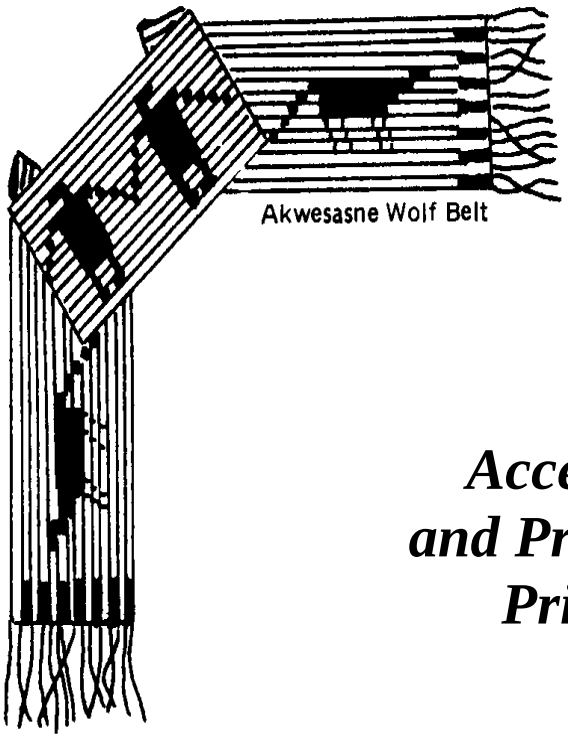
Note: this regulation is presently being reviewed and updated.



Access to Information and Protection of Personal Privacy Regulation

Final Version
March 12, 2004

Mohawk Council of Akwesasne

Interpretation of This Manual

The requirements for this Regulation are identified in the text by the use of terms such as "shall," "will" and "must." The guidelines, which are identified by terms such as "should," "may," "can" and "could," are meant to provide examples of best or recommended practices.

Key Definitions:

In this manual, the terms:

- "**Community**"**:** refers collectively to those individual people who are registered members of the Mohawk Council of Akwesasne.
- "**Council**": refers to the Mohawk Council of Akwesasne consisting of those candidates duly elected under the Election and Voting Custom Regulations.
- "**Chief Administrative Officer**" refers to the person appointed by Council to hold the principal, non-political management position for the government of the Mohawk Council of Akwesasne.
- "**Court**" refers to the Mohawk Court of Akwesasne.
- "**Department**" refers to a branch of the organization delivering specialized community services, under the authority of the Mohawk Council of Akwesasne.
- "**Director**" refers to a departmental administrator.
- "**Enactment**": refers to a code, a law or a regulation of the Mohawk Council of Akwesasne or an Act or a Regulation of another government.
- "**Mohawk Court**" refers to the Mohawk Court of Akwesasne.
- "**Mohawk Council of Akwesasne (MCA)**": refers to the community government as an organized entity. The government is governed by elected officials who have a governance branch, an administrative branch, and departments that deliver services to community members often under the advice of community boards.

- "**Program**" covers all planned and organized activities, including "projects," "systems," "policies" and "procedures" that seek to further the objective(s) of the Mohawk Council of Akwesasne. Those terms are interchangeable and must be understood in the specific context where they are used.

- "**System**" refers to a group or combination of interrelated electric and electronic components that are used for the collection, use, disclosure, sharing, transmission, distribution, retention and disposal of personal information. This definition includes computerized information management systems; data warehouses; servers; LANs; equipment that allows for the connection of a workstation to the Internet and to the departmental Intranet and email systems; traditional telephone systems; wireless telephone systems; and all other electronic means that are used to create, manipulate or communicate information.

Other Definitions:

We strongly encourage the readers of this manual to refer often to the other definitions provided in Appendix 2 (Definitions and Acronyms), as these definitions provide essential explanations of the terms that are commonly used in the access to government records, privacy protection and information security fields. Appendix 8 (Fundamentals of Privacy and Information Security) also provides a summary of the concepts that are key to the privacy and information security field and covers technical terms and expressions such as "need to know," "confidentiality," "integrity," "availability" and "value."

Structure of This Manual

This manual is comprised of the following chapters:

Chapter One – Regulation:

This chapter:

- provides the objectives of the Regulation as they relate to the right of access to Mohawk Council of Akwesasne's records, the management of personal information, and the protection of sensitive information by departments; and

- outlines the principles that must guide departments in interpreting and applying the Regulation.

Chapter Two – Access to Information:

This chapter constitutes the framework for the processing of requests for information under the Regulation. It identifies the categories of individuals who are eligible for a right of access under the Regulation; it establishes the requirements for the exercise of the right of access; it describes the procedure for the processing of access requests; and it provides the criteria for the disclosure and withholding of information.

Chapter Three – Protection of Personal Privacy:

This chapter establishes the framework for the collection, use, disclosure, retention and disposition of personal information by departments. It also outlines the requirements for the conduct of privacy impact assessments and provides guidance for the conduct of such assessments.

Chapter Four – Requirements For the Protection of Sensitive Information:

This chapter provides the criteria that must be used by departments to determine the sensitivity of personal and non-personal information, and it establishes baseline security requirements for the protection of that information.

Chapter Five - Appendices:

Table of Contents

Chapter One

Access to Information and Protection of Personal Privacy Regulation

1. Authority for This Regulation

This Regulation is issued under the authority of the Mohawk Council of Akwesasne through Council Resolution #02/03 - **.**

2. Regulation Objective

This Regulation supports the following objectives of the Mohawk Council of Akwesasne:

a) To promote government accountability and transparency by granting to the members of the Akwesasne community a right of access to the records of Council and departments;

b) To identify the categories of information that may or must be subject to an exception to the right of access;

c) To establish the framework for the collection, use, disclosure, retention and disposition of personal information by Council and departments;

d) To establish baseline security requirements for the protection of the sensitive information that is in the custody or under the control of Council and departments.

3. Representatives

a) An applicant may retain the services of a representative to assist him or her in the exercise of his or her rights under this Regulation;

b) The Director of a department may ask the representative to provide satisfactory evidence of his or her status as representative of another person before complying with any request for services by that person under this Regulation;

c) Except as specified in paragraph d), an appointed representative has the same rights and obligations under this Regulation as the person that he or she represents, and any notice required to be given to an individual under this Regulation may be given to the representative of that person;

d) Any right or power conferred on an individual by this Regulation may be exercised:

i. if the individual is deceased, by the individual's personal representative, but only for the administration of the individual's estate,

ii. if a guardian or trustee has been appointed for the individual under an enactment of the Mohawk Council of Akwesasne, Canada, Ontario or Quebec, by the guardian or trustee if the exercise of the right or power relates to the powers and duties of the guardian or trustee,

iii. if an agent has been designated under a personal directive under an enactment of the Mohawk Council of Akwesasne, Canada, Ontario or Quebec, by the agent under the authority of the directive if the directive so authorizes,

iv. if a power of attorney has been granted by the individual, by the attorney if the exercise of the right or power relates to the powers and duties of the attorney conferred by the power of attorney,

v. if the individual is a minor, by a guardian of the minor in circumstances where, in the opinion of the Director of the department concerned, the exercise of the right or power by the guardian would not constitute an unreasonable invasion of the personal privacy of the minor or jeopardize the safety of the minor, or

vi. by any person with written authorization from the individual to act on the individual's behalf.

4. Mandatory Requirements

Council and departments must:

a) allow the members of the Akwesasne community to have access to all the information contained in the records that are in their custody or under their control, except for the information in those records that qualifies for an exception under this Regulation;

b) collect, use, disclose, retain and dispose of personal information in accordance with this Regulation;

c) protect the sensitive information in their custody or under their control in accordance with this Regulation.

5. Application

a) This Regulation applies to all institutions, organizations and bodies that are listed in Appendix 1. For the purpose of this Regulation, the term "department" is applicable to all the institutions, organizations and bodies that are listed in Appendix 1.

b) This Regulation does not replace existing rights that individuals possess under other enactments of the Mohawk Council of Akwesasne or under enactments of Canada, Ontario and Quebec, including the right of access to the information that they need for court proceeding or similar hearing purposes.

6. Accountability and Non-Compliance

a) The Director of each department is accountable for implementing this Regulation;

b) The Director may delegate in writing any duties, powers or functions conferred upon him or her by this Regulation to any person;

c) Non-compliance with the requirements of this Regulation may lead to the imposition of sanctions, in accordance with Article 6 (Conduct) of the Mohawk Council of Akwesasne's General Personnel Policy.

7. Review and Complaint Mechanism

Subject to this Regulation, a member of the Mohawk community may complain in writing to the Mohawk Court about the interpretation, administration or implementation of this Regulation, including:

a) where the individual has been refused access to the information that the individual has requested under this Regulation;

b) where the individual has been informed by the Director of a department that the corrections that he or she has requested be made to his or her personal information will not be made;

c) where the individual disagrees with the amount of fees that he or she is being asked to pay in order to be granted access to information under this Regulation;

d) where the Director of a department has not responded to a request for information or a request for the correction to personal information within thirty days from the date of receipt of the access request;

e) where the individual believes that his or her personal information has been, is being or will be collected, used, disclosed, retained or disposed of by a department in contravention with this Regulation;

f) where the individual has reasons to believe that sensitive information about himself or herself or about the organization that the individual represents is not being accorded the level of protection required by this Regulation.

8. Coming Into Effect of This Regulation

a) This Regulation comes into effect ninety working days following Council's Resolution enacting it;

b) Notwithstanding paragraph a):

I. the right of access to Council's and department's records applies to all the records that existed at the time of the coming into effect of this Regulation,

II. the right of access to personal information and the right to request the correct of personal information apply to all the records that existed at the time of the coming into effect of this Regulation.

9. Priority of This Regulation

a) Subject to section 5 and except where otherwise specified in another Regulation, this Regulation takes priority over all other Regulations, policies and other administrative instruments of the Mohawk Council of Akwesasne;

b) Council may, at any time, amend an existing Regulation to include a provision whereby that other Regulation takes precedence over this

Regulation. Council may also stipulate the date on which such amendment takes effect.

10. Amendment of This Regulation:

Council may, at any time, amend or update this Regulation and stipulate the date on which such amendment or update takes effect.

11. Mohawk Court of Akwesasne

Subject to this Regulation, the Mohawk Court of Akwesasne:

a) must receive and investigate all complaints that pertain to the interpretation and the administration of this Regulation;

b) may establish procedures for the mediation, investigation or arbitration of complaints that the Court conducts under this Regulation;

c) may request the production of all documents that are in the custody or under the control of the Mohawk Council of Akwesasne or one of its departments that the Court needs for the exercise of its responsibilities under this Regulation;

d) may, where the mediation of a complaint has failed, make orders regarding the interpretation or the application of this Regulation;

e) may ask an employee of a department to testify under oath and to reveal information that the employee possesses in relation to a complaint under this Regulation;

f) may order the Director of a department to implement measures for the protection of an employee or a contractor against disciplinary or other administrative actions for:

    i. complying with a Court's request, or

    ii. reporting any facts in relation to the implementation of this Regulation to the attention of the Court.

12. Departmental Annual Reports on the Implementation of This Regulation

The Director of each department shall, within ninety days following the end of each fiscal year, present an annual report to Council on the administration of this Regulation. The report shall provide the following information:

- the number of access requests for personal and for non-personal received under this Regulation during the year and the final disposition of those requests;

- a summary of the important privacy-related issues that arose during the year and how those issues were disposed of;

- a summary of the important information security-related issues that arose during the year and how those issues were disposed of;

- statistical information in relation to the complaints that have been made to the Mohawk Court of Akwesasne in relation to the administration and the implementation of this Regulation;

- any other information which, in the opinion of the Director, should be reported to Council.

The Director of department shall make his or her report available in a convenient form to all the members of the community.

13. Departmental Annual Reports of the Mohawk Court of Akwesasne

The Mohawk Court shall, within ninety days following the end of each fiscal year, present an annual report to Council containing the following information:

- the number of complaints, by categories, received against departments under this Regulation during the year, and a summary of the final disposition of those complaints;

- a summary of the important privacy-related issues that arose during the year and how those issues were disposed of;

- a summary of the important information security-related issues that arose during the year and how those issues were disposed of;

- any other information which, in the opinion of the Court, should be brought to the attention of Council or to the attention of the members of the community.

The Court shall make its annual report available in a convenient form to all the members of the community.

Chapter Two

Access to Information

Part One – Submitting and Responding to Access Requests

14. Exercise of the Right of Access

a) An applicant must seek access directly from the Director of the department that he or she believes has custody or control of the records;

b) Except where otherwise specified in this Regulation, a request must be in writing and must provide enough detail to enable the department to identify the record;

c) A department may accept a verbal request from an individual who is not physically or otherwise capable to submit the request in writing;

d) An individual may ask to examine the record or to obtain a copy of the record.

15. Duty to Assist an Applicant

a) A department must make every reasonable effort to assist an applicant in identifying and locating the records to which he or she is seeking access.

b) Notwithstanding paragraph a), a department does not have to acknowledge the existence of a record where doing so would:

   i. constitute an unreasonable invasion of another person's privacy;

   ii. likely interfere with internal audit or law enforcement activities;

   iii. reveal information that may affect the ability of Council to negotiate land or other claims or to promote and defend the best interests of the members of the Akwesasne Community;

   iv. reveal information that has been obtained in confidence from another government.

c) A department must create a record for an applicant if:

i. the record can be created from information that exists in an electronic form at the time of receipt of the access request, using the department's normal computer hardware and software and technical expertise, and

ii. creating the record would not unreasonably interfere with the operations of the department.

16. Disruptive Access Requests

a) The Court may, after fully investigating the circumstances of the access request, exempt a department from its obligation to respond in whole or in part to one of the following types of access requests:

i. requests that are submitted with a clear intention to cause undue interference with the legitimate electoral process of the Mohawk Council of Akwesasne,

ii. requests that are submitted with a clear intention to cause undue interference with the functioning of Council; or

iii. requests that are submitted with a clear intention to cause undue interference with the business processes of a department.

b) In investigating the circumstances of an access request, the Court shall allow the applicant and the department to submit their observations in person, in writing or in any other way that the Court finds acceptable under the circumstances;

c) An access request shall not be categorized as disruptive for the sole reason that:

i. it involves a large number of records;

ii. it involves a search through a large number of records; or

iii. it could result in the disclosure of embarrassing information for a department or for the Mohawk Council of Akwesasne.

17. Time Limit for Responding to a Request

a) The Director of a department must make every reasonable effort to respond to an access request within thirty calendar days from the date of receipt of the access request at his or her office.

b) The letter of response must provide the following information:

   i. whether access to the record is granted in whole or in part or is denied,

   ii. where access is denied, the specific provision of this Regulation on which the decision to deny access is based,

   iii. that the applicant may make a complaint to the Court about the denial of access,

   iv. the address and the telephone number of an officer or employee of the Court who can answer questions about the complaint and the review process.

c) The Director of a department may extend the time limit for responding to an access request by a reasonable period if:

   i. the applicant does not give enough detail to enable the department to identify the requested record,

   ii. a large number of records are requested or must be searched in order to identify the requested record and responding within thirty calendar days would unreasonably interfere with the operations of the department,

   iii. more time is needed to consult with a third party, another government or another department before deciding whether to grant access to a record, or

   iv. a third party asks for a review of the department's decision to disclose its information.

d) When extending the time frame for responding to an access request, the Director of a department must send a notice to the applicant. The notice must provide the following information:

   i. the reason for the extension,

   ii. when a response can be expected,

iii. the right of the applicant to make a complaint about the extension to the Court,

iv. the address and telephone number of an officer or employee of the Court who can answer questions about the complaint and the review process.

18. Third Party Intervention

a) Where the Director of a department intends to disclose information pertaining to a third party as described in sections 21 and 22 of this Regulation, the Director must give the third party a notice to inform the third party that:

   i. the Director intends to disclose the third party's information in response to an access request received under this Regulation; and

   ii. the information will be disclosed to the applicant in thirty days unless the third party makes representations to the Director of the department before the end of that period.

b) Where the third party has deceased or cannot be located or reached and has no legally appointed representative to decide on his or her behalf, the Director of the department shall make the decision to disclose or not the third party's information on the basis of the relevant circumstances, including:

   i. whether the disclosure would be in the best interests of the party;

   ii. whether the disclosure would be in the best interests of another person or entity; or

   iii. whether the disclosure would be in the best interests of the Mohawk community.

c) Within twenty days following the receipt of the representations from the third party, the Director of the department must give a notice to inform the third party that:

   i. the Director will not disclose the information of the third party; or

ii. the information will be disclosed to the applicant in thirty days unless the third party asks the Mohawk Court to rule that the information not be disclosed.

d) Upon receipt of the request by the third party, the Court will investigate the circumstances of the request and inform the parties of its decision within sixty days.

19. Fees

a) Subject to section 19 k), an applicant must pay a twenty-five dollar application fee when requesting access to the records of a department;

b) The Director of a department must not charge a time processing fee for the first five hours of work that are required to process an access request;

c) When the processing of an access request requires more than five hours of search and preparation, the Director of a department may charge an additional processing fee of six dollars and twenty five cents per quarter of hour (twenty-five dollars per hour) for each quarter of hour in excess of the first five hours of processing time. The time processing fee may only be charged for the following activities:

i. identifying and locating the records,

ii. reproducing and preparing the records for disclosure.

d) The Director of a department must charge a fee of twenty cents per page for the production or the reproduction of the record copies that will be provided to the applicant;

e) The Director of a department must not charge a fee for the production or the reproduction of records that the department will use exclusively as working copies in order to process an access request;

f) The Director of a department may charge a fee in the amount prescribed by Council for all other activities that are involved in the processing of an access request, including the costs associated with the reprogramming of a computer;

g) The Director of a department must not charge a fee to recover the costs associated with the identification of the information in a record that may qualify for an exception to the right of access;

h) The Director of a department may exempt an applicant from having to pay the application, the processing or the document reproduction fees in the following circumstances:

   i. the applicant has produced evidence that he or she cannot afford to pay the requested fee,

   ii. the disclosure of the record is clearly in the public interest,

   iii. upon a decision or a recommendation to that effect from the Mohawk Court,

   iv. for any other reason that the Director of the department considers reasonable.

i) The Director of a department must not charge any fee in excess of the fee allowed by the Mohawk Court in any specific situation;

j) The Director of a department must inform the applicant in writing of the total amount of fees that will be charged for the processing of the access request before initiating its processing. The notice must also contain the following information:

   i. the manner in which the fee was calculated,

   ii. that a deposit representing fifty percent of the total payable fee must be received by the department before the processing of the access request is initiated,

   iii. that the applicant may ask for a total or partial exemption from the fee,

   iv. that the applicant may make a complaint to the Mohawk Court about the fee,

   v. the address and telephone number of an officer or employee of the Mohawk Court who can answer questions about the complaint and review process.

k) Notwithstanding paragraphs a) to i), an applicant must not be required to pay an application, a processing or a document reproduction fee for requesting access to his or her own personal information under this Regulation.

Part Two – Principles Governing the Application of the Exceptions to the Right of Access

20. Principles

The provisions of this part provide the framework for the decisions of departments to grant or refuse access to the records that are requested under this Regulation. The exceptions to the right of access are divided into the four following categories:

a) Mandatory exceptions:

Council has used those exception provisions to identify the categories of information that must not be disclosed by departments under this Regulation. These provisions are characterized by the wording "the Director of a department must refuse to disclose". Where the requested information falls within the scope of a mandatory provision, the Director of the department must refuse access to it and inform the applicant accordingly.

b) Discretionary exceptions:

These exceptions provide that "the Director of a department may refuse to disclose" the requested information. The exercise of the discretion by the Director must meet the following requirements:

- It must be exercised in a reasonable manner: this implies that the Director is able to present realistic and well-founded reasons for the refusal. Information cannot be refused just for administrative convenience or to prevent potential embarrassment;

- It must be adapted to the circumstances of each access request: always refusing access to a certain type of documents would qualify more as a blanket policy rather than as an exercise of discretion, therefore, such an approach would likely be easy to challenge;

- The refusal must not be discriminatory: this means that the Director of the department cannot refuse access to a record by an applicant while disclosing the same record to another person.

c) Exceptions based on a harm test:

The notion of "harm test" is based on the premise that undesirable consequences will result from the disclosure of the requested information. The harm may affect a person, an organization, the Mohawk community or any other interest that is specified in the exception provision. The claim that harm will result from the disclosure cannot be based solely on the subjective fears of an individual or on a subjective assessment of the circumstances by the Director of the department. It must be supported by clear and concrete evidence of certain or probable harm. The three following criteria usually form the basis for demonstrating the harm:

- The likelihood of harm is high: this means that the harm is more than just a remote possibility. The Director has a reasonable degree of certainty that the harm will materialize if the information is disclosed;

- The harm is immediate: this implies that the Director possesses information demonstrating that the harm will materialize in a very short period if the information is disclosed. It also implies that the Director can reasonably estimate the period during which the harm will continue to have effect after the disclosure;

- The harm is significant: this means that the disclosure of the information will cause serious damage; not just administrative inconvenience. This implies that the harm is assessed using reasonable criteria. An example of an acceptable demonstration of harm would be where the disclosure of information would allow a violent individual to learn the identity of a third party who has reported his or her criminal activities to the police.

d) Exceptions not based on a harm test:

Those provisions provide that certain categories of information may or must be refused even in the absence of any clear and concrete evidence of harm. This is so because Council has determined that the disclosure of the information listed in the exception provision would

invariably cause harm to the specified interest. As a result, Directors of departments are relieved from the obligation to demonstrate such harm. Paragraph 22(a)(i), which seeks to protect trade secrets from disclosure, constitutes a good example of a provision that does not require the demonstration of any specific harm. As soon as it is confirmed that the information contained in the requested document constitutes a “trade secret”, it must be refused to the applicant.

Part Three – Exception Provisions

This Part contains the provisions that constitute the only grounds for a refusal of access to information under this Regulation, and the information that is described in each exception provision can only be protected from access if it meets the criteria established by that provision.

21. Protection of Privacy

a) The Director of a department must refuse to disclose personal information where the disclosure of such information would cause an unreasonable invasion of the privacy of a third party;

b) The disclosure of personal information is not an unreasonable invasion of a third party's personal privacy if:

i. the third party has, in writing, consented to or requested the disclosure and understands the implications of his or her consent (informed consent),

ii. there are compelling circumstances affecting anyone's health or safety and notice of the disclosure is mailed to the last known address of the third party,

iii. a enactment of the Mohawk Council of Akwesasne, Canada, Ontario or Quebec authorizes or requires the disclosure,

iv. the disclosure is for research purposes and the conditions set out in section 44 of this Regulation have been met,

v. the information is about the third party's classification, salary range, discretionary benefits or employment responsibilities as an officer, employee or member of a department, as a member of the staff of a member of Council or as a member of Council,

vi. the disclosure reveals financial and other business or legal details of a contract to supply goods or services to a department,

vii. the information is about a licence, permit or other similar discretionary benefit relating to:

a. a commercial or professional activity, that has been granted to the third party by a department, or

b. real property, including a development permit or building permit, that has been granted to the third party by a department, and the disclosure is limited to the name of the third party and the nature of the licence, permit or other similar discretionary benefit,

viii. the disclosure reveals details of a discretionary benefit of a financial nature granted to the third party by a department,

ix. the disclosure is in accordance with the traditional approach to delivering health care or other assistance services to a member of the community, and is limited to the information that is necessary for the provision of such services;

x. the personal information is about an individual who has been dead for 20 years or more, or

xi. subject to paragraph (c), the disclosure is not contrary to the public interest and reveals only the following personal information about a third party:

a. enrolment in a school of an educational body or in a program offered by a post-secondary educational body,

b. admission to a facility or institution of a health or long term care body as a current patient or resident, except where the disclosure would reveal the nature of the third party's treatment or jeopardize the safety of the third party or of another person,

c. attendance at or participation in a public event or activity related to a department, including a graduation ceremony, sporting event, cultural program or club, or field trip, or receipt of an honour or award granted by or through a department.

c) The disclosure of personal information under section b) (xi) <u>is</u> an unreasonable invasion of personal privacy if the third party to whom the information pertains has requested that the information not be disclosed;

d) A disclosure of personal information is presumed to be an unreasonable invasion of a third party's personal privacy if:

   i. the personal information relates to a medical, psychiatric or psychological history, diagnosis, condition, treatment or evaluation, other than in the context of section b) ix,

   ii. the personal information relates to the spiritual or ceremonial values or beliefs of an individual,

   iii. the personal information is an identifiable part of a law enforcement record, except to the extent that the disclosure is necessary to dispose of the law enforcement matter or to continue an investigation,

   iv. the personal information relates to eligibility for income assistance or social service benefits or to the determination of benefit levels,

   v. the personal information relates to employment or educational history,

   vi. the personal information was collected on a tax return or on other revenue collection form by the Mohawk Council of Akwesasne,

   vii. the personal information consists of personal recommendations or evaluations, character references or personnel evaluations,

   viii. the personal information consists of the third party's name:

      a. when it appears with other personal information about the third party,

      b. the disclosure of the name itself would reveal personal information about the third party, or

      c. the personal information indicates the third party's racial, cultural or ethnic origin or religious or political beliefs or associations.

e) In determining under subsections (a) and (d) whether a disclosure of personal information constitutes an unreasonable invasion of a third party's personal privacy, the Director of the department must consider all the relevant circumstances, including whether:

i. the disclosure is desirable for the purpose of subjecting the activities of the Mohawk Council of Akwesasne or a department to public scrutiny,

ii. the disclosure is likely to promote public health and safety or the protection of the environment,

iii. the personal information is relevant to a fair determination of the applicant's rights,

iv. the disclosure will assist in researching or validating the claims, disputes or grievances of the Mohawk people, the Mohawk Council of Akwesasne or those of another First Nation community,

v. the third party will be exposed unfairly to financial or other harm,

vi. the personal information has been supplied explicitly or implicitly in confidence,

vii. the personal information is likely to be inaccurate or unreliable,

viii. the disclosure may unfairly damage the reputation or livelihood of any person referred to in the record requested by the applicant, and

ix. the personal information was originally provided by the applicant.

22. Protection of Third Party Business Information

a) The Director of a department must refuse to disclose the following information:

   a) trade secrets of a third party;

   b) commercial, financial, technical and scientific information of a third party, where the third party:

      a. has requested the confidentiality of such information, and

      b. treats the information in a confidential manner;

   c) information that could affect contractual negotiations of a third party, including collective bargaining negotiations;

d) information the disclosure of which could reasonably be expected to:

i. harm significantly the competitive position or interfere significantly with the negotiating position of a third party

ii. result in similar information no longer being supplied to the department when it is in the public interest that similar information continue to be supplied,

iii. result in undue financial loss or gain to any person or organization,

iv. unfairly damage the reputation of a third party,

v. expose a third party to unfair financial or other harm; or

vi. reveal information supplied to, or the report of, an arbitrator, mediator, labour relations officer or other person or body appointed to resolve or inquire into a labour relations dispute.

b) The Director of a department <u>may</u> disclose business information of a third party where:

i. the disclosure is clearly in the public interest as it relates to the protection of human life, public safety, protection of the environment or the protection of the vital interests of the Mohawk people, the Mohawk Council of Akwesasne, another government within Akwesasne or another First nation community;

ii. The third party has been given advanced notice of the disclosure or, where the circumstances do not allow for the giving of an advanced notice to the third party, a notice is served immediately after the disclosure;

iii. the Director of the department has taken all reasonable precautions to eliminate or minimize the harm caused to the third party by the disclosure; or

iv. Council has approved the disclosure.

23. Protection of Information Obtained In Confidence From Another Government or an International Organization of States

a) The Director of a department must refuse to disclose information that has been obtained implicitly or explicitly in confidence from:

   i) a First Nation government, including another government within Akwesasne, or one of its bodies;

   ii) the federal government or one of its bodies;

   iii) a provincial or a territorial government or one of its bodies;

   iv) a municipal or regional government or one of its bodies;

   v) a local government or one of its bodies;

   vi) a foreign government or one of its bodies;

   vii) an international organization of states or one of its bodies;

b) The Director of the department may disclose the information described in section a) if:

   i) the other government consents in writing to the disclosure or has made the information available to the public in the same context as the one in which it was provided to, or it is kept by the Mohawk Council of Akwesasne; and

   ii) Council has approved the disclosure.

24. Protection of Information That Could Have an Adverse Effect on the Mohawk People, the Mohawk Council of Akwesasne, Another Government Within Akwesasne or Another First Nation

a) The Director of a department may refuse to disclose information where the disclosure would affect the ability of Council to promote, represent or defend the interests of the Mohawk people, the Mohawk Council of Akwesasne, another government within Akwesasne or another First Nation community, including (but not limited to) the following information:

i. information the disclosure of which could affect the ability of Council, another government within Akwesasne or another First Nation to negotiate contractual agreements with any other party;

ii. information the disclosure of which could affect the ability of Council, another government within Akwesasne or another First Nation to research or validate a claim, dispute or a grievance;

b) In determining whether a disclosure of information would cause the harm described in section a), the Director of the department must seek an appropriate balance between the prevention of the harm and the principle of government accountability and transparency.

c) The Director of a department must refuse to disclose the following information:

i. information the disclosure of which could harm relations between the Mohawk Council of Akwesasne and another government within Akwesasne or another government, except where Council has approved the disclosure;

ii. information the disclosure of which could harm relations between the Mohawk Council of Akwesasne and an international organization of states, except where Council has approved the disclosure;

iii. information that could affect treaty rights of the Mohawk people, the Mohawk Council of Akwesasne, those of another government within Akwesasne or those of another First Nation community, except where Council has approved the disclosure.

25. Deliberations of Council

a) The Director of a department must refuse to disclose information that would reveal the substance of non-public deliberations of Council or any of its committees, including any advice, recommendations, policy considerations or draft regulations or policies submitted or prepared for submission to Council or any of its committees;

b) Subsection a) does not apply to:

i. information in a record that has been in existence for 15 years or more,

ii. information in a record of a decision made by Council or any of its committees on an appeal under an enactment of the Mohawk Council of Akwesasne, or

iii. information in a record the purpose of which is to present background facts to Council or any of its committees in making a decision if:

a. the decision has been made public,

b. the decision has been implemented, or

c. 5 years or more have passed since the decision was made or considered.

26. Advice From Officials

a) Subject to section b), the Director of a department may refuse to disclose information if the disclosure could reasonably be expected to reveal:

i. advice, proposals, recommendations, analyses or policy options developed by or for Council or for a department,

ii. consultations or deliberations involving officers or employees of a department, a board, a commission, a member of Council, or the staff of a Council member,

iii. positions, plans, procedures, criteria or instructions developed for the purpose of contractual or other negotiations by or on behalf of Council or a department, or considerations that relate to those negotiations,

iv. plans relating to the management of personnel or the administration of a department that have not yet been implemented,

v. the contents of draft policies and orders of Council members or the Grand Chief, or

vi. the content of agendas or minutes of meetings of a department.

b) Subsection a) does not apply to information that:

i. has been in existence for 15 years or more,

ii. is a statistical survey,

iii. is a statement of the reasons for a decision that is made in the exercise of a discretionary power or an adjudicative function, or

iv. is the result of product or environmental testing carried out by or for a department, that is complete or on which no progress has been made for at least 3 years, unless the testing was done:

a. for a fee as a service to a person other than a department, or

b. for the purpose of developing methods of testing or testing products for possible purchase,

27. Disclosure Harmful to Economic and Other Interests of a Department

a) The Director of a department may refuse to disclose information if the disclosure could reasonably be expected to harm the economic interests of a department or the ability of Council to manage the affairs of the community, including the following information:

i. trade secrets of a department;

ii. financial, commercial, scientific, technical or other information in which a department has a proprietary interest or a right of use and that has, or is reasonably likely to have, monetary value;

iii. information the disclosure of which could reasonably be expected to

a. result in financial loss to, or

b. prejudice the competitive position of, or

c. interfere with contractual or other negotiations of Council or of a department;

iv. the results of product or environmental testing carried out by or for a department where the disclosure could reasonably be expected to affect the interests of the Mohawk Council of Akwesasne or the members of the Mohawk community.

b) The Director of a department may refuse to disclose information obtained through research by an employee of a department, the disclosure of which could reasonably be expected to deprive that employee or the department of their priority of publication;

c) The Director of the department must not refuse to disclose under sections a) and b) the results of product or environmental testing carried out by or for a department, unless the testing was done:

i. for a fee as a service to a person, other than the department, or

ii. for the purpose of developing methods of testing or testing products for possible purchase,

unless the disclosure could reasonably be expected to affect the interests of the Mohawk Council of Akwesasne or the members of the Mohawk community.

28. Protection of Information That Could Have a Detrimental Effect On the Cultural Heritage of the Mohawk People, the Mohawk Council of Akwesasne, Another Government Within Akwesasne Or On Another First Nation Community

a) The Director of a department may refuse to disclose information where the disclosure would be detrimental to the cultural heritage of the Mohawk people, the Mohawk Council of Akwesasne, another government within Akwesasne or another First Nation community.

b) Paragraph b) must not be used to prevent the promotion and the transmission of the cultural values of the Mohawk people.

29. Protection of Information That Could Have an Adverse Effect on The Natural Environment Or Be Detrimental to a Vulnerable Species

The Director of a department may refuse to disclose information where the disclosure would result in damage to, or interfere with the protection or the conservation of:

a) the natural environment of the Mohawk Council of Akwesasne territory or in which the Mohawk Council of Akwesasne has an interest; or

b) any rare, endangered, threatened or vulnerable form of life.

30. Protection of Solicitor-Client and Other Privileged Information

a) The Director of a department may refuse to disclose:

i. information that is subject to any type of legal privilege, including solicitor-client privilege or parliamentary privilege,

ii. information prepared for the purpose of a criminal prosecution, litigation or other court action,

iii. information exchanged with an agent or lawyer of a department, in relation to a matter involving the provision of legal services, or

iv. information in correspondence between a department and the judicial authorities of another government.

b) The Director of the department must refuse to disclose information described in subsection section a) that relates to a person other than a department.

31. Protection of Information That Could Have An Adverse Effect On Audit Activities

The Director of a department may refuse to disclose information relating to:

a) testing or auditing procedures or techniques,

b) details of specific tests to be given or audits to be conducted, or

c) standardized tests used by a public body, including intelligence tests, if disclosure could reasonably be expected to prejudice the use or results of particular tests or audits.

32. Protection of Information That Could Have An Adverse Effect on Law Enforcement Activities

a) The Director of a department may refuse to disclose information if the disclosure could reasonably be expected to:

i. harm a law enforcement matter,

ii. weaken the protection of the members of the Mohawk Council of Akwesasne community against crime,

iii. prejudice the defence of Canada or of any foreign state allied to or associated with Canada or harm the detection, prevention or suppression of espionage, sabotage or terrorism,

iv. harm the effectiveness of investigative techniques and procedures currently used, or likely to be used, in law enforcement,

v. reveal the identity of a confidential source of law enforcement information,

vi. reveal criminal intelligence that has a reasonable connection with the detection, prevention or suppression of organized criminal activities or of serious and repetitive criminal activities,

vii. interfere with or harm an ongoing or unsolved law enforcement investigation, including a police investigation,

viii. reveal any information relating to or used in the exercise of prosecutorial discretion, except if the information has been in existence for 10 years or more,

ix. deprive a person of the right to a fair trial or impartial adjudication,

x. reveal a record that has been confiscated from a person by a peace officer in accordance with a law,

xi. facilitate the escape from custody of an individual who is being lawfully detained,

xii. facilitate the commission of an unlawful act or hamper the control of crime,

xiii. reveal technical information relating to weapons or potential weapons,

xiv. harm the security of any property or system, including a building, a vehicle, a computer system or a communications system,

xv. reveal information in a correctional record supplied, explicitly or implicitly, in confidence,

b) The Director of a department may refuse to disclose information that:

i. is in a law enforcement record and the disclosure of which could reasonably be expected to expose to civil liability the author of the record or an individual who has been quoted or paraphrased in the record, or

ii. is about the history, supervision or release of an individual who is under the control or supervision of a correctional authority, and the disclosure could reasonably be expected to harm the proper custody or supervision of that person.

c) The Director of a department must refuse to disclose information if the information is in a law enforcement record and the disclosure would be an offence under an enactment of the Mohawk Council of Akwesasne, Canada, Quebec or Ontario.

d) Subsections a), b) and c) do not apply to:

i. a report prepared in the course of routine inspections by a department that is authorized to enforce compliance under an enactment of the Mohawk Council of Akwesasne, or

ii. a report, including statistical analysis, on the degree of success achieved in a law enforcement program unless disclosure of the report could reasonably be expected to interfere with or harm any of the matters referred to in section a), b) or c).

e) After a police investigation is completed, the Director of a department may disclose under this subsection the reasons for a decision not to prosecute:

   i. to a person who knew of and was significantly interested in the investigation, including a victim or a relative or friend of a victim, or

   ii. to any other member of the public, if the fact of the investigation was made public.

33. Protection of Information That Could Be Harmful to Individual or Public Safety

a) The Director of a department may refuse to disclose information, including personal information about the applicant, if the disclosure could reasonably be expected to:

   i. threaten anyone else's safety or mental or physical health, or

   ii. interfere with public safety.

b) The Director of a department may refuse to disclose to an applicant personal information about the applicant if the disclosure could, in the opinion of a physician, a chartered psychologist or a psychiatrist or any other appropriate expert depending on the circumstances of the case, reasonably be expected to result in immediate and grave harm to the applicant's health or safety;

c) The Director of a department may refuse to disclose to an applicant information in a record that reveals the identity of an individual who has provided information to the department in confidence about a threat to an individual's safety or mental or physical health.

34. Protection of Evaluative Information Obtained Under Certain Circumstances

a) The Director of a department may refuse to disclose personal information that is evaluative or opinion material compiled for the purpose of determining the applicant's suitability, eligibility or qualifications for employment or for the awarding of contracts or other

benefits by a department when the information has been provided, explicitly or implicitly, in confidence;

b) The Director of a department may refuse to disclose personal information that identifies or could reasonably identify a participant in a formal employee evaluation process concerning the applicant when the information has been provided, explicitly or implicitly, in confidence;

c) For the purpose of section b), "participant" includes a peer, subordinate or client of an applicant, but does not include the applicant's supervisor or superior;

d) In deciding to disclose or not evaluative or opinion material about an individual to that individual, the Director of the department must consider the rules and principles of natural justice.

35. Protection of Information That Will Be Published Within One Hundred and Twenty Days

a) The Director of a department may refuse to disclose information:

   i. that is available for purchase by the public, or

   ii. that is to be published or released to the public within 120 days from the date of receipt of the applicant's request.

b) The Director of a department may notify an applicant of the publication or release of information that the Director has refused to disclose under paragraph a) ii.

c) If the information is not published or released within 120 days after the applicant's request is received, The Director of the department must reconsider the request as if it were a new request received on the last day of that period, and access to the information requested must not be refused under section a) ii.

Chapter Three

Protection of Personal Privacy

36. Authority for the Collection of Personal Information

No personal information may be collected by or for a department unless:

a) the collection of that information is expressly authorized by a enactment of the Mohawk Council of Akwesasne or an enactment of Canada, Ontario or Quebec,

b) the information is collected for the purposes of law enforcement, or

c) the information relates directly to and is necessary for an operating program or activity of the department.

37. How Personal Information May Be Collected

a) A department must collect personal information directly from the individual to whom the information pertains unless:

i. another method of collection is authorized by:

a. that individual,

b. an enactment of the Mohawk Council of Akwesasne, or

c. the Mohawk Court, a federal Court or a Court established by the government of Ontario or the government of Quebec.

ii. the information may be disclosed to the department under section 41, 43 or 44 of this Regulation,

iii. the information is collected in a health or safety emergency where:

a. the individual is not able to provide the information directly, or

b. direct collection could reasonably be expected to endanger the mental or physical health or safety of the individual or another person,

iv. the information concerns an individual who is designated as a person to be contacted in an emergency or under other specified circumstances,

v. the information is collected for the purpose of determining suitability of the individual for an honour or award, including an honorary degree, scholarship, prize or bursary,

vi. the information is collected from published or other public sources for the purpose of fund-raising,

vii. the information is collected for the purpose of law enforcement,

viii. the information is collected for the purpose of collecting a fine or a debt owed to the Mohawk Council of Akwesasne,

ix. the information concerns the history, release or supervision of an individual under the control or supervision of a correctional authority,

x. the information is collected for use in the provision of legal services to the Mohawk Council of Akwesasne,

xi. the information is necessary:

    a. to determine the eligibility of an individual to participate in a program of or receive a benefit, product or service from the Mohawk Council of Akwesasne, and is collected in the course of processing an application made by or on behalf of the individual to whom the information pertains, or

    b. to verify the eligibility of an individual who is participating in a program of or receiving a benefit, product or service from the Mohawk Council of Akwesasne and is collected for that purpose,

xii. the information is collected for the purpose of informing a provincial public trustee or public guardian of Ontario or Quebec or the Department of Health, the Department of Community and Social Services or the Department of Justice of the Mohawk Council of Akwesasne about clients or potential clients,

xiii. the information is collected for the purpose of enforcing a maintenance order under a maintenance enforcement enactment of Canada, Ontario or Quebec,

xiv. the information is collected for the purpose of managing or administering personnel of a department, or

xv. the information is collected for the purpose of assisting in researching or validating the claims, disputes or grievances of the of the Mohawk people, the Mohawk Council of Akwesasne, another government within Akwesasne or another First Nation community.

b) Where a department collects personal information from the individual to whom the information pertains, it must inform that individual of:

i. the purpose for which the information is collected,

ii. the specific policy authority for the collection, and

iii. the title, business address and business telephone number of an officer or employee of the department who can answer the individual's questions about the collection.

c) Paragraphs a) and b) do not apply if, in the opinion of the Director of the department concerned:

i. the information collected in compliance with those provisions will likely be inaccurate, or

ii. compliance with those provisions will likely defeat the purpose of the collection.

38. Accuracy and Retention of Personal Information

a) A department must make every reasonable effort to ensure that any personal information that is used to make a decision about an individual is as accurate, complete and up-to-date as possible.

b) A department must retain the personal information for at least one year after using it so that the individual has a reasonable

opportunity to obtain access to it, unless one of the following conditions applies:

i. the individual has consented in writing to the shorter retention period;

ii. the Director of the department has agreed to the shorter retention period; and

iii. The final disposition of the information is in accordance with an enactment of the Mohawk Council of Akwesasne, Canada, Quebec or Ontario or has been ordered by a court that has jurisdiction to make such an order.

c) The retention period referred to in section b) applies regardless of the retention period specified in the Mohawk Council of Akwesasne's Retention and Disposal Schedule.

39. Right to Request the Correction of Personal Information

a) An applicant who believes there is an error or omission in his or her personal information may request the Director of the department that has the information in its custody or under its control to correct the information;

b) Despite section a), the Director of a department must not correct an opinion, including a professional or expert opinion;

c) Where the Director of a department refuses to make the requested correction, he or she must annotate all the copies of the information that is the subject of the request for correction;

d) The Director must notify any other department or any third party to whom that information has been disclosed during the one year before the correction was requested that a correction, annotation or linkage has been made;

e) Despite section d), the Director of the department may dispense with notifying any other department or third party that a correction, annotation or linkage has been made if:

i. in the opinion of the Director of the department, the correction, annotation or linkage is not material, and

ii. the individual who requested the correction is advised and agrees in writing that notification is not necessary.

f) On being notified under section d) of a correction, annotation or linkage of personal information, the Director of the department must make the correction, annotation or linkage on any record of that information in its custody or under its control.

g) The Director of the department who has received a request for the correction of personal information must inform the applicant in writing within 30 days that the correction has been made or that an annotation or linkage has been made. The 30-time frame may be extended in accordance with the requirements of section 16 of this Regulation.

40. Transferring Request to Correct Personal Information

a) Within 15 days after a request for the correction of personal information has been received under section 38, the Director of the department may transfer the request to another department if:

i. the personal information was collected by the other department, or

ii. the other department created the record containing the personal information.

b) Where a request for correction is transferred under section a):

i. the Director of the department who transferred the request must notify the applicant of the transfer as soon as possible, and

ii. the Director of the department to which the request is transferred must make every reasonable effort to respond to the request not later than 30 days after receiving the request unless the time limit is extended in accordance with section 16 of this Regulation.

41. Use Of Personal Information

a) A department may use personal information only:

   i. for the purpose for which the information was collected or compiled or for a use consistent with that purpose,

   ii. if the individual to whom the information pertains has identified the information and consented, in the prescribed manner, to the use, or

   iii. for a purpose for which that information may be disclosed to that department under sections 41, 43 or 44.

b) A department may use personal information only to the extent necessary to enable it to carry out its purpose in a reasonable manner.

42. Disclosure Of Personal Information

a) A department may disclose personal information only:

   i. in accordance with Chapter Two of this Regulation,

   ii. if the disclosure would not be an unreasonable invasion of a third party's personal privacy under section 20 of this Regulation,

   iii. for the purpose for which the information was collected or compiled or for a use consistent with that purpose,

   iv. if the individual to whom the information pertains:

      a. has identified the information,

      b. has consented in writing to its disclosure, and

      c. understands the implications of his or her consent (informed consent).

   v. for the purpose of complying with an enactment of the Mohawk Council of Akwesasne;

vi. for the purpose of complying with an enactment of Canada, Ontario or Quebec or with a treaty, arrangement or agreement signed with another government,

iv. for the purpose of complying with a subpoena, warrant or order issued or made by a court, person or body having jurisdiction to compel the production of information or with a rule of court that relates to the production of information,

v. to an officer or employee of the department or to a Council member, if the information is necessary for the performance of the duties of the officer, employee or member,

vi. to an officer or employee of a department or to a Council member, if the disclosure is necessary for the delivery of a common or integrated programs or services and for the performance of the duties of the officer or employee or member to whom the information is disclosed,

vii. for the purpose of enforcing a legal right that the Mohawk Council of Akwesasne has against any person,

viii. for the purpose of:

a. collecting a fine or debt owing by an individual to the Mohawk Council of Akwesasne or to a department, or to an assignee of either of them, or

b. making a payment owing by the Mohawk Council of Akwesasne or by a department to an individual,

ix. for the purpose of determining or verifying an individual's suitability or eligibility for a program or benefit,

x. to an internal or an external auditor whose services have been retained by the Mohawk Council of Akwesasne or by a department for audit purposes,

xi. to a Council member who can prove that he or she has been requested by the individual to whom the information pertains to assist in resolving a problem,

xii. to a representative of a bargaining agent who has been authorized in writing by the employee to whom the information pertains to make an inquiry,

xiii. to the Archives Services of the Mohawk Council of Akwesasne or to the archives of a department for permanent preservation,

xiv. to a department or a law enforcement agency in Canada:

a. to assist in an investigation undertaken with a view to a law enforcement proceeding, or

b. from which a law enforcement proceeding is likely to result,

if the disclosure is in accordance with a legislative authority, a Regulation of Council or with an arrangement, written agreement or treaty approved by Council.

xv. if the department is a law enforcement agency and the information is disclosed to another law enforcement agency in Canada, or to a law enforcement agency in a foreign country under an arrangement, written agreement, treaty or legislative authority,

xvi. so that the spouse, relative or friend of an injured, ill or deceased individual may be contacted,

xvii. in accordance with sections 43 or 44,

xviii. to an expert for the purposes of section 33 (b),

xix. for use in a proceeding before a court or quasi-judicial body to which the Mohawk Council of Akwesasne or a department is a party,

xx. when disclosure is by the Director of the Department of Justice or an agent or lawyer of the Department of Justice to a place of lawful detention,

xxi. for the purpose of supervising an individual under the control or supervision of a correctional authority,

xxii. for the purpose of managing or administering personnel of the Mohawk Council of Akwesasne or a department,

xxiii. to the Director of a Maintenance Enforcement authority of Canada, Ontario or Quebec for the purpose of enforcing a maintenance order under the applicable Maintenance Enforcement legislation,

xxiv. when the information is available to the public in the same context in which it is kept by the department,

xxv. to a relative of a deceased individual if, in the opinion of the Director of the department, the disclosure is not an unreasonable invasion of the deceased's personal privacy,

xxvi. to a lawyer or student-at-law acting for an inmate under the control or supervision of a correctional authority, or

xxvii. if the Director of the department believes, on reasonable grounds, that the disclosure will avert or minimize an imminent danger to the health or safety of any person.

b) A department may disclose personal information under section a) only to the extent necessary to enable it to carry out its purpose in a reasonable manner.

43. Consistent Purposes

For the purposes of sections 41 a) i and 42 a) vi, a use or disclosure of personal information is consistent with the purpose for which the information was collected or compiled if the use or disclosure:

i. has a reasonable and direct connection to that purpose, and

ii. is necessary for performing the statutory duties of, or for operating a legally authorized program of, the department that uses or discloses the information.

44. Disclosure For Research Or Statistical Purposes

A department may disclose personal information for a research purpose, including statistical research, only if:

a) the research purpose cannot reasonably be accomplished unless that information is provided in individually identifiable form or the research purpose has been approved by a Court,

b) any record linkage is not harmful to the individuals the information is about and the benefits to be derived from the record linkage are clearly in the public interest,

c) the Director of the department has approved conditions relating to the following:

   i. security and confidentiality,

   ii. the removal or destruction of individual identifiers at the earliest reasonable time, and

   iii. the prohibition of any subsequent use or disclosure of the information in individually identifiable form without the express authorization of that department,

d) the person to whom the information is disclosed has signed an agreement to comply with the approved conditions, with this Regulation and with any other departmental policies and procedures relating to the confidentiality of personal information.

e) the Director of a department may enter into an agreement with a student or a researcher whereby information will be provided to the student or the researcher in return for a fee, information or other form of compensation.

45. Disclosure of Information In Archives

The Archives Division of the Mohawk Council of Akwesasne or the archives of a department may disclose for research purposes personal information that:

a) has been in existence for 25 years or more if the disclosure would not be an unreasonable invasion of personal privacy under section 21 of this Regulation,

b) is in accordance with section 44, or

c) is contained in a record that has been in existence for 75 years or more.

Chapter Four

Requirements for the Protection of Sensitive Information

46. Principles of Risk Management and Threat and Risk Assessments

a) The Mohawk Council of Akwesasne recognizes that information constitutes a critical component of the administration of the affairs of the community, including the delivery of programs and services to its members. As a result, information must be protected in accordance with the following four principles:

   i. the importance of the resources invested in the protection of information must reflect its value and sensitivity;

   ii. the threats and risks that may affect the information of the Mohawk Council of Akwesasne must be properly assessed through the conduct of a threat and risk assessment;

   iii. a wise risk management approach must be used in order to minimize the negative impact that the security measures may have on the activities of the Mohawk Council of Akwesasne and those of departments;

   iv. the security measures must contribute to the achievement of the objectives of the Mohawk Council of Akwesasne and its programs by providing a safe environment for all its contributors, as well as for the general public.

47. Conducting Threat and Risk Assessments (TRA)

a) The Directors of each department must analyze and assess the threats and risks to which sensitive information and assets are exposed, select risk-avoidance options and implement cost-effective safeguards. A TRA consists in reviewing the characteristics of a work environment in order to:

   i. identify the threats that could affect the information and the assets that are used to manage it;

   ii. evaluate the chances of these threats to materialize; and

   iii. evaluate the adequacy of the security measures that are already in place.

b) TRAs should be conducted regularly in every facility of the Mohawk Council of Akwesasne and, more specifically:

   i. every time a change is made in the operation, procedures or systems of a work environment;

   ii. at the time of a relocation or reorganization;

c) A TRA usually is usually comprised of the six following steps:

   i. determination of the scope of the TRA and preparation of the plan;

   ii. inventory of the information and assets that require protection;

   iii. identification of the threats (i.e. what could happen to the information and assets? Theft? Destruction?, etc.);

   iv. evaluation of the risks (i.e. the likelihood of the threats to materialize);

   v. evaluation of the adequacy of the security measures currently in place;

   vi. recommendations on how to correct the deficiencies identified during the review.

48. Identification of Assets and Information to Be Safeguarded

a) The Director of each department must identify all information and assets the compromise of which could reasonably be expected to cause injury to the Mohawk Council of Akwesasne or to any public or private interests.

b) Assets and information must be classified according to their level of sensitivity. The Director of each department must also categorize information and assets based on the degree of injury that could reasonably be expected to result from the loss of their confidentiality, availability, integrity or value, as defined in the following paragraphs:

i. confidentiality is the sensitivity of information or assets to unauthorized disclosure. The best way to preserve confidentiality is to limit access to the smallest number of individuals possible,

ii. availability is the condition of being usable on demand to support business functions,

iii. integrity refers to the accuracy and completeness of information and assets and the authenticity of transactions. More specifically, integrity refers to the level of certainty that the assets and information of a department have not been modified or altered in any way, shape or form,

iv. value refers to the financial and strategic importance of the asset or information for the Mohawk Council of Akwesasne. The financial value is usually established by calculating how much it would cost to replace the lost information or the asset, whereas the strategic value refers to the gravity of the consequences that would result from the temporary or permanent loss of the asset or information.

49. Identifying, Marking and Protecting Sensitive Information

a) The Director of a department must ensure that access to sensitive information is limited to those individuals who:

i. can demonstrate a legitimate need to know in relation to their duties; *and*

ii. have been authorized to have access to it.

b) The Director of a department must regularly review the information holdings of the department to determine the sensitivity of that information, in accordance with the following classification:

Security Classification	Description of Information and Examples
Public information:	Includes information that is routinely made accessible to the public because no adverse consequences would likely result from its wide dissemination. It includes information that is posted on the Internet web site of the Mohawk Council of Akwesasne, information that is published and information that is held in certain publicly accessible databases. Information that is available to the public does not require protection from a confidentiality point of view, however, security measures that seek to protect its integrity, accuracy and availability must be implemented where warranted. Such measures may include physical access controls and electronic mechanisms to prevent its modification (i.e., read-only access privileges).
Restricted information:	This category represents the bulk of the information held by the Mohawk Council of Akwesasne. It is assigned to information which, if disclosed or otherwise compromised, could affect any of the interests that are listed in the exception provisions contained in Chapter Two of this Regulation. Security measures aimed at preventing unauthorized access, use, modification or destruction of such information must be implemented, based on the results of a TRA.
Extremely sensitive information:	The compromise of this category of information could reasonably be expected to cause serious or even exceptionally grave harm to one of the interests listed in the exception provisions contained in Chapter Two of this Regulation. Examples of such harm include the loss of life of an individual, the extinction of a vulnerable form of life, an extremely grave injury to a privately owned company or to a large segment of society, to another government or to the Mohawk Council of Akwesasne. Extraordinary security measures are required, based on the results of a TRA or in accordance with the law or with a security protocol signed by the Mohawk Council of Akwesasne.
Important Notes:	
1	The above classifications are baseline requirements, which means that they constitute minimum safeguards. The specific classification of information for each

	physical and electronic record must be based on the nature of the information, the context in which the information or the record exists and the gravity of the harm that may result from its compromise. A TRA is required to determine if and what safeguards are needed, and these safeguards must be implemented if it is cost-effective to do so.
2	The classification of information for security purposes is not a factor in the decision to disclose a record or information under the exception provisions contained in Chapter Two of this Regulation. The exception provisions constitute the only authority for the decision to disclose information or not in response to an access request received under this Regulation.

50. Information Technology Security (ITS)

a) The Director of a department must ensure the adequate protection of the electronic information under his or her control by establishing appropriate requirements and procedures;

b) The Director of a department must ensure that ITS forms an integral part of each stage in the system development cycle, in order to ensure:

   i. the application of baseline security controls,

   ii. the continuous monitoring of service delivery levels,

   iii. that threats and identified / detected and controlled or eliminated;

   iv. the establishment of effective incident response and IT continuity mechanisms.

c) Computer Services is responsible for the development and the implementation of policies and procedures for the purchasing, installation, use, maintenance, modification and protection of hardware equipment and software for the Mohawk Council of Akwesasne;

d) In implementing security measures, the Director of a department must comply with all the policies and procedures developed by Computer Services as they relate to the purchasing, installation, use, maintenance, modification and protection of hardware equipment;

e) In implementing security measures, the Director of a department must comply with all the policies and procedures developed by Computer Services as they relate to purchasing, downloading, installation, use, maintenance, modification and protection of software;

f) Employees of the Mohawk Council of Akwesasne must use departmental equipment only for approved activities related to the department's business, except where otherwise authorized by someone with the delegated authority to approve another use;

g) Information that is created for public dissemination must be kept in directories different from those containing sensitive information, so as to facilitate the identification of the two categories of information. The directories that contain sensitive information must be clearly identified;

h) Nobody, regardless of their rank, level or status, is granted permanent or even temporary access rights to the information or the computer systems of a department. Access privileges are instead conferred upon individuals so that they can have access to the information that they require in order to perform their duties;

i) The custodians of electronic information are responsible for its proper safeguarding during all phases of its existence. As a result, they must ensure that the equipment that they intend to use for its collection, manipulation, sharing, transmission, storage and disposition meet the requirements established by the Director of the department and by Computer Services;

j) Directors of departments must sign a protocol before they approve any electronic information sharing activity. The protocol must comply with the policies established by Computer Services. Protocols must also specify the requirements pertaining to at least the following aspects:

    i. who has the authority for making decisions regarding the security and privacy standards that will apply to the shared system or activity;

    ii. the development and maintenance of the security features of the system;

    iii. security monitoring and reporting;

    iv. investigation of security breaches and violations.

51. Physical Access Controls

a) The Director of a department must implement physical security measures to protect the sensitive information and assets of the department. These measures must be:

   i. effective, which implies that they are regularly tested and the deficiencies discovered during the testing are corrected as soon as possible,

   ii. cost-efficient, both in terms of efforts and financial implications,

   iii. adapted to the operational context of the department to ensure that they interfere as little as possible with the smooth running of departmental operations.

b) Physical security measures for facilities and systems must be designed in accordance with the principles of zone delimitation and protection, detection, response and recovery, as described in the following paragraphs:

   i. the zone concept consists in dividing a building or other physical area or container into segments of progressive security levels that restrict access to only those individuals who have been authorized to enter those areas. Based on the type of information and assets that are kept in them, buildings can be divided into up to five zones, each presenting the following characteristics:

      a. public zone: This is the external zone of the area or facility, and is the public area immediately surrounding the facility (sidewalk, street, front lawn of the building, parking area and vehicles in it, etc.). The public zone presents the lowest level of security, and signs or video surveillance often may be used to discourage unauthorized activity,

      b. reception zone: This is usually the first point of contact between the visiting public and the employees of the organization. In this zone, services are provided to the public, information of a non-sensitive nature is exchanged, and access to restricted zones is controlled, either by personnel or security staff,

c. operations zone: Access to this zone is restricted to authorized personnel and to visitors who are escorted by a manager or employee of the Director of a department. Information of an extremely sensitive nature cannot be stored in this zone, but may be brought in for processing if measures commensurate to the level of sensitivity of the information are taken to ensure adequate protection,

d. security zone: this zone must be accessible only to employees who are authorized access and to visitors who are properly escorted. Security zones are monitored 24 hours a day, 7 days a week, by security staff, personnel or electronic means. The security zone can store extremely sensitive information and is the only zone authorized to process it on a regular basis,

e. high security zone: this zone may take the form of reinforced room with exceptional security features, such as a safe or vault. High security zones are usually only established where warranted by a TRA and with the prior approval of the Director of a department. This zone is normally used to store and process extremely sensitive information. High security zones are monitored 24 hours a day, 7 days a week, by security staff, personnel, or electronic means.

ii. protection is the use of physical, procedural and psychological barriers to delay or deter unauthorized access. Locks and doors are good examples of protection mechanisms. Protective measures are evaluated against the time that it takes to gain unauthorized access to a facility, area, system, etc.,

iii. detection involves the use of appropriate devices and methods to signal an attempted or actual unauthorized access. Alarm systems and CCTVs are examples of detection devices. Detection measures are evaluated against the time between the alarm signal and the probable target compromise,

iv. response is the reaction by personnel, the involvement of a guard or the police when an intrusion is detected. Response measures are evaluated based on the time required to mobilize the response force, cover the distance between their initial location at the time when they become aware of the intrusion and the facility, and to access the compromised area, and

v. recovery is the ability of the department to return to normal operations after an incident. Recovery measures are evaluated based on the time required to re-establish the operation of the department after an interruption.

52. Contracting and Security

a) The Mohawk Council of Akwesasne owns all records and information that are created, generated or obtained by contractors in the course of the performance of contracts or other duties for a department. As a result, contractors must adhere to all the requirements of this Regulation when performing activities for the Mohawk Council of Akwesasne or for a department or on their behalf;

b) Directors of departments must specify the following requirements in every contract that they enter into with an outside party:

i. the information generated or obtained by contractors in the course of the performance of the contract or other duties for the department is the sole and exclusive property of the Mohawk Council of Akwesasne,

ii. the contractor shall abide by this and all other regulations and policies of the Mohawk Council of Akwesasne as they relate to the collection, creation, use, disclosure, sharing, storage, protection and disposition of information and records,

iii. the contractor shall implement all the security measures requested by the departmental contracting authority with no additional financial compensation being paid to the contractor by the Mohawk Council of Akwesasne or one of its departments for the implementation of such measures,

iv. the contracting authority for the department reserves the right to inspect all physical areas, electronic systems and other devices that will be used by the contractor to store, transmit and manipulate information pertaining to the contract for a period of up to 2 years after the termination of the contract in order to verify that the information of the Mohawk Council of Akwesasne is handled and protected in accordance with the terms of the contract.

53. Personnel Screening and Background Verifications

a) In accordance with the Mohawk Council of Akwesasne's General Personnel Policy, the Director of a department must ensure that all individuals under his or her employ who have access to sensitive information and assets are reliable and trustworthy. The Director must specify the security requirements for the position or for the contract prior to the commencement of the hiring or contracting process;

b) The Director of a department must:

   i. ensure that the individual's consent is obtained before any check is initiated,

   ii. treat all individuals in a fair and unbiased manner and give them an opportunity to explain adverse information before a decision is reached,

   iii. where an adverse decision is made, advise the individual of his or her right to seek a review of the case before the Mohawk Court;

   iv. ensure that managers remain vigilant once an employee or a contractor has been hired and that they act on any new information that could put into question an individual's reliability or loyalty, and

   v. where required, recommend that administrative action be taken in relation to an employee or a contractor whose reliability or trustworthiness has been jeopardized.

54. Protecting Sensitive Information and Information Systems During Emergencies

a) The Director of a department is responsible for developing plans and procedures to increase security in the event of emergencies situations and increased threat situations;

b) The Director of a department must coordinate his or her plans for emergency recovery with other departmental prevention and response plans, including, fire, power failures, evacuations, bomb threats, etc.;

c) The Director of a department must coordinate his or her departmental plans for emergency recovery with those of other departments;

d) The objectives of emergency response plans must be developed in accordance with the following order of priorities:

i. to protect life: protecting individual safety must take precedence over all other considerations, and managers and employees must assess the risk to themselves and to others before attempting to protect the information and assets of the department. All employees, contractors, and other individuals who are present in a department's facility or vehicle must strictly obey the orders and instructions that they receive from the responsible emergency authorities,

ii. to protect the sensitive information and assets that are present in the department's facilities, vehicles and systems by preventing the source of the threat to come into contact with them: in most situations, protecting the physical assets and information of a department consists in physically or electronically blocking access to them or removing them from the facility. In extremely rare circumstances, the destruction of highly sensitive information can be the only way to protect it from unauthorized access during an emergency situation. Destroying information that is critical to departmental operations must only occur where no other viable alternatives exist, and a complete and detailed report of the incident must be presented to Council as soon as possible after the emergency,

iii. to minimize the harm resulting from the situation: where it is not possible to shield the asset or information of the department from the source of the threat, action must be taken to restore its original state of confidentiality, integrity, availability or value as soon as possible after the emergency situation. This can be done by recreating the information or by recovering the information or asset from the party who took it during the emergency situation. Where information has been compromised, the custodian must, as soon as possible after the emergency, prepare a written report detailing the circumstances and the nature of the compromise and what was done to minimize the adverse consequences,

iv. to resume the operations of the department as soon as possible after the emergency situation: in most cases, emergency situations cause an interruption in operations, which may in turn affect the delivery of services to the members of the community. The objective is to restore the delivery of the department's services and operations as soon as possible after the emergency situation is over so as to minimize the adverse consequences for the members of the community and for the department's employees. The order of priority in the restoration of a department's services is as follows:

a. Information, equipment and services that are critical to the delivery of services by the department: this includes information about the location and capabilities of emergency units and equipment; information and communication systems; and other critical equipment. It also includes information, equipment and services, the loss of which may jeopardize the department's ability to provide a safe and secure environment for its clients, managers, employees, contractors and other individuals whose presence is required in the department facilities,

b. information, equipment and services that are important, but not critical, for people: the computer systems used to manage and operate various programs of the department that are of less importance in emergency situations (i.e. general inquiries, complaints, etc.).

c. information, equipment and services that are important, but not critical, for the internal management of the department: these include human resources services and other internal services that have no direct and immediate impact on the community and the majority of employees (i.e. staff relations, collective bargaining process, non-urgent maintenance works and renovations, etc.).

55. Security Violations and Security Breaches

a) Without limiting the scope of the responsibilities outlined earlier in this Regulation, employees and contractors must immediately report to their superior or contracting agent, any security violation or breach that they become aware of. They may also be requested to assist in the investigation of the violation or breach;

b) The Director of a department is responsible for developing procedures for reporting and investigating security incidents and taking corrective action;

c) The Director of a department must ensure that all security violations and breaches that occur within his or her department are properly documented and investigated if required;

d) The Director of a department must apply sanctions as per Article 6 (Conduct) of the Mohawk Council of Akwesasne's General Personnel Policy in response to security incidents when there has been demonstrated misconduct or negligence;

e) The Director of a department may inform any party who could be affected by the security violation or breach of the situation and, where appropriate, refer the case to the law enforcement agency that has proper jurisdiction;

f) Security violations and breaches that involve personal information must immediately be reported to the Director of the department. The Director may inform the Mohawk Court of the circumstances of the incident;

g) Security violations and breaches that involve electronic equipment and systems or the compromise of information on the department's computer network must be immediately reported to Computer Services;

h) Investigation reports on security violations and security breaches shall:

   i. provide a detailed description of the circumstances of the breach or violation;

   ii. provide an analysis of the causes and consequences of the breach or violation;

   iii. establish the responsibility of the individuals who were involved in the breach or violation; and

iv. present recommendations on the measures that could or should be taken to prevent the re-occurrence of the breach or violation.

Chapter Five

Appendices

Appendix 1

Institutions, Organizations and Bodies to Which This Regulation Applies

- Department of Central Resource Services
- Department of Health
- Department of Community and Social Services
- Department of Justice
- Department of Environment
- Department of Housing
- Department of Economic Development
- Department of Public Safety
- Department of Technical Services
- Akwesasne Mohawk Police Services
- Ahkwesahsne Mohawk Board of Education
- Department of Administration
- Mohawk Government & Government Secretariat
- the District Recreation Committees
- any group receiving monetary donations from Council and, then, only towards expenditures of donations.

Appendix 2

Definitions and Acronyms

Applicant: an individual who submits a request for access to a record under this Regulation.

Availability: the condition of being usable on demand to support business functions.

Project manager: the manager who is responsible for the project that is the subject of a PIA (see the definition of the term "project").

Chief Administrative Officer: refers to the person appointed by Council to hold the principal, non-political management position for the government of the Mohawk Council of Akwesasne.

Collection of Information: the acquisition of knowledge about a person or a subject. Collection of personal information is governed by Chapter Three of this Regulation.

Compromise: unauthorized disclosure, destruction, removal (including theft), modification or interruption.

Community: refers collectively to those individual people who are registered members of the Mohawk Council of Akwesasne.

Confidentiality: the sensitivity of information or assets to unauthorized disclosure.

Council: refers to the Mohawk Council of Akwesasne consisting of those candidates duly elected under the Election and Voting Custom Regulations.

Court refers to the Mohawk Court of Akwesasne.

Department: refers to a branch of the organization delivering specialized community services, under the authority of the Mohawk Council of Akwesasne.

Director: refers to a departmental administrator.

Disclosure of Information: the act of allowing someone to have access to certain information. Disclosure may be deliberate or inadvertent.

Employee: in this Regulation, the term "employee" includes Council members, managers, contractors, volunteers and all other individuals who administer programs or deliver services for, or on behalf of, the Mohawk Council of Akwesasne. The definition of "employee" in this Regulation only applies in regards to this Regulation and does not in any way grant or affirm:

- the status as an employee of the Mohawk Council of Akwesasne to any person, or

- an entitlement to any rights or benefits that are normally granted to the employees of the Mohawk Council of Akwesasne under the other enactments and policies.

Enactment: in this Regulation, refers to a code, a law or a regulation of the Mohawk Council of Akwesasne or an Act or a Regulation of another government.

Facility: a work, construction, mobile installation or delimited geographical area that is used to administer the department or its programs or to deliver services to its clients.

Information: knowledge that is used to make business decisions of an administrative, operational, judicial or quasi-judicial nature.

Information Management System: a process, device or group of devices that are used to access, collect, use, disclose, share, store or transmit information.

Information Security: the mechanisms that are used to identify and protect the confidentiality, the integrity, the availability and the value of information;

Information Technology Security: the component of a security program that seeks to prevent the compromise of the confidentiality, the integrity, the availability and the value of electronic information, the equipment and the facilities that are used for its manipulation, storage and transmission.

Integrity: the accuracy and completeness of information and assets and the authenticity of transactions.

MCA: see Mohawk Council of Akwesasne.

Members: for the purpose of this Regulation, refers to the individuals who are members and / or registered with the Mohawk Council of Akwesasne.

Mohawk Council of Akwesasne (MCA): refers to the community government as an organized entity. The government is governed by elected officials who have a governance branch, an administrative branch, and departments who deliver services to community members often under the advice of community boards.

Mohawk Court refers to the Mohawk Court of Akwesasne.

Need to Know: an information handling principle that consists in limiting access to authorized individuals whose duties require such access. Conversely, individuals are not entitled to access information merely because of their status, rank or office.

Personal Information: as defined in Chapter Three of this Regulation, means recorded information about an identifiable individual.

Personnel Security: the use of procedures and mechanisms to verify the trustworthiness of individuals who will likely require access to sensitive or valuable information or assets in the course of their duties;

Physical Security: the use of mechanisms to control access to a facility;

PIA: see Privacy Impact Assessment.

PIA Team: a PIA team is comprised of the individuals who directly and actively participate in the conduct of the primary activities that are involved in the PIA process. The PIA team usually includes individuals who devote a significant part of their time and efforts to the conduct of the PIA, and does not include the individuals who are merely consulted on specific and narrow issues;

Planning: in relation to the development of an information management or communication system, means the phase that follows the approval of the objectives of a project by management and that precedes the functional or technical design of the system. The planning phase is characterized by the following activities:

- the identification and the listing of the technical requirements of the system to be developed;

- an examination of the options available for the development and implementation of the system;

- the development of the implementation strategies for the system development project;

- the identification of the resources that will be required for the development of the system;

- the appointment and the initial briefing of the members of the development project team;

- the determination of time frames and the prioritization of the components of the project.

Privacy Impact Assessment: a process that seeks to measure the consequences of any new project, program, system, regulation or procedure on the privacy of individuals;

Procedure: a series of steps or instructions followed in a specific order that seek to achieve a higher degree of consistency in the performance of a task;

Program: a planned and organized activity or project, structure or system that seeks to further the objective(s) of the Mohawk Council of Akwesasne. It meets one or more of the following criteria:

- It falls under the authority of the Mohawk Council of Akwesasne;

- It has an official and recognized status by the Mohawk Council of Akwesasne, through a resolution, a written Regulation, a contract, an agreement or a public announcement;

- The funds for its development and implementation have been approved by Council or by the management of a department;

- It is managed separately from other existing programs;

- It is placed under the responsibility of one or several officials of the Mohawk Council of Akwesasne

Project: see the definition of the term “Program”;

Record: any object that contains extractable information. Any media that is created, received and maintained by Council’s departments in the course of business transactions and which is kept as evidence of such activity. The term “record” does not apply to the computer applications that used to produce a record.

Security Breach: when sensitive information or assets placed under the responsibility of the Mohawk Council of Akwesasne have been compromised.

Security Investigations: an investigation into an alleged security breach or violation.

Security Violation: an act that causes information or assets to be vulnerable to theft, destruction or unauthorized access. It includes acts that contravene the security requirements in this Regulation.

Sharing of Information: an activity whereby two parties allow each other to acquire the knowledge of some of the information that they respectively possess.

Stakeholders: the stakeholders are the individuals, organizational units or departments who will use the information collected, managed or shared through the information management or communications system for which a PIA is being conducted. For the purpose of this Regulation, the term “stakeholders” does not include the individuals to whom the personal information relates.

Statement of Sensitivity: a description of the confidentiality, integrity or availability requirements associated with the information or assets stored, processed in or transmitted by an information system.

System: a group or combination of interrelated electric and electronic components that are used for the collection, use, disclosure, sharing, transmission, distribution, retention and disposal of personal information. This includes computerized information management systems, data warehouses, servers, LANs, intranet, internet, email systems, traditional and wireless telephone systems, and all other electronic means that are used to communicate information.

Technical Officer: the term “technical officer” refer to the employees or consultants who participated or will participate in the design or the development of the information management or communication system for which a PIA is being conducted.

Threat and Risk Assessment: an assessment of the adequacy of the security measures that are currently in place, based on the identified threats and risks.

TRA: see Threat and Risk Assessment.

Use: the decisions and the actions that are based on the knowledge that one gains from information.

Value: the financial and the strategic importance of information for the Mohawk Council of Akwesasne.

Appendix 3

Access to MCA's Records Form

Request Number: (For Office Use Only)

	IDENTITY OF REQUESTER
SURNAME:	
GIVEN NAME:	
YOUR ADDRESS:	
YOUR TELEPHONE NUMBER:	
YOUR FAX NUMBER:	
YOUR EMAIL ADDRESS:	

DESCRIPTION OF RECORDS SOUGHT:

PREFERRED METHOD OF ACCESS:

I would prefer receiving copies of the records: ☐

I would prefer to examine the originals at the nearest departmental office: ☐

Signature: _____

Dated: _____

Appendix 4

Personal Information Request Form

Request Number: (For Office Use Only)

	IDENTITY OF REQUESTER
SURNAME:	
GIVEN NAME:	
YOUR ADDRESS:	
YOUR TELEPHONE NUMBER:	
YOUR FAX NUMBER:	
YOUR EMAIL ADDRESS:	

DESCRIPTION OF RECORDS SOUGHT:

PREFERRED METHOD OF ACCESS:

I would prefer receiving copies of the records: ☐

I would prefer to examine the originals at the nearest departmental office: ☐

Signature: _____

Dated: _____

Appendix 5

Personal Information Correction Request Form

Request Number: (For Office Use Only)

	IDENTITY OF REQUESTER
SURNAME:	
GIVEN NAME:	
YOUR ADDRESS:	
YOUR TELEPHONE NUMBER:	
YOUR FAX NUMBER:	
YOUR EMAIL ADDRESS:	

DESCRIPTION OF CORRECTIONS SOUGHT:

(attach additional sheets if necessary)

SUPPORTING INFORMATION:

Supporting proof/information for the corrections is enclosed: ☐

Supporting proof/information for the corrections is not enclosed but can be obtained from the following source(s):

Signature: _____

Dated: _____

Appendix 6

Detailed Procedure for the Processing of Access Requests

1. Upon receipt of the access request, the Director of the department (hereafter the “Director”) stamps the date of receipt on the request form;

2. Where applicable, the Director of the department confirms the legitimacy of the request (proper authorization to release to third party, have all parties involved in the documentation signed the request, the individual has the right to request under the Regulation, etc.);

3. If necessary, the Director contacts the applicant to clarify the nature and the scope of the access request or to obtain more information about the information being sought;

4. The Director:

    (a) assigns a file number to the request;

    (b) sends a confirmation of receipt of request to the individual;

    (c) starts an activity log to record discussions, actions, communications, correspondence, etc.;

    (d) starts an access request tracking document;

5. Where the access request cannot be responded to within the thirty-day time limit, the Director sends a notice to the applicant, in accordance with section 4 of this Regulation;

6. The Director requests by e-mail or by fax the relevant files and documentation from all departmental areas where the information is likely to be kept. The covering note must specify the date by which the files or documentation must be sent to the Director’s by their respective custodians;

7. The Director consults with the file handlers for information relevant to the processing of the request and recognizing limitations under the Regulation (refer to fees);

8. Where appropriate, the Director sends a notice to inform the applicant of the fee that is associated with the processing of the access. The notice must

require payment of at least 50 % of the total fee before the access request is processed;

9. The Director photocopies and numbers all copies of the records to be processed for the purpose of the access request;

10. Where appropriate, the Director sends the documentation requiring third party consultation by courier or by registered mail to the third party with a cover letter of explanation. The letter must specify the date by which the response of the third party must be received by the Director;

11. The Director applies the exceptions to the records in accordance with the Regulation;

12. Once information is removed from the documents (words, paragraphs or complete pages, etc.) the Director prepares the copies of the records that will be provided to the applicant;

13. The Director prepares a cover letter informing the applicant of any exception applied to the records and specifying the section of the Regulation that served as a basis for each exception;

14. Where applicable, the Director collects any outstanding fees associated with the processing of the access request;

15. If the requester wishes to view the documents rather than be provided with copies, the Director makes the necessary arrangements (room, time, date, etc.) and informs the requester of the arrangements;

16. After the request has been processed, the Director returns the original documents to their areas of origin;

17. The Director completes the access request processing log;

18. The Director closes the file.

Appendix 7

Detailed Procedure for the Processing of Requests For the Correction of Personal Information

1. Upon receipt of the access request, the Director stamps the date of receipt on the request form or letter;

2. Where applicable, the Director confirms the legitimacy of the request (proper authorization to release to third party, have all parties involved in the documentation signed the request, the individual has the right to request under the Regulation, etc.);

3. If necessary, the Director contacts the applicant to clarify the nature and the scope of the correction request and to gather more contextual information about the correction requested;

4. The Director:

    (e) assigns a file number to the request;

    (f) sends a confirmation of receipt of request to the individual;

    (g) starts an activity log to record discussions, actions, communications, correspondence, etc.;

    (h) starts an access request tracking document;

5. Where the access request cannot be responded to within the thirty-day time limit, the Director sends a notice to the applicant, in accordance with section 16 of this Regulation;

6. The Director requests by e-mail or by fax the relevant files and documentation from all departmental areas where the information is likely to be kept. The covering note must specify the date by which the files or documentation must be sent to the Director's by their respective custodians;

7. The Director consults with the file handlers for information relevant to the correction requested;

8. Where appropriate, the Director sends the documentation requiring third party

consultation by courier or by registered mail to the third party with a cover letter of explanation. The letter must specify the date by which the response of the third party must be received by the Director;

9. Where the Director agrees to make the requested corrections, she or she cross-references all the relevant documents to indicate that their content has been replaced or altered by another record. The original records will not normally be destroyed, as this could deprive the department of a defence in case of litigation;

10. Once the corrections have been made, the Director sends a copy of the amended records to the applicant;

11. Where the Director refuses to make the requested corrections, he or she informs the applicant in writing of the reasons of the refusal. The letter must also specify that the applicant has a right to make a complaint to the Mohawk Court;

12. After the request has been processed, the Director returns the original documents to their areas of origin;

13. The Director completes the access request processing log;

14. The Director closes the file.

Appendix 8

Model Letters

Will be included at the end of the Regulation development process.

Appendix 9

Guide for the Conduct of Privacy Impact Assessments

Due to formatting constraints, this part exists as a separate electronic document

Appendix 10

Fundamentals of Privacy and Information Security

1. Introduction

Whereas Chapter Three establishes certain rules for the collection, use, disclosure, retention and disposal of personal information, Chapter Four provides the framework for the protection of both personal and non-personal information of a sensitive nature that is in the custody or under the control of the Mohawk Council of Akwesasne. Using a more user-friendly style, this Appendix provides more detailed explanations about the requirements of the Regulation, along with examples of recommended practices that employees should try to adopt while performing their duties.

2. Operational and Administrative Context of Security and Privacy

Simply put, confidentiality means restricting access to information of a sensitive nature to the smallest number of individuals possible. Access must be granted on each person's clear "need to know." The "need to know" principle operates on the following two premises:

a) only those who have a demonstrable requirement for information and who have been duly authorized should have the privilege of accessing it; and

b) access by those individuals must only be granted at the time where they really require access to the information.

It flows from the following two premises that the rank, title and role of a employee, manager or elected official are not necessarily relevant when it comes to determining whether that person should have access or not to sensitive information. The critical factor is the clear requirement for performing that person's immediate duties. In this context, the notion of "duties" refers to:

a) the making of a business or professional decision; or

b) the performance of a business-related or professional activity.

Strictly speaking, administrative convenience and cost saving factors do not just by themselves justify access to sensitive information, especially when such access is likely to cause an intrusion into the privacy of an individual. Other more compelling reasons should always be part of the decision to collect or share sensitive personal and non-personal information. Similarly, other circumstances that fit under the "nice to know" considerations do not necessarily meet the "need to know" criteria. The key is to assess the benefits and the risks associated with each activity, project, program, or system for which the sensitive information is to be used.

The sensitivity level of information is normally described in a **statement of sensitivity**, which also provides the rationale for such determination. The statement of sensitivity also constitutes the basis for:

a) the conduct of security **Threat and Risk Assessments** (TRA) – as explained Chapter Four;

b) the conduct of **Privacy Impact Assessments** (PIA) – see the Guide for the Conduct of PIAs in Appendix 9 of this Chapter; and

c) the implementation of **security measures**, as described in the following paragraph.

3. Implementation of Security Measures

By security measures, we mean the use of physical design, physical and electronic devices as well as personnel-related safeguards to protect the sensitive and valuable information of a department against unauthorized access, use, disclosure, interception, removal and destruction. Security measures seek to achieve the following objectives:

a) to minimize:

i. the unauthorized collection, use and disclosure of personal information that could result in a loss of life, harm to clients, embarrassment, undue media attention, etc.;

ii. the waste of resources that may result from over-protecting information or assets or from protecting information or assets that do not require protection;

iii. liability for the Mohawk Council of Akwesasne;

iv. the interruption of services;

v. the costs associated with the protection of sensitive information and with the protection of the equipment and the facility in which is it stored or processed;

vi. administrative and operational inconveniences.

b) to maximize:

i. access to the information that is required by those who need it to perform their duties;

ii. the efficiency and the effectiveness in the delivery of the services;

iii. reporting and accountability;

iv. transparency of departments and the effective exchange of essential information with the public;

v. the safe access to the facilities and areas where the public is admitted;

vi. the safety of the staff and the clients of departments.

c) to make employees more aware of the rules that govern the management of sensitive personal and non-personal information, including:

i. what information can be disclosed to individuals outside their respective department;

ii. when that information can be disclosed;

iii. in what form the information can be disclosed; and

iv. what information must be protected and how it must be protected.

The following paragraphs provide examples of recommended security measures that employees should adopt while performing their duties. These

measures must not be viewed as the only measures that can be taken to reduce the risks, as they only represent a small number of available options to ensure the protection of information. They should not either be applied blindly in all situations regardless of the specific circumstances, as some of them may not be appropriate in certain operational environments or contexts. A threat and risk assessment and a good dosage of common sense should guide employees in deciding what security measures they should implement in each situation.

4. Protection of Electronic Information

Electronic information is formed of electromagnetic particles, and as a result, does not take an eye visible form. Electronic information includes electronic files and documents, telephone conversations and other electronic signals and emissions such as those that transit through optical cables and devices and through cellular and cordless telephones.

Although its non-tangible form offers some protection against accidental access by people who may walk into an office, electronic information remains more difficult to protect than conventional paper records or files as it is virtually impossible to know where it is, what form it takes, and how many copies of it exist at any given time. For these reasons, the best approach in protecting electronic information is to implement security measures that cover the **hardware**, the **software** and all the **environmental elements** of the information or communications system. Those three main groups are defined in the following paragraphs

a) hardware: the hardware consists of the physical components such as the servers, personal computers, portable devices, printers and all other peripherals. Hardware security seeks to ensure the protection of those components from theft, destruction, alteration and misuse. It also seeks to ensure that information is not accidentally lost or altered as it travels within or between those devices;

b) software : Software security refers to the safeguarding of computer applications, data, operating systems, programming languages and controllers of IT systems. Software security encompasses administrative controls, quality assurance, development and maintenance procedures, management of the configuration, isolation and access, and audit controls. Software can be viewed in three ways:

i. As a safeguard: software provides access control, encryption, network management, etc.,

ii. As an asset: software protection is necessary to maintain the availability and integrity of systems,

iii. As a threat: certain software is capable of bypassing, over-riding or altering controls and can be used to gain unauthorized access to sensitive applications and data.

c) environmental elements of information management and communications systems: these elements include of LANs, e-mail, intranet and internet, the office environment and all other environmental factors that can affect the continuity aspect in the delivery of services by departments.

5. Installation of Software and Computer Attachments

Every time someone installs or downloads a new application such as a game or a screen saver on an office computer, there is a risk (often high) that this will affect the functioning or the performance of that computer, of the server to which that computer is connected or of another computer that is connected to the server. Peripherals such as printers, modems and routers can also be affected. As is often the case in those situations, if the IT technicians are not aware of the source of the problem, they will likely have to spend dozens, if not hundreds of hours and maybe hundreds, if not thousands of dollars trying to reconfigure the entire system to accommodate the new application.

Employees should also remember that several computer applications that can be purchased on the market or downloaded from an internet web site contain hidden commands that connect the computer on which they are installed to an outside device. That outside computer or device then scans the content of the computer hard drive on which the application was installed and searches it for commercial secrets and other politically sensitive information that can later be resold to third parties. Installing such applications constitutes a security breach that can seriously compromise the operations and the credibility of a department, if not the credibility of the Mohawk Council of Akwesasne. For those reasons, no computer applications of any type and origin should be downloaded or installed without prior permission from Computer Services.

6. Use of Office Computer and Other Office Equipment

The best way to avoid technical and security problems is to limit the use of office computer and other equipment to what they were designed and configured for: official business of the department. As a result, employees should always discuss their intentions with their manager and with Computer Services before they use an office computer for a purpose that is not directly related to official business of their department. If permission is granted, arrangements will be made to ensure that the new use does not cause security problems or interference with the business processes of the department.

Employees should also remember that all departmental electronic information management and communications systems are subject to the Access to Records Regulation of the Mohawk Council of Akwesasne, therefore, individuals from outside those departments have a right to request access to the information that is kept in those systems. The same applies to court challenges, which may eventually bring some outside parties to request access to the information that is kept in those as well. The best approach when creating information is to make sure that you are comfortable with the possible release of that information to the general public.

7. Use of Local Area Networks (LANs), E-mail, Intranet and Internet

Because all electronic information management and communications systems may be monitored from a distance and keep traces of the information that transits through them, they should never be considered as totally safe, especially when it comes to exchanging sensitive information. Where applicable and where feasible, other options should be considered for the transmission of such information.

8. Use of Portable Computers

The risks associated with the use of portable computers and hand-size electronic agendas are mainly loss and theft. The following precautions should be taken when using those assets:

a) portable computers should be physically secured in a proper storage area at all times when not in use;

b) they must never be left unattended in a vehicle or in a public area;

c) the password feature of portable computers should be activated so as to prevent their use in case of theft or loss;

d) where possible, an encryption software should be installed on all computers that are used in areas where they could be vulnerable to theft or loss;

e) the removal of a portable computer from the department's premises must be accounted for in a register so as to ensure that someone is aware of who has it and where it is;

f) the procedure for disposing of computers applies to all portable computers and hand-size electronic agendas.

9. Working and Accessing Information From Outside a Department's Premises

Operational requirements combined with employees' preference to work form their home and technological evolution have been the three main contributing factors to the practice of working outside a department's premises. But from a security perspective, this practice raises two main issues:

a) paper based records and files usually have to be taken out of the office;

b) often employees will try to connect to the office server from a remote location so that they can gain timely access to the information that they require to perform their duties.

The following precautions should be taken in order to minimize the risks of loss and unauthorized access:

a) sensitive information must never be taken out of a department's premises;

b) in transporting sensitive information and equipment outside a department's premises, care must be taken to ensure that its confidentiality, integrity and value are not compromised. For example, sensitive information must never be left unattended in an area where unauthorized individuals could view it;

c) sensitive information must not be processed using an employee's home personal computer, as the information may remain on the hard drive of that computer. *Not saving information on the hard drive does not mean that no part of the information will be recorded on it*;

d) the removal of information and assets from a department's premises should be accounted for in a register so as to ensure that someone is aware of who has it and where it is;

e) precautions must be taken to prevent unauthorized access, modification or elimination of the department's information. For example, managers and employees must not use or leave restricted information in a place where the other occupants of their residence could view it and they must not use their personal, cordless telephone to conduct business for the department, as telephone signals can be easily picked up by their surrounding neighbours;

f) in order to minimize the risk factor, all departmental information and equipment that are used to do work from a remote location must be returned to the department's premises as soon as possible.

10. Deletion of Electronic Information and Disposal of Computer Equipment and Accessories

Deleting a file from a hard drive, a diskette or a backup tape using the conventional "delete" feature in Windows (or any other similar application) does not really erase the file. Instead, it only removes the title of that file from the directory of the disk, leaving all the information totally intact in the background.

As a result, it is possible that information that was once saved on a disk, diskette or backup tape may be recovered and read by someone who will have access to that media, even years after the information was deleted from it. As a result:

a) diskettes and other electronic storage media that once contained sensitive information, especially personal information, must never be re-used unless the information on them has been deleted using a method approved by Computer Services;

b) all computers and storage media (i.e. hard drives, diskettes, backup tapes, etc.) that were at any point in time used to collect, manipulate,

transmit, or store sensitive information must be disposed of in accordance with the standards approved by Computer Services;

c) Computer Services must also be consulted before any computer is transferred from one program or unit of a department to another, so as to ensure that the information that is stored on the hard drive of that computer does not become accessible to individuals who do not have a need to know.

11. Use of Fax Machines

The following is a list of some of the main security issues associated to the use of fax machines:

a) the risk of the sender dialling a wrong number, thus causing unauthorized access to the faxed document. The risk here is high because it involves the human error factor;

b) the risk associated with the location of the fax machine in the receiving office. Because fax machines are not always located in protected areas, the risk of unauthorized access to the documents that are received on them is high;

c) the interception of the fax signals by third parties as they travel on regular telephone and satellite communications systems;

d) mechanical and electronic defects in the sending or the receiving machines;

e) line interference that could prevent the document or part of it from reaching its intended destination. This can result in a loss of integrity or availability of the information;

f) the risk associated with the fact that other users of the fax machine at the receiving end may inadvertently take the document or a part of it. This also results in a loss of integrity or availability of information.

Some of the safe rules for the use of fax machines include:

a) placing fax machines in restricted areas so as to minimize the risk of unauthorized access to the documents that are received on them;

b) using a department's fax machines only for official business of the department, so as to reduce the number of users, unless otherwise specified by Regulation;

c) making advance arrangements by telephone with the individual to whom the document s being sent to ensure that someone stands by the fax machine to prevent loss or unauthorized access;

d) where feasible, removing all identifiers from the document prior to sending it by fax, or by dividing multiple page documents in two, three, or even four segments and sending each segment as separate fax messages;

e) verifying the fax number of the addressee at least twice before pressing the 'send' or 'start' button on the fax machine;

f) always dialling the fax number of the addressee in full instead of using the pre-programmed number for that person as an error in pressing the wrong pre-programmed button would result in the information going to the wrong place;

g) where possible, using secure fax machines (with an encryption feature on both the sending and receiving machines) to transmit documents that contain extremely sensitive information.

12. Use of Cellular Phones and Other Wireless Equipment

Cellular and cordless telephones and radio-transmitters found in vehicles use airwaves to transmit electronic signals. The risks associated with the use of wireless equipment include interception of the signals, and because such equipment is usually easy to carry, theft and loss are also risks. As a result, the following precautions must be taken when using such equipment:

a) never sending or discussing sensitive information while using wireless equipment, unless encryption methods have been approved by the Computer Services to transmit such information;

b) making sure that mobile wireless equipment is physically secured in a proper storage area at all times when not in use. Employees travelling with such equipment should ensure that their vehicle is locked at all times and keys are never left in the vehicle in their absence.

c) where available, the password feature of cellular telephones should be activated so as to prevent the use of the telephone in the event of a theft or loss.

13. Protection of Paper Based Records and Other Tangible Media

The physical handling and storage of paper and other tangible files and records are made easier by the fact that they are visible. This characteristic, however, also makes their confidentiality more vulnerable, as they can be read without any sophisticated tools or instruments. For example, the paper copy of a document left on a desk is more vulnerable than the electronic version of the same record that would be kept on the hard drive of the computer located on the same desk. This is because the person wanting to read the electronic record would have to turn the computer on, successfully by-pass the password protection feature, and then search for the specific record. This reality demonstrates the importance of implementing physical security measures to minimize the risks of unauthorized access to information that exists in a physical format.

Employees can practice simple, basic physical security awareness by:

a) Not posting personal information in an identifiable form on whiteboards and other publicly visible surfaces

b) Not discussing the particulars of one's job with people outside the organization, especially if the information may allow someone to identify some of the individuals who are involved in the issues;

c) Not leaving sensitive documents on a desk or counter where they can potentially be viewed by individuals who have no right or need to have access to them;

d) Being careful not to leave or forget records in the photocopier or fax machine;

e) Removing all records from the briefcase that was used to transport them;

f) Storing sensitive records in an appropriate filing cabinet or in another safe container when leaving the office, even if it is only for a short period of time. This is known as the "clean desk Regulation";

g) Turning files upside down when someone enters their work area, and not placing sensitive or valuable information in a position where it could be viewed by visitors, maintenance or repair personnel;

h) Leaving a note to ensure that someone in the office is aware of the fact that they are taking a file out of the office. So if anything ever happens to that person (death, medical emergency, etc.) while they have the file under their control, the department can initiate immediate action to recover the file and minimize the security risks to it.

14. Physical Access Controls

Physical security involves the use of physical, procedural and psychological barriers to delay or deter unauthorized access. Locks and doors are good examples of protection mechanisms.

To facilitate monitoring and access control of areas where sensitive information is kept, offices are often divided into **zones** established in progressive security levels. This is often the case in building with a reception area where the public is allowed access into the building up to the exterior side of the reception counter; all employees are allowed access to the general office area located inside the counter; and each employee is allowed unlimited access to their respective private office area but not those of other employees.

Office procedures and signage normally specify who is allowed aces to each area of the building, and employees must at all times comply with the security directives prescribed for each zone. They are also expected to challenge any person who may try to enter an area in which they have not been authorized to enter and to immediately report to their superior or to their security contact person, any real or perceived violation or breach of security rules.

The effective use of zones depends on the implementation of appropriate security procedures by everyone:

a) respecting the need to access principle;

b) respecting zone perimeters;

c) escorting visitors;

d) not leaving records, files, diskettes and other media that contain sensitive information in places where they can be viewed or taken by unauthorized individuals;

e) taking precautions when discussing sensitive information;

f) locating shredders and other containers (filing cabinets, bookshelves, safes, etc.) so that sensitive information and assets are not left unattended or vulnerable.

15. Transmission and Transport of Records and Information

The highest risks to the confidentiality, integrity and value of records or information often occur when they are transmitted or transported from one location to another. This is so because the transport and the transmission of information involves the removal of the record or information from a safe environment (filing cabinet, building, unit, etc.) where it is usually kept, and its physical displacement to another environment. The objective is to therefore do everything possible to:

a) Minimize the length of time during which the record or information is left outside a safe environment;

b) Recreate the secure conditions in which the record or information is normally kept during its transmission or transport; and

c) Ensure that the environment where the record or information is transported or transmitted presents the same security characteristics as the originating area.

The following suggestions should also provide for optimum protection of records and information throughout the transmission or transport process, under normal circumstances:

a) not telling anyone who does not have an absolute need to know that a sensitive record or information is being sent to another person or location;

b) If highly sensitive information is being transmitted via insecure infrastructure (i.e. telephone, internet, diskettes, etc.), ensuring that this is done in accordance with the approved standards and procedures of Computer Services;

c) not using a computer that is directly or indirectly linked to an outside network r to the internet, unless otherwise permitted by a person with proper authority;

d) always using the appropriate container to send physical records;

e) double checking the address of the recipient and add his/her telephone number on the box or envelope that is used to send a physical record;

f) making sure that the box or envelope is addressed to an individual and not to an organization; this way, it will be easier to track down the shipment if required;

g) contacting the addressee before sending the box or envelope and asking them to inspect it upon reception to ensure that no tampering occurred during the transport or transmission and to confirm reception as soon as possible;

h) conducting an assessment of the threats and risks before sending a sensitive or valuable record or information in order to determine the most secure way to send it or transport it;

i) properly identifying the originator of the box or envelope prior to sending it as this will facilitate its retrieval by the shipping company;

j) sealing the box or envelope so that it cannot be easily opened, and without leaving evidence of tampering;

k) not writing anything on the box or envelope that might suggest the existence of sensitive or valuable information in it. Markings such as ‘confidential’ attract attention and are likely to prompt unauthorized individuals to open the package;

l) assessing the reliability of the individual, moving company, courier company or computer system that will be used to send the record or information, and clearly establishing the required security conditions to implement during the transport or transmission;

m) providing clear and precise instructions for the transport or transmission, including the mode of transport or transmission (by air, etc.), and the delivery procedure (directly to the individual to whom it is addressed, etc.);

n) asking for, and keeping the shipment reference number in a safe place for easier tracking of the package.

16. Transport and Transmission of Publicly Available Records and Information

Confidentiality is not generally an issue for publicly available records and information, however, reasonable precautions should be taken to prevent its loss and protect its integrity. Such measures may include keeping a copy of the document so that it can be replaced in the event of loss or alteration.

Appendix 11
Contacts and References

1. Departmental Contacts:

Individuals who have questions about the implementation of this Regulation may contact:

Email:

Telephone:

In person:

Traditional mail:

2. To Obtain an Electronic Copy of This Regulation:

This Regulation is available at the following Internet address:

URL:

3. The Mohawk Court:

The Mohawk Court is mostly responsible for promoting this Regulation and for handling complaints in relation to its implementation. The Court may be contacted at the following address:

Phone:

Fax:

Internet :