Know your law
Guide respecting the management of technology-based documents

An Act to establish a legal framework for information technology (R.S.Q., C-1.1)
ACKNOWLEDGEMENTS

This Guide respecting the management of technology-based documents is about new law on a topic, information technology, which is still obscure for many users. The support given by several participants has therefore greatly contributed to making these pages more accurate and accessible. I would also like to sincerely thank Claire Morency (Director General, Bar of Quebec Foundation) and Guy Lefebvre (Vice-Dean, Development and Planning, University of Montreal Faculty of Law) for their helpful advice at all stages of the drafting of this guide. I also give my heartfelt thanks to various people who have carefully commented on this guide: Claudette Archambault (Sogique); Ugo Bellavance (e-commerce Master’s student); Diane Campeau (Sogique); Mario Dallaire (Abitibi Consolidated); Daniel Lafortune (Lafortune Leduc, Attorneys); Christian Lavoie (Bar of Quebec); Ghislain Massé (University of Montreal Faculty of Law); and Daniel Poulin (University of Montreal Faculty of Law). Lastly, I would like to thank Christian Saint-Georges (in charge of editing at Éditions Thémis) for editorial corrections made to the final version.

Thank you all,

Vincent Gautrais
Attorney and Professor
Faculty of Law
University of Montreal
<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>Legal change, new legislation... a guide</td>
</tr>
<tr>
<td>1.1</td>
<td>Information technology</td>
</tr>
<tr>
<td>1.2</td>
<td>The Act to establish a legal framework for information technology</td>
</tr>
<tr>
<td>1.3</td>
<td>Use of this guide</td>
</tr>
<tr>
<td>2.0</td>
<td>Guiding principles of the Act</td>
</tr>
<tr>
<td>2.1</td>
<td>Functional equivalence</td>
</tr>
<tr>
<td>2.2</td>
<td>Technological neutrality</td>
</tr>
<tr>
<td>2.3</td>
<td>Integrity</td>
</tr>
<tr>
<td>3.0</td>
<td>Managing technology-based documents in a secure manner</td>
</tr>
<tr>
<td>3.1</td>
<td>How to transfer a technology-based document to another medium</td>
</tr>
<tr>
<td>3.2</td>
<td>How to retain a technology-based document</td>
</tr>
<tr>
<td>3.3</td>
<td>How to ensure that a technology-based document is accessible at all times</td>
</tr>
<tr>
<td>3.4</td>
<td>How to ensure the transmission of a technology-based document in accordance with the Act</td>
</tr>
<tr>
<td>4.0</td>
<td>Use of technology-based documents as evidence</td>
</tr>
<tr>
<td>4.1</td>
<td>Can a technology-based document be used in court?</td>
</tr>
<tr>
<td>4.2</td>
<td>Is a technology-based document the equivalent of a “written document”?</td>
</tr>
<tr>
<td>4.3</td>
<td>Is an electronic “signature” legal?</td>
</tr>
<tr>
<td>4.4</td>
<td>Can a technology-based document be an “original”?</td>
</tr>
<tr>
<td>4.5</td>
<td>Is an electronic “contract” legal?</td>
</tr>
<tr>
<td>5.0</td>
<td>Liability associated with technology-based documents</td>
</tr>
<tr>
<td>5.1</td>
<td>In general, who is liable for technology-based documents?</td>
</tr>
<tr>
<td>5.2</td>
<td>Who is liable for confidential technology-based documents?</td>
</tr>
<tr>
<td>5.3</td>
<td>What liability does an information technology services company have?</td>
</tr>
<tr>
<td>6.0</td>
<td>Framework of a security agreement</td>
</tr>
<tr>
<td>7.0</td>
<td>Security agreement</td>
</tr>
<tr>
<td>8.0</td>
<td>Lexicon</td>
</tr>
<tr>
<td>9.0</td>
<td>References</td>
</tr>
</tbody>
</table>
The Act to establish a legal framework for information technology (R.S.Q., C-1.1) is new legislation in Quebec which governs documents used in what is commonly called e-commerce. This major text was implemented to take into account developments caused by the move from paper to information technology and describes how to use technology-based documents in a legal and secure manner.

The Act applies to all current and future information technology, such as the Internet, EDI, intranet, etc.

In this Guide, the Act to establish a legal framework for information technology will be referred to as the Act.
1.1 INFORMATION TECHNOLOGY

Although paper has for a long time been the traditional tool for communication and more particularly for doing business and, after centuries of a well-established tradition, users know how to manage such documents, this is not the case for new media. All information technology leads to profound change, and it is important that it provide the same or better ease of use with comparable security.

We are certainly not claiming that information technology does not have the benefits of paper! We will see that several technological, organizational or legal solutions provide equivalent and often superior quality to a paper document. We should point out, however, that e-mail, for example, which does not have special protection, has the following disadvantages:

- there is no assurance that the holder of the e-mail address is the person who has sent it (sender’s identity);
- there is no assurance of the identity of the recipient (identity of the addressee);
- it is easy to change the content of an e-mail (document integrity);
- it is not always possible to ensure that the document is not seen by unauthorized persons (document confidentiality);
- it is easy for a sender to claim later that he never sent such a document (author irrevocability).

Normal e-mail has serious security disadvantages compared to paper documents. It may therefore be important, in some circumstances, to correct this situation through technological and organizational changes to make it more secure.

1.2 THE ACT TO ESTABLISH A LEGAL FRAMEWORK FOR INFORMATION TECHNOLOGY

The Act was passed to manage this new reality. In 2001 the Government of Quebec, like the rest of Canada and most countries in the world, passed a specific law governing technology-based documents. This law has three main goals:

Eliminate legal barriers which existed in certain legislative and regulatory texts

Certain laws explicitly refer to a written document, a signature, an original, a paper document or more indirectly to circumstances assuming the use of paper. An insurance policy which is set out in writing is a good example. It was therefore essential to ensure that the use of information technology was not unlawful as a result of such a provision.

Set out certain general principles to manage technology-based documents in a secure manner

Although all laws must be general and impersonal, they nonetheless govern very different situations. Accordingly, the security of a large company with sensitive information is not necessarily comparable to that of a small business. As a result, it is important to find criteria and conditions which can help everyone ensure that their technology-based documents are secure.
Ensure that information technology is used in accordance with fundamental principles related to human rights

Document management, regardless of the medium, requires careful handling given the confidential nature of certain information. For example, a person who has documents containing personal information about an individual cannot treat it lightly. For the same reasons, the use of certain technology such as biometrics is strictly controlled in the Act.

1.3 USE OF THIS GUIDE

Who is it for?

To the extent that everyone may use technology-based documents in business or socially, we are all affected by the Act, whether individually, in corporations or in public institutions.

However, the Act sets out duties and requirements which may vary depending on the category to which it refers. Thus, an individual, whether a consumer or simply a citizen, does not have the same responsibilities as a private or public institution.

Given the importance of determining the impact of information technology in day-to-day business, this guide is therefore intended for the following people in particular:

- people designated within a business to manage technology-based documents;
- technicians in charge of a web site;
- managers of small businesses;
- lawyers;
- notaries; or
- individuals interested in the prudent management of the technology-based documents they use.

To facilitate comprehension of this guide, it is strongly recommended that you read the Act.

What is it for?

The Act identifies certain criteria to ensure the adequate management of technology-based documents. This guide is intended to offer concrete solutions to meet those criteria. However, it should be noted that technological solutions are only proposed as examples. As a result, they are neither unique nor necessarily adapted to all situations as, although the Act sets out the legal criteria, it does not say specifically how they may be met.

The following analysis is therefore intended to respond to the Act by identifying the importance of better awareness of the advantages of proper document management and by informing readers about the legal conditions which must be met.
The Act is often seen by analysts as a technical text with new concepts not found in other laws. Although there is a lexicon with definitions at the end of this guide, we should clarify the following three guiding principles at this point.
2.1 FUNCTIONAL EQUIVALENCE

**Definition**
An approach according to which requirements which are found in certain laws, such as a written document, a signature or the original, may also be applied to a technology-based medium provided they fulfil the same functions as paper.

**Examples**
- Written document: a written document is legal when it is complete, regardless of the medium (see section 4.2).
- Signature: a signature may also be used on paper or with information technology provided it 1) allows a person to be identified; and 2) demonstrates consent (see section 4.3).
- Original: an original fills three basic functions, depending on the case: to be the first source of a document, to be a single document and to be the first source of a document relating to a person (see section 4.4).

2.2 TECHNOLOGICAL NEUTRALITY

**Definition**
Characteristic feature of a law which does not favour one means of communication (paper or information technology) over another. In such a case, a court cannot refuse to recognize a document merely because it is in a technology-based medium.

**Examples**
- A sale of goods between two companies may be entered into through one or more technology-based documents. In case of dispute, either party could validly submit such documents provided they meet the necessary conditions. The fact that it is on paper or in electronic form is not a determining factor.
- On the other hand, the Act provides that certain contracts, such as the sale of an automobile to a consumer or a consumer loan contract, must be on paper. For such contracts in particular, the Act is not technology-neutral.
Unless indicated otherwise in the Act, and provided the necessary conditions are met, a document may be either in a technology-based form or on paper.

### 2.3 INTEGRITY

#### Definition
A fundamental requirement of the Act which ensures that a document, regardless of the medium used, has full and complete legal value provided its integrity can be established. For integrity to be ensured, a document must not be altered or modified.

#### Examples
Although this feature is difficult to prove for unprotected e-mail, there are solutions to ensure the integrity of technology-based documents:

- an encrypted tool such as MD5 allows a document to be digitally encoded. The person in charge may therefore keep it, ensuring the integrity of the document, as any modification would show the discrepancy between the document and its encoded version;

- a public key infrastructure ensures the integrity of a document during its transmission and storage;

- the PGP tool (or other security tool) may be recommended for smaller organizations;

- a system of “notarization” where, for example, an archiving service keeps documents to ensure their integrity (see section 5.3);

- it is also possible in certain circumstances to use a medium which is not technology-based, such as paper, which has better overall integrity than unprotected technology-based documents;

- the use of certain CD-ROMs may also be a possible solution.
Managing technology-based documents in a secure manner

Security is often considered the main impediment to the use of information technology and there is a broad diversity of methods in business. For example, the banking industry has for several decades used a series of very elaborate security procedures. However, this care is not necessary in other less risky areas. Moreover, security must be ensured throughout the life cycle of a technology-based document, and in particular during the four special operations governed by the Act, namely: transfer (3.1); retention (3.2); consultation (3.3); and transmission (3.4).

Security is not the same in all circumstances. It depends on the amount of risk. Assessment of this consideration is the first step in choosing what steps to take.
Four operations specially governed by the Act

01 Transfert

To change a technology-based document from one medium to another. The document in the new medium has the same legal value as the former one and the document in the former medium may then be destroyed.

02 Retention

To store documents so that they can be found later, on request, without having been altered. For tax, administrative or legal reasons, most businesses are required to keep certain documents.
03 Consultation

To make a document presented in an intelligible form available to authorized persons.

04 Transmission

To send a document from one person to another using information technology, unless prohibited by law or regulation.
### 3.1 HOW TO TRANSFER A TECHNOLOGY-BASED DOCUMENT TO ANOTHER MEDIUM

<table>
<thead>
<tr>
<th>Definition</th>
<th>To change a technology-based document from one medium to another. The document in the new medium has the same legal value as the former, and the document in the former medium may then be destroyed.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example</td>
<td>Businesses digitize many paper documents, because of archival costs or to facilitate searches, and then transfer them to a CD-ROM.</td>
</tr>
</tbody>
</table>
| Legal conditions | - Document in advance how the transfer will be done. A business must plan its procedure by drafting a security agreement (also called a security policy, procedure, measure or code) explaining how it will be done. It should indicate, among other things:  
  - the original format;  
  - the guaranties offered by the chosen solution;  
  - the electronic process used.  
  - Preserve the integrity of the transferred documents.  
  N.B. An individual is not covered by these requirements. |
| Solutions | - Designate an assigned person within the organization or sub-contract to a third party service.  
- Carry out these steps in a systematic fashion for all documents.  
- Attach the documentation when the time comes to prove the transferred document. |
3.2 HOW TO RETAIN A TECHNOLOGY-BASED DOCUMENT

**Definition**
To store documents in such a manner that they can be found later, on request, without having been altered. For tax, administrative or legal reasons, most businesses are required to keep certain documents.

**Examples**
- An individual who purchases a product on-line should keep track of an acknowledgement of receipt sent to him by the merchant after payment has been sent but before he receives the product.
- For accounting purposes, a business may be required to keep certain documents for 10 years.

**Legal conditions**
- Designate an assigned person, within the organization, for security matters or sub-contract to a third party service.
- Ensure that the documents kept are:
  - complete; and
  - available throughout the time they are retained (which includes the software needed to read the document).
- Ensure that the assigned person who modifies a retained document, and thus knowingly compromises its integrity, explains in the document itself or in a related document:
  - who asked for the modification;
  - who modified the document;
  - when the modification was done;
  - why it was done.

**Solutions**
- Set up an organizational structure under which an assigned person decides in advance what procedure will be used. This may include, among other things, the preparation of a security agreement.
- Choose among the solutions identified above to meet the integrity requirement.
- Use a third party for archiving.
### 3.3 HOW TO ENSURE THAT A TECHNOLOGY-BASED DOCUMENT IS ACCESSIBLE AT ALL TIMES

<table>
<thead>
<tr>
<th>Definition</th>
<th>To make a document presented in an intelligible form available to authorized persons.</th>
</tr>
</thead>
</table>
| Examples | - The Act respecting access to documents held by public bodies and the protection of personal information requires public institutions to make the personal information they have on people accessible to them.  
- The Act respecting the protection of personal information in the private sector requires businesses to make documents containing personal information about users accessible to them.  
- The Securities Act sometimes requires companies to send investors certain documents respecting their business, such as financial statements or press releases. |
| Legal conditions | - Ensure that the documents are intelligible and legible.  
- Give a person who has a right of access the freedom to choose between a paper document and a technology-based document.  
- Organize special access when documents which must be made accessible contain personal or confidential information, by nature more sensitive, such as:  
  - limiting access to authorized documents and prohibiting access to others;  
  - identifying an assigned person;  
  - ensuring that it is impossible to do an extensive search, eg. it should not be possible to check the names of the parties in a database of legal decisions;  
  - setting up an adequate security system; and  
  - ensuring that the conditions which apply for documents containing personal information are met (see section 5.2). |
| Solutions | - Prevent an individual who is authorized to consult only certain information from consulting other information.  
- Set up a firewall, detection system, authentication system, log, etc. which controls unauthorized access.  
- Prepare a security agreement (see Chapter 6) which sets out all these solutions. |
3.4 HOW TO ENSURE THE TRANSMISSION OF A TECHNOLOGY-BASED DOCUMENT IN ACCORDANCE WITH THE ACT

Definition
To send a document from one person to another using information technology, unless prohibited by law or regulation.

Examples
- E-mail is the usual way to send an attachment.
- Businesses very often send technology-based documents: exchanges of computerized documents, electronic fund transfers, etc.

Legal conditions
- For a sent document to have the same validity as a received document:
  - ensure the integrity of both documents; and
  - document how this is ensured.
- Assume that a technology-based document is sent when the sender no longer has control of it. For greater certainty, a transmission slip may be generated by the sender’s system.
- Assume that a technology-based document is received when it is available to the recipient. For greater certainty, an acknowledgement of receipt may be generated by the recipient’s system.
- Ensure that a document which contains confidential information:
  - is sent by a method considered appropriate; and
  - that the transmission is recorded.

Solutions
- Use a public key infrastructure to ensure, among other things:
  - the integrity of a document;
  - the authenticity of the sender and recipient;
  - the confidentiality of the information;
  - the irrevocability of the sender, who cannot say that he was not the one who sent the document.

These criteria will be more or less ensured depending on the quality of the PKI.
- Use PGP.
Security and evidence are two sides of the same coin. The more a technology-based document is generated in a secure manner, the greater its admissibility as evidence. In litigation, it is very likely that a judge or arbitrator who must weigh the evidence presented by the parties will give more weight to that which was made with the greatest care. Accordingly, it is important to look in this chapter at how the new provisions of the Act affect the usual rules on evidence.

It should also be remembered that laws often prescribe special conditions for a document to be admissible in court. Thus,

1. certain contracts may only be made in writing (such as copyright licences, contracts over a certain amount, arbitration clauses, etc.);
2. certain documents must be signed; and
3. certain operations require an original.

It is therefore important to know how these conditions may be met in a technology-based environment.
### CAN A TECHNOLOGY-BASED DOCUMENT BE USED IN COURT?

<table>
<thead>
<tr>
<th>Principle</th>
<th>A technology-based document may not be refused by a judge merely because it is technology-based. It may thus be an element of proof admissible in the same way as a paper document.</th>
</tr>
</thead>
</table>
| Examples | - A business may enter into contracts by e-mail. Nevertheless, businesses would sometimes be well advised to use appropriate technological processes to make the document more secure.  
- A recording on a “webcam” or a digital photograph may also be admissible as evidence. |
| Legal conditions | - Ensure the document’s integrity. Integrity depends on circumstances and the sensitivity of information contained in the document. Regarding the issue of integrity, the Act states that:  
  - it is not necessary to prove that the document environment is appropriate; proof of the document’s integrity is sufficient;  
  - the integrity of a document coming from a business or the State is presumed. Therefore, for example, a consumer may produce in evidence a printed copy or a disk of an e-mail from a business and its integrity will be presumed. It is up to the business to prove the contrary.  
- Confirm, when the document is not signed, the identity of the author of the document. |
| Solutions | - Adobe software, for example, generates standard “pdf” documents which may, when the stakes and risks are not high, be a sufficient tool. However, such a document can be changed.  
- Several software products using various technologies provide solutions to ensure document integrity.  
- See also the solutions proposed in the analysis of the integrity criteria in section 2.3. |

**The value of a technology-based document is up to the judge. The more the person presenting such a document acted diligently to manage it, the more likely the judge is to consider it as admissible and of evidentiary value.**
4.2 IS A TECHNOLOGY-BASED DOCUMENT THE EQUIVALENT OF A "WRITTEN DOCUMENT"?

<table>
<thead>
<tr>
<th>Principle</th>
<th>Based on the principle of functional equivalence (see section 2.1), the Act allows electronic documents, which may be in any medium, whether paper or technology-based.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Examples</td>
<td>Many documents must be drafted in writing. This is the case in particular for:</td>
</tr>
<tr>
<td></td>
<td>- wills;</td>
</tr>
<tr>
<td></td>
<td>- insurance policies.</td>
</tr>
<tr>
<td></td>
<td>Be aware, however, that some consumer contracts which also require a written document, such as an automobile purchase contract or a consumer loan contract, may not be drafted using a technology-based medium, as the Act expressly provides that they may only be on paper.</td>
</tr>
<tr>
<td>Legal conditions</td>
<td>Ensure the integrity of the document.</td>
</tr>
<tr>
<td></td>
<td>More generally, determine who the document comes from and where it originated.</td>
</tr>
<tr>
<td>Solutions</td>
<td>See the solutions to ensure the integrity of a document in section 4.1.</td>
</tr>
</tbody>
</table>

A written document is no longer necessarily synonymous with “paper”. An electronic written document is thus possible provided it fulfils the same functions as paper.
### 4.3 IS AN ELECTRONIC “SIGNATURE” LEGAL?

| Definition | A tool representing a personal mark which is commonly used by a person to show consent. The definition of signature is not related to any particular medium (paper or electronic). |
| Example | - Several documents are only valid when signed, including:  
  - wills;  
  - mandates;  
  - certain contracts. |
| Legal conditions | - Allow the person to be identified.  
- Allow the person to show his approval, undertaking, consent.  
- Use a degree of reliability for the signature which corresponds to what is at stake, the circumstances, the habits or the trust between the parties. |
| Legal conditions specific to biometrics | The Act sets out very strict rules respecting the identification of a person through certain physical characteristics such as digital fingerprinting, retinal scan, DNA or voice recognition.  
- Carefully manage biometric data during its use and, more specifically:  
  - protect biometric data from interception and more generally from identity theft;  
  - preserve the integrity of biometric data;  
  - log the use of biometric data;  
  - destroy biometric data when its use is complete.  
- Before using biometric data, ask for the clear consent of the person in question. Unless indicated otherwise in the law, no one is required to use such a tool.  
- Tell the Commission d’accès à l’information that biometric data is being used. The Commission has a right to monitor it. |
| Solutions | - A signature may thus be valid by simply putting a name at the end of an e-mail. However, this process is not very reliable, as it is easy to sign for another person by sending an e-mail as if it had come from somebody else.  
- Biometrics and electronic certificates are often considered to be electronic tools which allow a person to be identified with some certainty.  
- More commonly, a “click” (clicking on an “I accept” icon) may easily be considered to be a valid signature. The identification condition is complied with more if the signatory inserts an identifier such as a password, a personal identification number (PIN), or even a credit card number.  
- A public key infrastructure is a process which may clearly be used as a signature when manifestation of consent is clear. |
A person may obviously sign with a pen but also with a “click”, a personal identification number or his name at the bottom of an e-mail. However, in all cases, the identity of the signatory and the fact that the action represents his consent must be ensured.
4.4 CAN A TECHNOLOGY-BASED DOCUMENT BE AN "ORIGINAL"?

**Definition**
A physical document corresponding to its first writing which is often used to prove an act or a fact. Usually associated with paper, the Act sets out legal conditions so that, when certain laws require an original, it may be met by a technology-based document.

An original should fulfil three functions.

**Legal conditions**

1. For a document to fulfil the first function of the original, namely the primary source of a copy, such as a contract signed in two counterparts:
   - the integrity of the document must be ensured;
   - the document must be retained;
   - it must be available for consultation later.

2. For a document to fulfil the second function of an original, namely being the sole document (such as a cheque, a bill of lading or security in bearer form):
   - the integrity of the document must be ensured;
   - a technological solution must be integrated*;
   - an exclusive element must be integrated or a procedure to prevent any form of reproduction must be set up.

3. For a document to fulfil the third function of an original, namely being the primary source of a document relating to a person (for example a will or digital certificate):
   - the integrity of the document must be ensured;
   - its uniqueness must be stated;
   - the person to whom the document relates must be identified*;
   - this relationship must be maintained throughout the life cycle of the document.

* In situations two and three, the legislator refers to technological solutions that should be determined by an accepted technical standard. Such technical standards could, for example, be issued by international organisations like ISO (International Organization for Standardization) or IETF (Internet Engineering Task Force). Some national organizations, such as SCC (Standards Council of Canada) or BNQ (Bureau de normalisation du Québec), would equally be able to act in kind.

Although it is a concept traditionally associated with paper documents, a technology-based original is possible. On the other hand, it must be ensured that the functions normally reserved for it have been met in that environment.
4.5 IS AN ELECTRONIC “CONTRACT” LEGAL?

Principle
A contract is a meeting of the minds which can be made in any medium provided the parties indicate their consent. It is therefore legally possible to enter into a contract using any medium to communicate the two basic elements of a transaction, namely offer and acceptance.

A signature may be used to show consent but a contract may be entered into in another way when the intention is clear.

Example
A contract may therefore be entered into by the exchange of e-mail or faxes, by telephone or by filling out a form on the Internet.

Legal conditions
- Draft a clear and unmistakable offer.
- Provide for acceptance on-line where the person clearly agrees in a free and informed manner. For example:
  - by clicking on an “I accept” icon;
  - through the mention on a web site that merely logging onto a web site is acceptance of the conditions which follow. This method is questionable.

Legal conditions specific to an electronic contract
It is possible for contracting parties to mutually agree through electronic means or other technological processes. Such tools may have various degrees of sophistication:

- through advance software which has been programmed to allow certain acts (such as EDI);
- by forms found on a web site which allow acceptance by clicking on an “I accept” button.

The Act requires that a person who uses such a process, under penalty of nullity:
- allow the opposite party to correct errors which may have occurred;
- give clear instructions on how to proceed.

For example, an acknowledgement of receipt may meet these conditions.

A contract may be verbal, on paper or electronic, provided the offer is accepted.
We have seen that in several respects there is a requirement to manage some documents by meeting a certain degree of security. The failure to do so must be penalized and a number of examples may be given, such as:

- a “cyber merchant” who lets an unauthorized third party have access to personal information of his customers; or

- a person who forgets to verify the validity of the digital certificate of the other party with whom he plans to do business.
5.1 IN GENERAL, WHO IS LIABLE FOR TECHNOLOGY-BASED DOCUMENTS?

**Principle**  
Generally, any person, whether a business, a public institution or an individual, may be held liable for damage caused to another merely because he has technology-based documents.

**Example**  
A person who sends a technology-based document containing a virus may be held liable for the damage caused if:
- a fault is committed;
- damage is caused;
- a connection can be established between the fault and the damage.

**Legal conditions**  
There is no general obligation of security. On the other hand, a person who does not take special care in managing his technology-based documents will be unable to assert his rights due to a lack of evidence. The Act sets out strict conditions in certain cases, such as when managing confidential technology-based documents (see section 5.2) and when managing a digital certificate (see section 5.3).

5.2 WHO IS LIABLE FOR CONFIDENTIAL TECHNOLOGY-BASED DOCUMENTS?

**Principle**  
A confidential document may only be accessible to authorized persons. Those who possess such documents have an obligation to ensure an adequate degree of security.

**Examples**  
- A business which has personal information on its customers, such as their credit card number, must comply with security requirements.
- Members of most professional bodies, such as lawyers, doctors or architects, must keep certain information confidential.

**Legal conditions respecting the protection of personal information**  
- Develop a privacy policy explaining the treatment and purpose of personal information.
- Have a serious and legitimate interest in setting up a file.
- Only collect information necessary for the purpose in question.
- Allow individuals, with exceptions, to access (see section 3.3), correct or remove their own personal information.
- Prohibit the transmission of personal information to a third party without clear consent by the affected person.
Legal conditions respecting security

- Set up security measures which are in proportion and appropriate to the circumstances.
- Prevent the duty of access to technology-based documents from impairing the confidentiality of certain information. With respect to public data in particular, it is possible to set up a reduced visibility system which would prevent overly broad searching by key words (see section 3.3).
- Ensure, when transmitting confidential information, that:
  - the parties who receive it also have adequate security; and
  - the operation is documented.

Solutions

- Set up a security agreement to explain the security measures to take such as:
  - the setting up of physical measures, such as locks;
  - implementation of organizational measures, control of access or identification of assigned persons;
  - implementation of technological methods such as number codes or passwords;
  - make staff aware of the importance of keeping such documents confidential.

Personal information is any information allowing an individual to be identified, such as his name, his address, a medical report, banking history or a credit card number.

Unless the affected person consents, a business cannot use the information for a purpose other than that for which it was collected. An individual has the right to know what information a business or public institution has about him.
5.3 WHAT LIABILITY DOES AN INFORMATION TECHNOLOGY SERVICES COMPANY HAVE?

Notwithstanding the fact that the Act sets up a general system exempting intermediaries, with exceptions, whose role is limited to offering technical support, certain services using information technology are subject to special rules.

More particularly, we will examine:
Hosting services
Hosting consists of making disk space available to others in order to post information on a web site. Illegal documents are sometimes available on the Internet, whether they be hate literature or statements which are defamatory, against public order or an invasion of privacy. The question is who is liable—the author or the host.

- General exemption. The role of the host is limited to posting pages on the Internet without any control over them, even though it could control them.

- Possible liability where:
  - the host is aware of the unlawful activities of persons hosted by it, particularly when it is made aware of them by letter or e-mail;
  - the host is aware of circumstances which make unlawful activities by persons hosted by it apparent;
  - the host does nothing to prevent unlawful activities from being carried on by persons hosted by it.

Referral services
Operations related to hypertext link pages, search engines, indices or other directories are called referral services. Their liability is similar to that of hosting services.

Transmission services
Transmission services refer to a purely technical function through which a service provider sends technology-based documents from one point to another.

- General exemption. Its role is limited to a technical action.

- Possible liability when:
  - it is the originator of the transmission;
  - it selects or modifies the transmitted document;
  - it selects the person who sends, receives or accesses the questionable document;
  - it keeps the document longer than required to send it.
Retention services involve the retention of documents to ensure better efficiency in the transmission of technology-based documents. They correspond to the following two main situations:

- “Caching”, which consists of storing aspects of a web page on a computer or server to facilitate later access;
- the retention of documents necessary for use by a controlled access Intranet server (in particular for security reasons).

General exemption. Liability similar to the preceding one applies to retention service providers.

Possible liability:

- in one of the four situations which apply to liability of the sender [see Transmission services];
- the provider does not comply with the conditions for accessing a document;
- the provider prevents verification of who has accessed a document;
- the provider fails to withdraw promptly from the network or does not block access after becoming aware that:
  - the document has been removed from its original position;
  - persons entitled to access the document cannot do so;
  - an authority having jurisdiction has ordered that the document be removed.

Archiving services To retain certain important documents, it is possible to use a company which provides archiving services.

- Contrary to several other services, it is not subject to a general exemption
- An archiving service provider:
  - has a general security obligation;
  - must preserve the integrity of the documents entrusted to it;
  - must maintain the conditions related to retention (see section 3.2).
- Users of archiving services must make the service provider aware that the documents they entrust to it must:
  - not be accessed by unauthorized persons;
  - be kept confidential.
Certification services  The services of a certification authority involve certifying the identity or one or more aspects of a certified person and allowing a third party to ensure that the certified person is in fact who he claims to be.

— Certification authority obligations:
- draft a certification policy explaining the essential technical requirements (content of certificate, revision period, term, conditions of issue, conditions to ensure confidentiality, handling of complaints);
- announce the certification policy;
- give assurances of impartiality;
- enter any invalid certificate promptly on the list provided for such effects;
- ensure the integrity of the certificate.

— Obligations of a certified person:
- keep secret any device that allows the certificate to be used, as any use of it is presumed to be made by him;
- disclose to the certification authority anything which would suggest that the device has been compromised by a third party;
- inform the certification authority of any change in his status.

— Third party obligations:
- verify the identity of participants;
- verify the validity of the certificate on the list set up by the certification authority.

— Allocation of liability:
- liability not proven - All parties are liable.
- shared liability - Each party assumes his share, but if one party cannot do so, his share should not be assumed by the others.
- liability impossible to establish - Liability is shared equally.
- no one liable - Liability is assumed jointly and equally.

Whatever the allocation, it is of public order and cannot be modified by contract.
The drafting of a security agreement is often the position to take in prudent document management.
SECURITY AGREEMENT

A security agreement may be drafted for various situations or for the following operations:

- the transfer of a technology-based document (see section 3.1);
- the retention of a technology-based document (see section 3.2);
- when a technology-based document is confidential (see section 5.2);
- the transmission of a technology-based document (see section 3.4);
- to enhance the evidentiary value of a technology-based document;
- to set out the obligations of participants within a company (who does what!).

Whatever terms the parties use to describe the document (security agreement, security policy, security protocol, security procedure, security measures, security code, etc.), the goals of a security agreement are the following:

1. comply with applicable legal provisions;
2. allow proper comprehension by affected users;
3. offer a degree of security considered appropriate for the sensitivity of the technology-based documents;
4. allow flexibility so that it may be used in a broad number of cases.
A security agreement is a tool setting out the security requirements of the employees of a business and its partners.

From a legal point of view, a security agreement sometimes corresponds to a contract which the parties sign or an internal document of an institution setting out the obligations of each participant.

With respect to the structure of a security agreement, the circumstances will have a major impact on how such a document is drafted. Depending on the degree of trust between the parties, how sensitive the documents handled are, the risks inherent in the activities, the means available and the capacity of the parties, the document will be more or less elaborate and more or less precise.

Nonetheless, it is possible to suggest several types of clauses which may be found in a security agreement. Firstly, there are the “standard” clauses found in many contracts (purpose, definitions, protection of personal information, liability). There may also be clauses related to the agreement itself, document management and security of the environment.
## ESSENTIAL ELEMENTS OF A SECURITY AGREEMENT

| Identification of the parties | A clause identifying the persons with an interest in the agreement by their name, address and contact information. |
| Purpose of agreement | A clause intended to set out the extent and goal of the agreement. The objectives and obligations may be summarized here. |
| Definition | Help the parties interpret or define certain terms. |
| Conclusion of agreement | Organize the relationship between the parties. A distinction should be made between the security agreement itself and what it is asking to be done. It is therefore necessary to include the terms of formation of the agreement, such as: |
| - its scope; |
| - how it will be entered into (signature); |
| - its amendment or renewal; |
| - its term. |
| Management of documents during their life cycle | Identify the documents and operations to be covered. The agreement is made to cover a certain number of documents and operations (for example, a contract). For each, identify the security functions which apply throughout their life cycle. This last, basic concept involves organizing document management with respect to: |
| - their creation; |
| - their transfer; |
| - their consultation; |
| - their transmission; |
| - their retention; |
| - their eventual destruction; |
| - the essential documents of a contract. |
Security of the environment

Include terms respecting the organizational framework such as:

- determine an assigned person;
- inform, make accountable (by contract) and educate employees;
- report unauthorized intrusions into the environment;
- set up a contingency plan, i.e. a document which sets out the procedure to be followed if there are security problems;
- have an outside company conduct audits and perform tests;
- periodically review the terms respecting the organizational framework;
- assess risk.

Include terms respecting the technological framework such as:

- organize physical security (doors, locks);
- control access to documents;
- anti-virus protection;
- ensure security during transmission (encoding).

Protection of personal and confidential information

Verify compliance with this area of law when documents allow individuals to be identified or confidential information protected by law, a regulation or an agreement to be obtained.

Liability

Include liability, non-liability or superior force clauses.

Schedules

For more complex security agreements, create schedules setting out technical measures to be followed.
**LEXICON**

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Biometrics</td>
<td>The science of studying biological variations which allow a person to be identified based on certain physical characteristics. Examples: fingerprints, voice recognition, retinal scan, DNA, etc.</td>
</tr>
<tr>
<td>Digital certificate</td>
<td>Technology-based document issued by a certification authority containing a certain amount of relevant information forming a kind of electronic ID card.</td>
</tr>
<tr>
<td>Certification of a document</td>
<td>Identification procedure whereby a certification authority creates a link between a person and a document called a certificate. Based on the digital certificate issued by the certification authority, the certified person may be identified to third persons receiving the certificate. Third parties can therefore be assured that the certified person is in fact the person he claims to be. Note also that certain certificates are called certificates of attribution, in which case the certificate assures third parties that the holder has a certain quality. For example: certificates confirming that a person is a member of a professional body, has credit from a bank, is an employee of a company or a government, etc.</td>
</tr>
<tr>
<td>Encoding</td>
<td>Technique used to keep electronic documents confidential: an algorithm transforms the data to make it unintelligible to someone who does not have the key to decode it.</td>
</tr>
<tr>
<td>Life cycle of a document</td>
<td>Period from the time a document is created until it is destroyed. It includes, among other things, the various stages in the life of a document, which are its transfer, consultation, transmission or retention.</td>
</tr>
<tr>
<td>Technology-based document</td>
<td>An element made up of information (<a href="#">document</a>) which uses a medium based on one or more types of information technology. Such technology may be, but need not be, electronic. Magnetic, optic, etc. media should be included also. The application of the Act is therefore intentionally broad in order not to exclude new technology which may emerge later. The Act therefore uses the term &quot;technology-based document&quot; (information technology) and not only &quot;electronic document&quot; (which is a subset of the first) to avoid leaving out any particular type of technology. For example: e-mail; &quot;Word&quot; or &quot;PowerPoint&quot; file; magnetic tape; CD-ROM; MP3 file.</td>
</tr>
<tr>
<td>EDI</td>
<td>(Electronic document interchange) Computer application ensuring the transmission of electronic documents in a standardized and structured format which allows mechanization.</td>
</tr>
</tbody>
</table>
| Public key infrastructure (PKI) | A public key infrastructure is made up of three elements:  
  - a private key for each participant;  
  - a public key corresponding to the private key;  
  - a certificate issued by a certification authority which identifies a person.  
A public key infrastructure is the tool most often presented as the secure solution in open environments such as the Internet. It:  
  - allows the integrity of a document to be ensured during its delivery;  
  - allows the document to be sent in confidence with encoding which makes the document unreadable during transmission;  
  - ensures that the document originates from the designated person.  
For example: Alice sends Ben a document using a public key infrastructure.  
  - Alice encodes the document to be sent (using a coding tool which makes it unreadable) with Ben's public key which can be accessed anywhere;  
  - Ben decodes the document sent by Alice with his private key. Confidentiality is thereby ensured.  
It is also possible to ensure integrity and authenticity in the following manner:  
  - Alice makes a condensed version of the document to be sent using her private key and creates what is called a digital signature;  
  - Ben uses Alice's public key to open Alice's signature. If the signature becomes a readable document identical to the document sent, Alice must have sent it.  
To be sure that Alice and Ben are the people they claim to be, they may use a certificate issued by a certification authority which, after checking their identity, sends them a document identifying them and containing a public key. |
| Act                      | In this document, "Act" means the Act to establish a legal framework for information technology, R.S.Q., c. C-1.1. |
REFERENCES

General site respecting the Act to establish a legal framework for information technology (2001 - Quebec)
http://www.autoroute.gouv.qc.ca/loi_en_ligne/

PME Quebec Clic (e-business site) (Quebec)
http://www.pmequebeclic.com

Act respecting the protection of personal information in the private sector (1994 - Quebec)
http://www.canlii.org/qc/laws/sta/p-39.1/20040901/whole.html

Guide to Internet rights (Quebec)
http://www.droitsurinternet.ca/

Personal Information Protection and Electronic Documents Act. (2000 - Canada)
http://www.canlii.org/ca/sta/p-8.6/whole.html

Online E-Security and Privacy Guide (2003 –Canada)
http://www.guidevies privee.icce.ca/

Electronic Commerce Act (2000 - Ontario)
http://www.canlii.org/on/laws/sta/2000c.17/20041008/whole.html

Code of practice for information security management (ISO/CEI 17799 - international)

ISBN 2-9808666-0-1

Legal Deposit - Bibliothèque nationale du Québec, 2005
Legal Deposit - Bibliothèque nationale du Canada, 2005

© La Fondation du Barreau du Québec, November 2005.
All rights reserved.
The Quebec Bar Foundation is a non-profit organization whose mission is to serve the interests of Quebecers by informing them of their rights and duties. This guide has been created for anyone who is interested in the management of technology-based documents.

fondation@barreau.qc.ca

About the author:

Vincent Gautrais is a law professor with the University of Montreal and a member of the Bar of Quebec. His specialty is e-commerce and he is currently director of the Master’s program in e-commerce.

vincent.gautrais@umontreal.ca

Our Partners:

Ressources Entreprises

Services-conseils en affaires électroniques
www.affaireselectroniques.info

Info entrepreneurs

Canadas Business Network