Framework for the protection of information held by a Quebec First Nation community or organization

[COMMUNITY]

[ACT / REGULATION / POLICY]

on the protection of information held by

[COMMUNITY]

March 2014

This document constitutes the version 1.0 of the framework.

Document drafted jointly by:

Mr. Michel Deschênes, FNQLHSSC
Mr. Yvon Gauthier, Yvon Gauthier Info
Ms. Nancy Gros-Louis McHugh, FNQLHSSC
Ms. Elisabeth Patterson, Attorney, Dionne Schulze S.E.N.C.
Ms. Marjolaine Siouï, FNQLHSSC

Graphic design and page layout:
Code jaune
Patricia Mathias, CSSSPNQL

We thank the Akwesasne Mohawk Council for allowing the consultation of the document entitled: *Access to Information and Protection of Personal Privacy Regulation*.

This document is available in French.

A complete version of this document is available on the FNQLHSSC website at: http://centredoc.cssspnql.com/opac/notice_view.php?id=755.

Reproduction is authorized for non-commercial purposes on the condition that the source is mentioned.

ISBN: 978-1-926553-54-2

© 2014 FNQLHSSC. All rights reserved.

Note to readers

This document proposes a framework *adopted by the Assembly of the First Nations of Quebec and Labrador in its resolution no. 07/2012*[1]. It was drafted primarily for the communities, but it can also serve First Nations organizations, particularly regional organizations. However, they will need to make the necessary adjustments to the text so that the document reflects the particularities of their organizational structures and the nature of their powers.

As revealed in the preliminary report[2] that preceded the development of this framework, the protection of personal information and confidential information in First Nations communities is not supported by clear legal rules. We are freely proposing this framework to the communities and organizations in order to fill this void and address a need raised by several communities that wish to improve their administrative practices. This basic document groups together a set of definitions, principles and regulations that respect the laws and regulations in force, as well as the codes of practice used within public administrations of Canada and Quebec. Basically, it covers regulations associated with the protection of personal information, but also includes measures related to the protection of collective data and any other information considered confidential by a band council or the management of a service or organization.

The content of the framework is drafted in a formal manner so that a community may use it as is, simply by determining, at the time of its adoption, that it is in fact a band council administrative regulation (under the terms of the Indian Act), an internal regulation or a council policy. It will also be possible to decide to designate it as a law during its adoption, thereby further asserting the will for governmental autonomy. Regional First Nations organizations, on the other hand, will be able to make it a by-law or internal policy. This choice is important with respect to the scope conferred to the framework regarding employees, third parties or, if necessary, the population[3].

Ideally, the adoption of this framework by a community or organization should be accompanied by information sessions and training sessions for leadership, managers, directors and employees. Moreover, the population of a community should be properly informed of its rights and the measures implemented to protect them.

---

[1] Resolution no. 07/2012 — *Framework related to the protection of information held by a First Nation community or organization of Quebec*. (Included in Annex A of this document)

[2] FNQLHSSC, *Analysis Committee regarding the development of an act or policy related to the protection of personal information and access to information intended for the First Nations of Quebec – Preliminary report on the options*, submitted to the Assembly of First Nations of Quebec and Labrador, Hotel Delta, Montreal, June 2011. (Included in Annex C of this document)

[3] *Id.* see page 7 and following ones.

Table of contents

Preamble

The Council[4] of the [COMMUNITY][5] acknowledges that its administrative services hold and use a considerable amount of personal and confidential information;

The Council of the [COMMUNITY] recognizes that persons who accept to provide their personal data for administrative purposes have the right to see the use of this information limited to the purpose for which it was collected and that the information held by administrative services be protected;

The Council of the [COMMUNITY] acknowledges the fact that various information management systems are or will be implemented in collaboration with First Nations commissions and regional organizations along with other partners;

The Council of the [COMMUNITY] acknowledges that the right to protection of personal and confidential information held by the administrative services of band councils and First Nation organizations rests on an imprecise statutory basis;

The Council of the [COMMUNITY] declares that it has the right, will and capacity to implement its own administrative mechanisms to protect personal information and access to information in the organization that it manages, within the territory that it administers;

This [Regulation/Policy/Act][6] is adopted by the Council in response to the needs of the population with regard to the protection of personal information and access to information, as expressed in resolution no. 02/2011, adopted by the Chiefs of the Assembly of First Nations of Quebec and Labrador (AFNQL) on January 27, 2011;

This [Regulation/Policy/Act] is also adopted to take into account the concerns of the [COMMUNITY] with regard to the protection of their collective data and confidential information. These concerns were raised in resolution no. 03/2011, adopted by the AFNQL Chiefs on the aforementioned day;

This [Regulation/Policy/Act] is intended for the band council and its administrative services and applies to the entire territory of the [COMMUNITY].

4 Band Council or Board of Directors
5 Insert the name of your Community or your organization. If the policy applies to an organization, it must be adapted.
6 The Community or organization will choose the form of this document.

Chapter 1 – Interpretation and definitions

In this [Regulation/Policy/Act], the sections that present requirements are formulated using terms such as “must” and “will have to” while suggestions, guidelines and working examples are presented using terms such as “can”, “will be able to” and “should.”

Glossary of terms and expressions used in this [Regulation/Policy/Act]:

- “[**COMMUNITY**]”: includes all entities of the [COMMUNITY], including the Council, services and general administration.
- “**Council**”: an entity composed of persons elected to govern the [COMMUNITY] according to rules in force within the community.
- “**Director**”: the person in charge of a service (general administration, education, health, social services, police, housing, etc.) of the government of [COMMUNITY] or a director of an entity (such as an economic development corporation that belongs to the community) under the jurisdiction of the government of [COMMUNITY]. In addition, it includes any other person authorized by the [COMMUNITY].
- “**Collective Data**”: all data held by the [COMMUNITY] as defined in section 15.
- “**Employee**”: any person who acts for the [COMMUNITY] or agencies under the jurisdiction of the [COMMUNITY], regardless of employment status (permanent, contract or volunteer).
- “**Individual**”: any person whose personal information has been collected by the [COMMUNITY].
- “**Confidential information**”: information held by the [COMMUNITY] that the [COMMUNITY] wishes to keep confidential as described more fully in section 16.
- “**OCAP Principles**”: The principles of Ownership, Control, Access and Possession crystallize themes that First Nations of Canada have been advocating for a very long time. The main notions conveyed concern the collective ownership of group information, First Nations control over research and information, First Nations management of access to their data and physical possession of said data. The OCAP Principles are described more fully in **Annex B.**
- “**Personal Information**”: any information regarding a natural person that allows the person to be identified, except for the person’s name, employment title in an organization, work address and telephone number at work.
- “**Person in charge**”: a member of [COMMUNITY] management who acts as the person responsible for the protection of personal information, collective data and confidential information belonging to the [COMMUNITY].

- "**Service**": any component (including, for example, general administration, education, health, social services, police, housing, and so on) of the government of [COMMUNITY] or any entity (such as an economic development corporation) under the jurisdiction of the government of [COMMUNITY].

- "**System**": any electronic component or device that serves to collect, use, process, store or transmit personal information including communication and information management systems and their components. Services allowing access to the Internet, an intranet and email are included. Hand-held electronic storage and communication devices are also included.

Chapter 2 – General Provisions

1. Authority under which this [Regulation/Policy/Act] is adopted

This [Regulation/Policy/Act] is adopted by means of a [RESOLUTION, REFERENDUM, ETC.] in accordance with the rules in force in the [COMMUNITY].

2. The coming into force of this [Regulation/Policy/Act]

This [Regulation/Policy/Act] will come into force on [DATE]. [It] applies to all personal information, collective data and confidential information in the Council's possession as well as the services and agencies under the jurisdiction of the Council at the time this [Regulation/Policy/Act] comes into force, regardless of when the information was collected by the [COMMUNITY].

3. Guiding Principles

This [Regulation/Policy/Act] respects the following guiding principles:

- First Nations have the right to enjoy protection of their information at least equivalent to the protection enjoyed by all Canadians;
- The rules governing the protection of personal information and collective data must be applied in accordance with the principles of Ownership, Control, Access and Possession (OCAP) as recognized by First Nations;
- Every First Nation has the inherent right to decide on the rules regarding the protection of personal information and collective data within its territory;
- As an autonomous government, the Council can exercise its inherent powers over the community's territory through a policy, regulation or act;
- The rules regarding the protection of information and collective data must be applied in compliance with international agreements, including the *Universal Declaration of Human Rights*, the *International Covenant on Civil and Political Rights*, the *United Nations Declaration on the Rights of Indigenous Peoples*, and the *American Declaration of the Rights and Duties of Man*.

4. Purpose

In the spirit of the guiding principles stated above as well as in accordance with the principles of accountability and transparency with regard to personal information and collective data under the jurisdiction of the [COMMUNITY], this [Regulation/Policy/Act] aims to protect and more specifically:

a) to enact rules and requirements with regard to the collection, use, protection, communication, sharing, conservation and disposal of personal information and collective data;

b) to grant individuals the right to request access to their own personal information and request correction of this information;

c) to clarify and make public the responsibilities and rights of leadership, directors, managers workers, personnel and individuals with regard to the protection of personal information and collective data.

5. Application

This [Regulation/Policy/Act] applies to all components of the [COMMUNITY] as well as to all entities under its control, to its employees, and members of Council, including the Chief.

6. Amendment to this [Regulation/Policy/Act]

The Council can, at its discretion, amend this [Regulation/Policy/Act] and specify when the amendment is to take effect.

7. Offences

Any offence against this [Regulation/Policy/Act] can lead to penalties including dismissal or legal remedies.

8. Person in charge, complaints and reviews

a) The [COMMUNITY] will name a member of the management to be the person in charge of the protection of personal information, confidential information and collective data;

b) Any individual can file a complaint with the person in charge regarding a real or presumed offence against this [Regulation/Policy/Act];

c) Upon receiving a complaint filed under section 8(a), the person in charge will lead an investigation and take measures aimed at correcting the situation, including, if necessary, penalties pursuant to section 7.

d) If need be, the person in charge can refer to a community legal advisor or the person responsible for the protection of personal information at the FNQLHSSC to discuss the subject or a specific situation.

Chapter 3 – Rules regarding the collection and protection of personal information

9. The collection of personal information

9.1. Collection in line with the mission of the [COMMUNITY]

Generally speaking, the collection of personal information by the [COMMUNITY] is limited to information that has a direct link with the mission of the [COMMUNITY] and is required to undertake its activities. The mission of the [COMMUNITY] is to act as the elected government of the [COMMUNITY], in the best interest of all its members, and in particular: [EACH COMMUNITY CAN MODIFY THIS AS NEEDED].

a) To ensure the general wellbeing of the population by providing services in the following sectors: socio-economic development, health and social services, education and culture, housing, assets and infrastructure, police, land management, and so on;

b) To defend and promote the collective rights of its members [*THE COMMUNITY CAN COMPLETE THIS BY ADDING FOR EXAMPLE: as listed on the band registry/regardless of their place of residence (OR BOTH)*].

9.2. Collection from an individual

Unless obtained from a third party in accordance with section 9.3, personal information collected by the [COMMUNITY] must originate directly from the individual in question by obtaining his or her implicit or explicit informed consent, in writing or otherwise.

The Council or service that collects personal information must, when possible, provide the following information to the individual:

a) The purpose of the collection;

b) The third parties with whom the personal information could be shared;

c) The title, business address and telephone number of the person in charge.

9.3. Collection through a third party

The informed consent of the individual in question must be obtained, in writing or otherwise, before collecting personal information through a third party. However, the [COMMUNITY] can obtain personal information through a third party without an individual's consent in the following situations:

a) The collection is authorized by a Canadian or Quebec law or regulation or by a [COMMUNITY] regulation or resolution;

b) The collection is necessary for service delivery;

c) The collection is in the individual's best interest, and consent cannot be obtained in a timely manner or could pose a risk to the person's mental or physical health;

d) The information is collected as part of an investigation of an offence committed against an act or a regulation of the [COMMUNITY], Canada or Quebec.

10. Accuracy and retention of personal information

a) The [COMMUNITY] must take all reasonable measures to ensure that the personal information that it plans to use in making a decision about an individual is as complete, up-to-date and accurate as possible;

b) The [COMMUNITY] must retain personal information for at least one year after its last use in order to allow the individual access to it. When the initial retention period of one year has expired, the [COMMUNITY] must erase or destroy the person's information once it becomes clear that this information no longer serves the use for which it was collected and that no statutory disposition requires that retention be prolonged. The destruction must be undertaken in a secure manner and in compliance with applicable legal or other rules (for example, rules regarding tax laws or as required by financial agreements with government agencies);

c) Personal information can be erased or destroyed during the one year period in the following situations:

    i. The individual has consented in writing to a shorter retention period; or

    ii. The retention of the information for a shorter time period is required by a [COMMUNITY] regulation or policy, a Canadian or Quebec law or regulation, or is ordered by a court or other agency empowered by law to issue such an order.

d) Personal information must be retained for a longer period of time when a Canadian or Quebec law or regulation requires that it be retained for more than one year. Certain professionals are required to retain client files for up to seven (7) years. For example, if the [COMMUNITY] has entered into agreements with regard to health and youth protection, the laws applying to these sectors indicate specific rules related to document retention. In such case, the [COMMUNITY] will draw up a retention schedule in which it determines periods of use and the medium of retention of its documents.

11. Use and communication of personal information

11.1 Use and consistent use

a) Generally speaking, as described in section 9, the [COMMUNITY] uses personal information in order to carry out its mission.

b) The delivery of each service relies on different types of personal information. Each Service uses personal information for the purpose given when collecting the information with the consent of the individuals in question.

c) A service can also use personal information for another purpose but this use must be consistent with the original purpose given for collecting the information. It must take into account the nature of the services that it aims to support. Consistent use is a secondary use that is linked directly and logically to the initial use of the information. Obviously, consistent use must always be reasonable and take into account the circumstances and expectations of the individual in question.

> *For example, if a home telephone number was collected for nursing visits, using this same number to facilitate social worker visits would be a consistent use. Communication of a student's personal information by a teacher or school principal in order to provide the student with counselling services would also be an example of consistent use. However, the use of information regarding an employee's absenteeism to determine whether the employee is qualified for another position is not an example of consistent use. Providing information about the identities of people living in subsidized public housing to the police is another example of inconsistent use.*

11.2 Use limited to persons in question

Personal information can only be transmitted to employees and members of the Council who need the information to perform their duties. In addition, employees working under the Professional Code, including nurses, nursing assistants, social workers, lawyers, accountants and guidance counsellors, are required to respect confidentiality.

The title, status or position of an employee, manager or elected member of the Council does not constitute, in itself, an acceptable reason for having access to an individual's personal information. Any pressure or threat from an employee, manager or elected member must be brought to the attention of the person in charge who will take the necessary measures, as described in sections 7 and 8.

It would be perfectly acceptable, however, for an elected member of a Council to have access to relevant personal information about a community member if this person has requested the Council member's help in resolving an administrative problem with a Service.

11.3 Use between Services

A Service can transfer personal information to another Service if the information is to be used in the same manner as initially foreseen or in cases of consistent use. However, if the transfer is for an inconsistent use, consent must be obtained once again.

> *For example, certain medical information might, in some cases (mental illness, an individual's suicidal tendencies, etc.) need to be shared with social services. However, this information could not be shared with senior management without the individual's consent if this person were to apply for a job.*

11.4 Other uses and communication with third parties

The [COMMUNITY] cannot use personal information for reasons other than those described in section 11.1 unless: consent has been obtained once again from the individual in question; use or communication to another entity is covered in section 11.5 "Research;" or use or communication is covered by one of the following exceptions:

a) When it is otherwise prescribed by a [COMMUNITY] regulation or resolution or by a Canadian or Quebec law or regulation;

b) When it is required by an authorized representative of a [COMMUNITY] who needs such personal information for the reason it was originally provided or for a consistent use, in the pursuit of his or her legitimate activities in the name of the [COMMUNITY], as long as the representative agrees in writing to use the information only as necessary and keep it confidential;

c) When the information is required to provide services;

d) When the information helps determine an individual's eligibility for benefits or programs;

e) When the information is required by internal or external auditors or by a lawyer whose services have been retained by the Council;

f) When required in an investigation into an offence against a [COMMUNITY] resolution or regulation or against a Canadian or Quebec law or regulation;

g) When the information is the subject to an order by a court, judicial body or quasi-judicial body;

h) When the information is already public, insofar as communicating the information does not risk revealing new facts or information not yet in the public domain;

i) When, in the opinion of the director or person in charge, the use or communication of the information is in the best interest of the individual and the individual's consent cannot be reasonably obtained;

j) When, in the opinion of the director or person in charge, the use or communication of the information is necessary to protect the life, safety, or physical or mental health of the individual or another person;

k) When the use or communication of the information serves to recognize the ancestral rights of the [COMMUNITY] or to settle its claims, as long as the use or crosschecking undertaken is part of research and:

   i. will not injure individuals;

   ii. brings advantages that will clearly serve the public interest or support the claims of the [COMMUNITY].

11.5 Communication for research purposes

A service can release personal information for research purposes without authorization from targeted individuals only when:

a) The research topic could not be addressed without releasing the information in question;

b) It is not reasonably possible to obtain the consent of the individuals targeted;

c) The director has received a commitment in writing from the recipient of the information that ensures:

   i. the confidentiality of the personal information;

   ii. the security of the personal information by committing the recipient to inform the director as quickly as possible of any security incident that affects or risks affecting the personal information in question;

   iii. the return or destruction of data that would allow the targeted individuals to be identified;

   iv. a publication ban on research results in a form that risks revealing the identity of the targeted individuals;

11.6 No communication for commercial purposes

Personal information on individuals will never be used or transferred for commercial purposes. Should this occur, explicit consent from the persons in question will be requested.

12. Personal information regarding employees

12.1 Application of this section to employees of the [COMMUNITY]

a) This section applies to personal information collected or retained by the [COMMUNITY] regarding its employees. This personal information is governed by the Personal Information Protection and Electronic Documents Act (S.C. 2000, c. 5). The other sections of this policy can be used in a supplementary manner if they do not contradict with the above Act.

b) If the employees of the [COMMUNITY] are also part of the [COMMUNITY], their personal information will also be collected as part of their relations with the [COMMUNITY] and its status of First Nation government. In this case, they will be governed by the present policy.

c) The [COMMUNITY] processes the personal information of its employees, collected as part of their employment, separately from the information collected as part of its role as a First Nation government. For example, the [COMMUNITY] knows the salary of its employees. It will not use such information to evaluate whether an individual is eligible for a program. The information will be obtained again from the individual with his or her consent.

12.2 Collection and use of personal information

a) Every employee must be informed of any collection, use or communication of personal information that concerns the employee and consent thereto, except when this would be inappropriate (for example, as part of a fraud investigation).

b) The [COMMUNITY] collects and uses employees' personal information for the purpose of managing employment relationships, including hiring, pay, pension, benefits, management and protection of goods belonging to the [COMMUNITY], performance evaluations, benefit applications and compliance with [COMMUNITY] policies and regulations as well as applicable laws.

c) The [COMMUNITY] will not use this personal information for other purposes unless permitted by law, the employee has given his or her consent, or the employee can reasonably expect the new use. For example, the law permits the use of personal information without consent in order to respond to an emergency situation that puts the life, health or safety of an individual in danger.

d) For example, collected information can include an employee's personal address, date of birth, salary, health status, performance review, information relating to lateness or absenteeism, any disciplinary notices, information recorded on the computer used by the employee, the employee's electronic communications or his or her use of the Internet.

12.3 Communication of personal information

The [COMMUNITY] does not transmit to a third party personal information that it has received from its employees in relation to their employment, except where required for the administration of the employment relationship (such as information transmitted to the government for employee deductions), where permitted by law or where consent has been given by the employee.

For example, the law allows the use of personal information without consent if the information is provided to a lawyer who represents an organization taking part in a recovery action or a governmental institution enforcing a law. Personal information may also be used without consent in an emergency situation where the life, safety, or health of a person is in danger.

12.4 Person in charge, rights of access and security

a) The person in charge must respond to any questions or complaints regarding the personal files of employees and the protection of personal employee information. Any changes to the personal address, telephone number, marital status, dependant(s), beneficiary, or emergency contacts must be communicated to the person in charge as soon as possible.

b) The right of access and correction in section 13 as well as the security measures in section 19 apply to personal information collected as part of the employment relationship, along with any necessary modifications.

Chapter 4 – Right of access and correction

13. Right of access and correction

a) An individual has the right to request access to his or her own personal information held by the Council or a Service, subject to section 14.

b) The [COMMUNITY] can charge the applicant reasonable fees to cover the cost of research and reproduction of documents that include the personal information. At no time can the [COMMUNITY] charge a fee greater than the real cost of processing the access request.

c) An individual has the right to request the correction of his or her personal information held by the [COMMUNITY] without cost.

d) The individual must be informed, within thirty days following the receipt of a written request for access or correction, of whether access will be granted or whether the corrections will be made. Where pertinent, the response letter must also specify the reason why the access or corrections requested will not be provided or undertaken.

e) An additional period of thirty days may be granted if justified, but the individual must be informed of any extension in the processing of his or her request for access or correction.

14. Exceptions to the right of access

An individual can be refused his or her right of access to his or her own personal information in the following circumstances:

a) Access would likely endanger the life, safety or health of the individual or another person;

b) Access would likely interfere with law enforcement or an investigation;

c) Access is prohibited by a Canadian or Quebec law, court order, or order issued by a quasi-judicial body;

d) The information is covered by lawyer-client privilege;

e) The information was obtained confidentially from another government, including another First Nation government or any of its agencies;

f) The information contains personal information about a third party who refuses to provide access, and the information requested cannot be separated from such third party information;

g) The information is part of closed-door deliberations held by the Council or its members as part of their work as councillors;

The aforementioned exceptions do not apply in cases where an individual's access to his or her own personal information can help protect the life, safety or health of the individual or another person.

Chapter 5 – Protection of collective data and confidential information

15. Collective data

In addition to personal information, the [COMMUNITY] possesses other information that it wishes to protect in order to ensure compliance with OCAP principles.

The [COMMUNITY] holds sets of nominal and redacted data created from the personal information of members of the [COMMUNITY], related, in particular, to health, social services, and education. These data are referred to as “collective data.”

The [COMMUNITY] possesses data relating to the uses and characteristics of its territory, such as information regarding the soil, subsoil, natural features, fauna and flora. This is all considered to be “collective data.”

“Collective data” also includes the traditional knowledge of the [COMMUNITY]. This knowledge can come in different forms (data collection, studies, books, musical or video recordings, etc.).

Collective data are protected regardless of their media format, whether physical, electronic or otherwise. Such data are considered to be confidential information unless the [COMMUNITY] decides to make the data public.

16. Confidential Information

The [COMMUNITY] holds information, orally, in writing, or otherwise, that is not generally accessible and that the [COMMUNITY] works to keep secret. This information is referred to as “confidential information”. This information can belong to the [COMMUNITY], to its members individually, to all the members of the [COMMUNITY] as a collective, or to a third party.

As stated in section 15, confidential information includes collective data in cases where the [COMMUNITY] has not decided to make this information public.

Confidential information can also include:

- The strategies used by the [COMMUNITY] when negotiating with other governments (federal, provincial or municipal) or with contract workers, unions, individuals or businesses;
- Information regarding minutes or statements made during meetings, negotiations or as part of [COMMUNITY] activities;
- Information obtained confidentially from other governments;

- Information regarding law enforcement, investigations or audits, including the techniques and strategies used when undertaking such activities;
- Information that, if released, would likely compromise the safety of an individual or of the Community;
- Information covered by lawyer-client privilege;
- Information about notices, recommendations, or analyses obtained or produced as part of [COMMUNITY] activities;
- Information regarding budgetary, financial and administrative matters;
- Information that is covered by a signed agreement between the [COMMUNITY] and another party, such as another government (federal, provincial or municipal), individual, or business, that prohibits the release of such information;
- Certain information regarding the protection of [COMMUNITY] infrastructures such as buildings, data processing systems, and so on.

17. General protection measures

In order to protect collective data and confidential information, the [COMMUNITY] makes sure to:

a) Limit the release of such information to persons who legitimately need it in order to do their work;

b) Train employees on how to protect information (protect written and electronic records, obtain authorization from the director or person in charge before transmitting collective data and confidential information, avoid discussing or processing confidential information in public places, not releasing confidential information belonging to the [COMMUNITY] following the end of employment...);

c) Apply the security measures described in section 19 with necessary modifications regarding collective data and confidential information.

It is understood that these measures do not apply to collective data that the [COMMUNITY] has decided to make public.

18. Third party access

a) If a third party wishes to have access to collective data or confidential information, the [COMMUNITY] will make sure to apply the OCAP principles.

b) The [COMMUNITY] will ensure that the third party requesting access to collective data not yet made public or to confidential information has a statutory or contractual basis for

requesting access to this information, or that this access is in the interest of the [COMMUNITY]. For example, in the case of a contribution agreement or a tax law.

c) The [COMMUNITY] will ensure compliance with the principles stated below and, if possible, will have the third party sign a confidentiality or use of information agreement that:

- Clearly describes permissible use by the third party and indicates that any other use requires additional consent from the [COMMUNITY];
- Indicates the interest of the [COMMUNITY] in permitting the use of its data;
- Prohibits the public release of data and its transmission to a third party;
- Requires an accountability report on the results of data use and compliance with the agreement.

Chapter 6 – Security Measures

19. Security Measures

Personal information, confidential information and collective data held by the [COMMUNITY] must be properly protected from unauthorized collection, use, modification, access or destruction. This implies the implementation of a security program that includes the following elements:

a) The nomination of a **person in charge of security** responsible for implementing reasonable security measures to ensure the adequate protection of information against unauthorized access, modification, use, or destruction;

b) **Physical security**: that includes the implementation of security measures to control and limit access to each service including padlocks, doors, fences, and so on;

c) **Information technology security**: that includes the implementation of measures to protect data processing systems as well as other electronic devices (fax machines, telephones and handheld organizers, computers, servers and peripherals) used to collect, process, store and transmit sensitive information of both a personal and impersonal nature;

d) **Contract security**: aimed at ensuring that authorized third parties adhere scrupulously to the requirements of the [COMMUNITY] with regard to security and privacy protection;

e) **Personnel security:** aimed at ensuring that employees and members of Council adhere scrupulously to all the requirements of the [COMMUNITY] with regard to security and privacy protection. Employees must respect the present Policy;

f) **Conducting threat and risk assessments as well as audits and investigations:** aimed at regularly identifying situations that could affect the confidentiality, integrity, availability and strategic value of information as well as effective reactions to security incidents;

g) **Developing plans for emergency measures and operational continuity:** aimed at ensuring the continual delivery of services to community members as well as consistent access to the information essential to service delivery.

Annex A
RESOLUTION no. 07/2012

Secrétariat
de l'Assemblée des
Premières Nations
du Québec
et du Labrador

Secretariat of the
Assembly of the
First Nations
of Quebec
and Labrador

250, Place Chef Michel Laveau, bur. 201, Wendake, QC G0A 4V0
Tél. : (418) 842-5020 / 842-5274 Téléc. : (418) 842-2660

RESOLUTION NO. 07/2012

FRAMEWORK RELATED TO THE PROTECTION OF INFORMATION HELD BY A FIRST NATION COMMUNITY OR ORGANISATION OF QUEBEC

WHEREAS the administrative services of the First Nation governments and organizations possess and utilize a vast amount of personal information;

WHEREAS the people who accept to provide their personal data for administrative purposes have the right to ensure that it is only being used for the purposes that it is collected for;

WHEREAS the First Nation governments and the regional commissions and organizations are currently implementing, or will eventually implement, various information management systems;

WHEREAS the information in the possession of the First Nation governments, interveners and citizens must be protected;

WHEREAS the legal opinions produced in accordance with the requests of the FNQLHSSC indicate that the right regarding the protection of the personal information in the possession of the administrative services of the First Nation governments and organizations is supported by an imprecise legislative foundation;

WHEREAS the First Nations of Quebec and Labrador have the right, the political will and the capacity to implement their own administrative mechanisms related to the protection of personal information and access to information;

WHEREAS the Assembly of First Nations of Quebec and Labrador adopted on January 27, 2011, resolution 02/2011 supporting the FNQLHSSC for the creation of a committee targeting the analysis of the possibilities surrounding the development of an Act or policy related to the protection of personal information and access to information intended for the First Nations of Quebec communities and organizations;

WHEREAS on June 14, 2011, this committee submitted a preliminary report of the options to the Chiefs' Assembly of the First Nations of Quebec and Labrador which approved the continuation of the work;

WHEREAS the committee's work led to the development of a framework related to the protection of information held by a First Nations community or organisation of Quebec;

WHEREAS the proposed framework can be adopted as is by any community that so desires in the form of a law, regulation or policy or, if the need arises, it can be adopted by any organisation in the form of an internal regulation or policy;

WHEREAS the proposed framework is a means specifically designed to support the communities and organisations that are required to implement appropriate regulations in order to protect the personal information, collective data and confidential information they are holding,

BE IT RESOLVED THAT the Assembly of First Nations of Quebec and Labrador hereby adopt the framework related to the protection of information held by a First Nations community or organisation of Quebec in order to put it forward as a model for the First Nation governments and organisations;

BE IT RESOLVED THAT the Assembly of First Nations of Quebec and Labrador support the FNQLHSSC in the development of training and information documents intended for the managers and employees of the communities and organisations adopting the framework.

PROPOSED BY: Chief Terence McBride, Timiskaming
SECONDED BY: Chief Raphaël Picard, Pessamit
ADOPTED BY CONSENSUS IN MONTREAL ON JUNE 12, 2012

Ghislain Picard
Chief of the AFNQL

Annex B
OCAP Principles

Taken from **The First Nations of Quebec and Labrador Research Protocol by the AFNQL (2005)**

OCAP principles promote self-determination applied to research; it is a political response to persistent colonial approaches to research and information management. They can be applied to research, monitoring and surveillance, surveys, statistics, cultural knowledge and so on. Generally speaking, these principles concern all aspects of information, including its creation and management.

- Ownership: The notion of ownership refers to the relationship of a First Nation community with its cultural knowledge, data and information. According to this principle, a community or a group owns information in the same way individuals own their personal information. It is distinct from stewardship. The stewardship or care taking of data or information by an institution that is accountable to the group is a mechanism through which ownership may be asserted.

- Control: The aspirations and rights of First Nations members to maintain and regain control of all aspects of their lives and institutions extend to research, information and data. The principle of control asserts that First Nations members, their communities and representative bodies are within their rights in seeking to control all aspects of research and management processes that affect them. First Nations' control of research can include all stages of a specific research project, from its conception to its completion. The principle extends to the control of resources and review processes, the formulation of conceptual frameworks, data management and so on.

- Access: First Nations members must have access to information and data about themselves and their communities, regardless of where they are held. The principle also refers to the right of First Nations communities and organizations to manage and make decisions regarding access to their collective information. In practice, this may be achieved through standardized, formal protocols.

- Possession: In principle, ownership identifies the relationship between a people and its data while possession and stewardship are more literal. Even if possession (of data) is not a condition of ownership per se, it constitutes a mechanism by which ownership can be asserted and protected. When a party owns data belonging to another party, there is a risk of breech or mistrust. Such a situation requires unending vigilance, particularly when there is lack of trust between the owner and the possessor.

www.cssspnql.com