), system access management in case of a network system or a system functioning through Internet, procedure to follow for digitizing documents, preservation of the integrity of documents, etc.