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;
- ✓ 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 (use of full backup, incremental backup; differential backup);
- ✓ the frequency, 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. Note that the OACIQ allows storage locations in Canada and United States, since privacy standards are recognized and secure there. However, Canada is preferred, since the OACIQ reassesses, at any time and on a regular basis, the relevance to allow or withdraw the authorization for storage locations outside Canada.

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. DATA INTEGRITY

EXPANATORY NOTE:
The integrity of a document results from two elements:

- --- When there is a possibility to verify that data is not altered and is fully maintained.
- --- When the medium carrying this data provides it with the stability and durability required.

The criteria below aim at ensuring that these two elements are respected.

2.1. 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.

2.2. Recording of transactions

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

- ✓ List all actions and the users' group 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. 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.

--- Integrity: We have the guarantee that a document has not been altered, either accidently of intentionally.

--- Non---repudiation: the author of a document cannot deny his work.

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

3.1. 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).

3.2. 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;
- ✓ their rights and their privileges.
  - 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 the 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.

3.3. 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.

3.4. Cancellation 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 cancellation and immediate interruption of access.

3.5. System access management

3.5.1. 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.

3.5.2 Network system

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

4. SYSTEM CONTENT TYPES

4.1. 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.

5. INFORMATION SHARING

5.1. Description of information-sharing tool

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

- ✓ type of information than can be shared;
- ✓ method of information-sharing;
- ✓ information-sharing automation level.

The designer must provide s 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.

5.2. 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.

5.3. Background

The designer shall 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 include, at minimum, the date, the time the sharing began and the recipient.

6. DOCUMENT AUTHENTICATION

6.1. Document digitization

6.1.1. 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 requirement 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)**.

6.1.2. 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.

6.2. Authentication of documents

The designer shall indicate the procedure put in place to ensure that:

- ✓ the information will be accessible only to authorized persons,
- ✓ the metadata includes the author of the document;
- ✓ the document has not been altered either accidentally or intentionally;
- ✓ each operation made in the document is automatically saved in a way that no individual can deny having made a change.

6.3. 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 accidently. In addition, it is impossible for a broker (or any other user) to change a document that is already in the system.

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 when transferring records.

Example:

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

7.5. History

The designer shall 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 shall 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 it 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 or she 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. User groups* and *3.2. Allocation of access* criteria.

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. User groups* and *3.2. Allocation of access* criteria.

RECOMMENDATIONS MADE TO USERS AND USE PROCEDURES

A system designed in full conformity with the confidentiality, integrity and information preservation rules 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 b e informed of the measures to take to ensure that these requirements are met and that the integrity, confidentiality and the information preservation are not compromised.

To complete his accreditation, the designer must provide to the OACIQ the relevant documentation that 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 application 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.