Statement of Policy and Procedure	
Policy No.	
Issue/Effective Date	**June 19, 2019**

Chippewas of the Thames First Nation

Information Management Policy

Approved by Council on June 19, 2019

Table of Contents

1. Definitions

"Classification"	is the process of categorising records according to a predetermined hierarchy or scheme. Functional-based classification is the arrangement of records based on the business functions and activities of the Chippewas of the Thames First Nation. This allows the Council to understand the records collected and created related to each business process / activity and how that record is used.
"Information"	is knowledge communicated or received and may be any documentary material regardless of communications source, information format, production mode or recording medium.
"Information Security"	refers to the physical, electronic and policy instruments that are used to protect information from unauthorized access (protecting confidentiality), unauthorized use (protecting integrity), unauthorized modification (also protecting integrity) and unauthorized destruction (protecting availability).
"Officers"	means an individual appointed by Council as the Executive Administrator, Comptroller, Tax Administrator or any other employee appointed by Council as an Officer with the delegated authority to bind the First Nation;
"Personal information"	refers to all information that reveals factual or subjective elements of knowledge about an identifiable individual. In addition to the basic elements that are commonly used to identify and interact with an individual - such as the individual's name, gender, physical characteristics, address, contact information and identification and file numbers - it also includes criminal, medical, financial, family and educational history as well as evaluative information and other details of the individual's life.
"Privacy Protection"	refers to the decisions made by a Chippewas of the Thames First Nation in regards to the acceptable ways to collect, create, use, share/disclose, retain, protect and dispose of the Personal Information that it needs for its administrative and operational needs.
"Record"	is a special form of information, and for the purposes of this policy refers to information created, received, and maintained by the Chippewas of the Thames First Nation for business purposes or legal obligations, which enable and document decision-making,

	and support Chippewas of the Thames First Nation reporting, performance and accountability requirements. A record may be electronic or hardcopy paper based.
"Recordkeeping"	is a framework of accountability and stewardship in which records are created or acquired, captured, and managed as a vital business asset and knowledge resource to support effective decision-making and achievement of results for the Chippewas of the Thames First Nation.
"Repository"	refers to a preservation environment for a record. It includes specified physical or electronic storage space and the associated infrastructure required for its maintenance. Business rules for the management of records in a Repository need to be established, and there must be sufficient control for the resources to be authentic, reliable, accessible and usable on a continuing basis.
"Rollback Procedure"	means the ability to restore system to previous configuration prior to change, with documented procedures and steps to complete the process.
"Virtual Private Network"	means a Virtual Private Network ("VPN") which is a way to use a public telecommunication infrastructure, such as the Internet, to provide remote offices or individual users with secure access to their organization's network.

2. Information Technology

A. Policy

The Chippewas of the Thames First Nation's information systems will support its operational requirements and have appropriate safeguards and monitoring processes in place to adequately protect the Chippewas of the Thames First Nation's information.

B. Purpose

The purpose of this policy is to ensure that information system integrity, specifically as it relates to the financial administration system, is maintained and supports the strategic and operational requirements of the Chippewas of the Thames First Nation.

C. Scope

This policy applies to all staff involved in the selection, implementation, operations, or ongoing maintenance of the Chippewas of the Thames First Nation's information systems. This includes the Executive Administrator, and information technology staff.

D. Responsibilities

(1) Council is responsible for:

a. Establishing and implementing documented procedures for information technology used by the Chippewas of the Thames First Nation in its operations.

(2) The Executive Administrator is responsible for:

a. Ensuring that controls are in place over information technology, whether performed by an internal staff member or outsourced to an external organization;

b. Monitoring the performance of internal and/or external information technology professionals.

(3) The information technology professional is responsible for:

a. Maintaining the integrity of information systems within the Chippewas of the Thames First Nation.

E. Procedures

(1) Planning and evaluation

a. The Council, with the assistance of the Executive Administrator and input from information technology staff, will ensure that information systems are developed that support the Chippewas of the Thames First Nation's strategic plan and operations.

b. When there are no individuals internally with the requisite technical skills to identify information technology requirements or evaluate options, the Executive Administrator will seek advice from a qualified external individual or organization.

(2) Outsourcing

a. Subject to the Procurement Policy, the Executive Administrator is responsible for the selection of contractors providing information technology services, the definition of services in their contracts, establishing service level agreements and the administration of the contracts.

b. Specific items which should be included in the procurement of information technology services and final contract with the chosen provider include:

i. A requirement that the service provider submits regular reports of all work performed on the Chippewas of the Thames First Nation's information systems;

ii. A requirement that outsourced parties are responsible to comply with legal and regulatory requirements, including the protection of confidential and private information;

iii. Access by outsourced parties to Chippewas of the Thames First Nation information is provided on a 'need to know basis' only.

(3) Data management

a. Subject to the Records and Information Policy, data retention allows access to appropriate data to specified personnel where required, depending on the type of data retained.

b. All sensitive, valuable, or critical information/data residing on the Chippewas of the Thames First Nation's information technology systems must be periodically backed-up. Backups will occur incrementally on a daily basis for the financial information system by an offsite provider and it is saved electronically offsite. Full backups of the entire information system is performed on a daily basis by a separate provider and saved electronically offsite.

(4) Access management

a. All individuals requiring access to Chippewas of the Thames First Nation information systems will have unique user identification. Shared user IDs or passwords will not be permitted.

b. Requests for access to the Chippewas of the Thames First Nation's network, accounting system, or other access restricted information system must include a description of an employee's role and rationale for the level of access required. Signed approval must be obtained from the Executive Administrator (or designate).

c. User ID and password are required for access to the network and other critical programs/areas such as the accounting system. Automatic authentication using scripts or macros inserting user IDs and/or passwords are prohibited.

d. Individuals will be given access privileges to the extent necessary to fulfill their individual job function and no more. Systems and applications should not be configured with unrestricted access to all data.

e. When an individual or contractor is terminated or ends employment with the Chippewas of the Thames First Nation, their user IDs must be disabled immediately.

f. Support personnel must notify the user when attempting to take control of a workstation. All instances where specific software is loaded to remotely control a workstation must be removed when the support function is completed. The use of the remote control software must be in accordance to applicable agreements.

(5) Information system security

a. Security tools and techniques are implemented to enable restrictions on access to programs and data.

b. Security tools and techniques are administered to restrict access to programs and data.

c. Each computer resource must have an approved antivirus program installed. The following standards must be met:

    a. The antivirus program must not be disabled (other than on a temporary basis when required to complete a repair) and must be configured to scan all programs and files upon execution and must have real time protection enabled. If encrypted and password protected files cannot be virus checked, it is the responsibility of the user to ensure that virus checking takes place whenever this protection is removed;

    b. Antivirus files are updated automatically.

d. Network firewalls must be configured to support a 'least-privilege' approach to security, allowing only specific systems, services and protocols to communicate through the network perimeter. Logical and physical access to these systems must be limited strictly to those personnel with specific training and authorization to manage the device. Additionally, the following Firewall standards must be addressed:

    i. Firewall and proxy servers must be securely installed;

    ii. Detailed firewall logs must be maintained;

    iii. Alerts must be raised if important services or processes crash.

(6) Change management

a. All new data structure and modifications to data structure will be tested before implementation.

b. All computers, hardware, software and communication systems used for a production environment must employ a documented change control process. The change management process should include the following activities:

i. The data structure is consistent with the needs of the Chippewas of the Thames First Nation;

ii. Description and rationale for the new network, hardware, communication and systems software change and how it is consistent for the needs of the Chippewas of the Thames First Nation;

iii. An assessment of any risks involved with the change;

iv. Roll-back considerations;

v. Implementation considerations;

vi. A description of the testing required;

vii. Approval from the Executive Administrator;

viii. Communication of changes to Chippewas of the Thames First Nation staff as appropriate.

(7) Monitoring

a. Only approved and authorized programs will be implemented onto Chippewas of the Thames First Nation information management systems. Periodic reviews of the workstations and the system will take place to monitor compliance with this requirement.

b. A log of staff, their user IDs, and their access levels within Chippewas of the Thames First Nation information systems will be maintained. On a semi-annual basis, the Executive Administrator will review the log to ensure users and the associated access rights are appropriate. Access rights that will be monitored include the following:

i. User access management (i.e. the accounting system);

ii. Third party access (i.e. outsourced information technology professionals);

iii. Network access and file sharing;

iv. Remote and VPN access.

c. Network system performance is monitored on a regular basis.

d. The firewalls must be monitored daily and their functionality audited semi-annually.

F. References and Related Authorities

(1) FMB's Financial Management System Standards

a. Standard 19.8 - Information Technology Controls

(2) FMB's Financial Administration Law Standards

a. Standard 17.6.2 - Information Technology Controls

G. Attachments

None

3. Record Information Management

A. Policy

Records are a special form of information that is created, received, and maintained by the Chippewas of the Thames First Nation for business purposes or legal obligations, which enable document decision-making, and support Chippewas of the Thames First Nation reporting, performance and accountability requirements. Records must be created and collected, organized, retained, and safeguarded in a manner that enables their long term availability, understandability and usability.

The Sage 300 Advanced (ACCPAC) system is to be maintained to record all financial transactions affecting assets, liabilities, equity, receipts and expenditures. The general ledger is departmentalized to accommodate the reporting requirements of the First Nation. The Chippewas of the Thames First Nation uses fund accounting procedures for the following funds:

i. Operating fund;
ii. Capital funds;
iii. Trust funds; and
iv. Restricted and other funds.

B. Purpose

The purpose of the policy is to provide guidance on effective Recordkeeping practices that enable the Chippewas of the Thames First Nation to create and acquire; manage; and, protect the integrity of its records that support its decision-making, and support Chippewas of the Thames First Nation reporting, performance and accountability requirements.

C. Scope

This policy applies to all Council members, members of the Finance and Audit Committee, Officers and employees of the Chippewas of the Thames First Nation and any contractors or volunteers performing services on behalf of the Council. The direction provided in this policy applies to all records created and acquired by the Chippewas of the Thames First Nation regardless of format (i.e., both electronic and hardcopy paper records).

D. Responsibilities

(1) Council is responsible for:

a. Establishing and implementing documented procedures for records management within the Chippewas of the Thames First Nation.

(2) The Executive Administrator is responsible for:

a. Implementing appropriate Recordkeeping practices,

b. Ensure appropriate safeguards of the Chippewas of the Thames First Nation's records;

c. Ensuring compliance with the established records retention and disposition schedule and overseeing the disposition process;

d. Ensuring that employees and any contractors or volunteers performing services on behalf of the Council are fully knowledgeable of their responsibilities as they relate to Recordkeeping practices.

(3) The Comptroller is responsible for the creation of new account codes and departments within the accounting bookkeeping system.

(4) Employees, contractors and volunteers are responsible for:

a. Complying with the established records management policy.

b. Immediately reporting to their supervisor any potential breach related to compliance with the record keeping policy, including the incidents in which the safeguarding of records may have been compromised.

E. Procedures

(1) Accountability

a. Each record shall have a designated steward that ensures the Recordkeeping framework outlined in this policy is applied to the record. All employees, contractors, or volunteers that are in custody of a record must ensure it is managed in accordance with this policy.

b. Permanent records such as operations manuals, policies, and procedures will be reviewed and updated by the steward periodically, but at least every two years, or more frequently as required.

c. Records under the stewardship of an employee or any contractor or volunteer that is departing must be formally transferred to another employee through a knowledge transfer process. This process should include information on the types of records to be transferred, how the records are organized, in which Repository the records are kept, and required safeguards.

(2) Creation and Collection

a. The accounting records consist of computerized:
   i. Accounts Payable
   ii. Accounts Receivable
   iii. Canadian Payroll
   iv. General Ledger
   v. Common Services
   vi. Administrative Services

b. All important activities and decision making processes of the Chippewas of the Thames First Nation should be identified, including the records required to support those processes, to

ensure accountability, preserve an audit trail, and protect the Chippewas of the Thames First Nation from liability.

c. All information at its time of creation or collection should be assessed to determine if it supports Council's business purposes or legal obligations, and enables decision-making. If determined to be a record its management should comply with the procedures outlined within this policy.

d. The Chippewas of the Thames First Nation's records shall be created using the most appropriate application so as to ensure that they adequately support the objectives for which they are created and can easily be used by those who need them to perform their duties – i.e., using MS Excel instead of MS Word to develop spreadsheets with financial figures, etc.

e. The Chippewas of the Thames First Nation's records shall contain all the information which is necessary to achieve the objectives for which each of them is created; yet their contents shall be limited to only what is necessary to achieve those objectives. This should include limiting the information collected through forms to only that which is required.

f. Whenever possible, the record shall contain information about one single function or activity so as to facilitate information classification, organization, retention and retrieval.

g. The Chippewas of the Thames First Nation's records shall be legible, written in plain language and adapted to their specific audience.

h. Only one copy of each record should be created or collected. When creating or collecting a record, individuals should first check to see if the record is already in existence. In instances of multiple copies of the same record, copies should be securely disposed of in accordance with the requirements of this policy.

(3) Organization and Classification

a. A filing system is to be established for the retention of minutes of all financial agreements and amendments, contracts, First Nation Council meetings, resolutions, all vouchers and documents including bank statements and cancelled cheques that support the transactions recorded in the bookkeeping system.

b. Within the accounting bookkeeping system - Account codes are five digits preceded by department codes. Department codes are two alfa and four digits and are placed within the range of the department that it best fits.

c. The title of the document should be short but meaningful.

d. The title may contain multiple words, and should be ordered from most specific to less specific related to the business activity or function.

e. Common words such as 'draft' or 'letter' should not be at the start of the title.

f. Records should be made accessible, shared and re-used to the greatest extent possible, subject to technological, legal policy and security restrictions.

(4) Maintenance, Protection and Preservation

a. Records must be protected and stored in the appropriate repositories in a way that preserves their long-term availability, understandability and usability.

b. Electronic backups should be taken of all electronic records on a regular basis.

c. Any records that are only in hardcopy paper-based format should be assessed to determine if they need to be scanned or if other physical security measures need to be taken (e.g. use of fire/water proof cabinets) to ensure their long term availability.

d. Records that contain Personal Information or information of a confidential nature related to the Council, or a third party, such as the confidential financial information related to a business, should be labelled as CONFIDENTIAL.

e. Confidential records should be protected with appropriate safeguards to ensure only those with a need to know will have access to the records:

   i. For electronic records, confidential records should be protected with controls on the document itself (such as password protection) and other administrative controls, such as restricting access to the electronic repositories in which the record is stored. Confidential records should not be emailed 'in the clear' without appropriate protection.

   ii. For hardcopy paper-based records, confidential records should be stored in secure filing cabinets at all times unless being used, and transported in a secure manner if required to be offsite.

(5) Retention and Disposition

a. The Chippewas of the Thames First Nation records shall be retained for the period specified in the records and information retention and disposition schedule, as outlined in Appendix A. They shall be disposed of in a manner that prevents their reconstruction (for paper based records) or recovery (for electronic records).

F. References and Related Authorities

(1) The FMB's Financial Management System Standards

a. Standard 19.0 - Risk Management

b. Standard 23.0 - Records and Information

(2) The FMB's Financial Administration Law Standards

a. Standard 21.0 - Records and Information

G. Attachments

(1) **Appendix A** – Document Retention Periods

4. Information Privacy

A. Policy

Ensuring the privacy of Personal Information provided to the Chippewas of the Thames First Nation by individuals is essential to not only ensure compliance with legislative requirements such as those outlined in the Personal Information Protection and Electronic Documents Act or substantially similar legislation, but also to ensure continued stakeholder confidence in the Chippewas of the Thames First Nation and that accountability is maintained.

B. Purpose

The purpose of this policy is to provide guidance on the implementation and maintenance of appropriate information privacy practices within the Chippewas of the Thames First Nation related to the collection, use, disclosure, retention, and safeguarding of Personal Information.

C. Scope

This policy applies to all Council members, members of the Finance and Audit Committee, Officers and employees of the Chippewas of the Thames First Nation and any contractors or volunteers performing services on behalf of the Council. The direction provided in this policy applies to all Personal Information created and acquired by the Chippewas of the Thames First Nation regardless of format (i.e., both electronic and hardcopy paper records).

D. Responsibilities

(1) Council is responsible for:

a. Establishing and implementing documented procedures for privacy and the management of Personal Information within the Chippewas of the Thames First Nation; and

b. Appointing a Privacy Officer to manage and oversee the Chippewas of the Thames First Nation's compliance with privacy requirements; and this policy;

c. Reviewing and approving all requests by third parties to conduct surveys / gather information from individuals in the COTTFN community.

(2) The Executive Administrator is responsible for:

a. Ensuring compliance with the established information privacy policy.

(3) The Privacy Officer is responsible for:

a. Developing and maintaining standards, policies and procedures that support the objectives of the Chippewas of the Thames First Nation's privacy program;

b. Ensuring that all the activities of the Chippewas of the Thames First Nation are conducted in compliance with the established privacy standards, policies and procedures and in accordance with the generally accepted privacy principles. For this, the Privacy Officer will:

i. Provide training and awareness on Privacy Protection.

ii. Ensure that community members are aware of their rights as they relate to privacy, including their right of access to, and the right to request the correction of, all the Personal Information which is kept about them by the Chippewas of the Thames First Nation.

iii. Act as an expert resource on privacy matters within the Chippewas of the Thames First Nation.

iv. Conduct periodic reviews of the Chippewas of the Thames First Nation's activities that involve the collection, use, disclosure, retention, and safeguarding of Personal Information.

c. Investigating all complaints regarding the collection/creation, accuracy, use, sharing/disclosure, protection, retention and destruction of Personal Information and reporting the results to the appropriate managers and, where warranted, to Council;

d. Recommending changes to policies, procedures and practices in response to the issues raised in the complaints; and

e. Responding in writing to the requests for access to, and correction of Personal Information submitted by employees and community members within thirty calendar days from the date of the receipt.

(4) Employees, contractors and volunteers are responsible for:

a. Complying with the established information privacy policy; and

b. Immediately reporting to their supervisor privacy breaches of which they become aware.

E. Procedures

(1) Accountability

a. The Chippewas of the Thames First Nation must appoint a Privacy Officer to ensure the principles outlined in this policy are appropriately implemented.

b. The Chippewas of the Thames First Nation is responsible for Personal Information in its possession or custody, including information that has been transferred to a third party for processing. The organization should use contractual or other means to provide a comparable level of protection while the information is being processed by a third party.

(2) Identifying Purpose

a. The purposes for the collection of Personal Information should be communicated to individuals at or before the time of collection. Depending upon the way in which the

information is collected, this can be done orally or in writing. An application form, for example, may give notice of the purposes.

b. Personal information should be collected directly from the individual whenever possible.

c. Persons collecting personal information must be able to explain to individuals the purposes for which the information is being collected.

(3) Consent

a. With limited exceptions, the Chippewas of the Thames First Nation must obtain consent from an individual before collecting their personal information. Consent requires that the individual is advised of the purposes for which the information is being collected and how it will be subsequently used and disclosed.

b. Consent must be stated in such a manner that the individual can reasonably understand how the information will be used or disclosed. Consent must not be obtained through deception.

c. Personal information can be collected, used, or disclosed without the knowledge and consent of the individual in only limited circumstances. For example, legal or security reasons may make it impossible or impractical to seek consent. When information is being collected for the detection and prevention of fraud or for law enforcement, seeking the consent of the individual might defeat the purpose of collecting the information. Consent may be sought from an individual's authorized representative in certain cases, for example, when an individual is seriously ill, mentally incapacitated, a minor, or has died.

d. If personal information is intended to be used or disclosed for a new purpose not identified during the original collection, and not related to the original purpose of the collection, the consent of the individual must be obtained.

e. Individuals can give consent in many ways. For example:

   i. a form may be used to seek consent, collect information, and inform the individual of the use that will be made of the information. By completing and signing the form, the individual is giving consent to the collection and the specified uses;

   ii. consent may be given orally; or,

   iii. consent may be given through electronic means.

f. An individual may withdraw consent at any time, subject to legal or contractual restrictions and reasonable notice. The Chippewas of the Thames First Nation must stop using the individual's personal information within a reasonable time period and inform the individual of this time period and the implications of such withdrawal;

g. For collection of information of individuals by third parties: Council may require access to the information collected if it can be used for the purposes of serving the COTTFN citizenship. If information identifiable to specific individuals will be made available to COTTFN, the third party must disclose this when collecting the information.

(4) Limiting Collection

a. The Chippewas of the Thames First Nation cannot collect personal information indiscriminately. Both the amount and the type of information collected must be limited to that which is necessary to fulfill the purposes identified.

(5) Limiting Use, Disclosure and Retention

a. The Chippewas of the Thames First Nation may only use or disclose personal information for the purpose for which it was collected, unless:

   i. The use or disclosure of the personal information is consistent with the original collection of the personal information;

   ii. The consent of the individual is obtained; or,

   iii. It is for the purpose of complying with a subpoena or warrant issued or order made by a court, person or body with jurisdiction to compel the production of information or for the purpose of complying with rules of court relating to the production of information.

b. Personal information that has been used to make a decision about an individual must be retained long enough to allow the individual access to the information after the decision has been made.

c. Identifiable personal information must only be used and disclosed if required. For instance, consider if reports, research, or audits/assessments can be done through de-identified or anonymous data.

d. Personal information that is no longer required to fulfill the identified purposes will be destroyed, erased, or made anonymous in accordance with the Chippewas of the Thames First Nation's retention and disposition schedule.

(6) Accuracy

a. The Chippewas of the Thames First Nation shall take all reasonable steps to ensure that personal information that is used to make a decision on an individual is as accurate, up-to-date and complete as possible to minimize the possibility that inappropriate information may be used to make a decision about the individual.

(7) Safeguards

a. Personal information should be protected with appropriate safeguards to ensure only those with a need to know will have access to the records:

   i. For electronic records containing personal information, the records should be protected with controls on the document itself (such as password protection) and other administrative controls, such as restricting access to the electronic repositories in which the record is stored. Personal information should not be emailed 'in the clear' without appropriate protection.

ii. For hardcopy paper-based records, containing personal information, the records should be stored in secure filing cabinets at all times unless being used, and transported in a secure manner if required to be taken offsite.

b. The Chippewas of the Thames First Nation must make its employees, contractors, and volunteers aware of the importance of maintaining the confidentiality of personal information.

c. Care must be used in the disposal or destruction of personal information, to prevent unauthorized parties from gaining access to the information.

(8) Openness

a. The Chippewas of the Thames First Nation must be open about its policies and practices with respect to the management of personal information. Individuals will be able to acquire information about its policies and practices without unreasonable effort. This information must be made available in a form that is generally understandable.

b. The information made available should include:

i. the name or title, and the address, of the Privacy Officer, who is accountable for the Chippewas of the Thames First Nation's policies and practices, and to whom complaints or inquiries can be forwarded;

ii. the means of gaining access to personal information held by the Chippewas of the Thames First Nation; and,

iii. a description of the type of personal information held by Chippewas of the Thames First Nation, including a general account of its use.

(9) Individual Access

a. When requested, an individual must be informed if the Chippewas of the Thames First Nation holds personal information about the individual and provide an account of the use that has been made or is being made of this information and an account of the third parties to which it has been disclosed.

b. The identity of an individual must be authenticated before discussing their personal information with them.

c. When requested, the Chippewas of the Thames First Nation must provide an individual with access to their personal information within a reasonable time and at minimal or no cost to the individual in the presence of the Privacy Officer and/or the Director of the relevant program that is holding the information. The requested information will be provided or made available in a form that is generally understandable.

d. Individuals who are given access to their personal information may:

i. request correction of the personal information where the individual believes there is an error or omission therein;

ii. require that a notation be attached to the information reflecting any correction requested but not made; and,

iii. require that any person or body to whom that information has been disclosed for use for a decision-making process within two years prior to the time a correction is requested or a notation was made be notified of the correction or notation.

e. In certain situations, the Chippewas of the Thames First Nation may not be able to provide access to all the personal information it holds about an individual. Exceptions to the access requirement will be limited and specific. The reasons for denying access will be provided to the individual upon request. Exceptions may include information that:

i. is prohibitively costly to provide;

ii. contains references to other individuals;

iii. cannot be disclosed for legal, security, or commercial proprietary reasons; or,

iv. is subject to solicitor-client or litigation privilege.

(10)Challenging Compliance

a. The Chippewas of the Thames First Nation must ensure that a process exists to receive and respond to complaints or inquiries about its policies and practices relating to the handling of personal information. The complaint procedures will be easily accessible and simple to use.

b. The Chippewas of the Thames First Nation must investigate all complaints. If a complaint is found to be justified, the Chippewas of the Thames First Nation will take appropriate measures, including, if necessary, amending its policies and practices.

F. References and Related Authorities

(1) FMB's Financial Management System Standards

a. Standard 12.6 - Human Resource records

b. Standard 19.0 - Risk Management

c. Standard 23.0 - Records and Information

(2) FMB's Financial Administration Law Standards

a. Standard 21.0 - Records and Information

G. Attachments

None

Appendix A – Document Retention Periods

Record or information	Duration
General Chippewas of the Thames First Nation governance records	
All Chippewas of the Thames First Nation bylaws, amendments to the bylaws, the Chippewas of the Thames First Nation constitution, and membership resolutions	Permanent
Appointments and terms of appointments	Permanent
Applicable legislation, agreements, funding arrangements, council commitments, land codes in force, financial administration codes for oil & gas monies management	Permanent
The Chippewas of the Thames First Nation's Financial Administration Law	Permanent
The Chippewas of the Thames First Nation's Property Taxation Law or By-law	Permanent
The Chippewas of the Thames First Nation's Borrowing Law	Permanent
Minutes from the meetings of the Council and all council committees, annual reports, debenture records and council, committee and membership records, public notices, records of incorporation, corporate seal	Permanent
Legal files and papers	
Customer and supplier contracts and correspondence related to the terms of the contracts	7 years beyond life of contract
Contractual or other agreements (e.g., contribution, impact benefit, trust) between the Chippewas of the Thames First Nation and others and correspondence related to the terms of the contracts	7 years beyond life of the contract
Papers relating to major litigation including those documents relating to internal financial misconduct	5 years after expiration of the legal appeal period or as specified by legal counsel
Papers relating to minor litigation including those documents relating to internal financial misconduct	2 years after the expiration of the legal appeal period
Insurance policies including product or service liability, council and Officers liability, general liability, and third-party liability, property and crime coverage	7 years after the policy has been superseded
Documents pertaining to the purchase, sale or lease of property	Permanent
Documents pertaining to equity investments or joint ventures	Permanent
Human Resources	
Personnel manuals and procedures	Permanent
Organization charts	Permanent

Where there is a pension plan (excluding RRSP plans): Original plan documents; records of pensionable employee service and eligibility; associated personal information including name, address, social insurance number, pay history, pension rate	7 years after the death of the employee or employee's spouse in the case of spousal eligibility
Letters of offer and individual contracts of employment	2 years after termination of the employee
Signed Code of Conduct obligations and signed Conflict of Interest declarations	5 years after termination of the employee
Attendance records	2 years after termination of the employee
Financial information such as payroll history including RRSP contributions, commission and bonus history	5 years after termination of the employee
Medical information	2 years after termination of the employee
Job descriptions	2 years beyond the period to which it applies
Performance assessments	5 years after termination of the employee
Applications, resumes, and correspondence related to individuals not hired	2 years beyond the period to which it applies
Documentation surrounding termination / quit (eg. Exit Interview, Disciplinary action)	10 years after termination of the employee
Financial records	
Operations manuals, procedures, and internal control guidelines	Permanent
Signed annual financial statements and corresponding signed independent auditor reports	Permanent
Internal reports, including but not limited to: Reviews Annual operations report Special purpose reports Internal audit reports	10 years
Accounting documentation, including but not limited to: General ledgers, general journals, financial records and supporting documentation Monthly and quarterly financial statements Monthly and quarterly management reports Month / Quarter / Year-end Financial Closing and Reporting work papers Financial institution account statements and reconciliations Cancelled cheques and cash register tapes Invoices	8 years

Annual budgets Multi-year financial plans	
Asset management documentation, including but not limited to: Tangible capital asset register Reserve fund reports Life cycle planning Capital project budgeting Contract and tendering provisions	8 years beyond completion of the project or asset utilization
If applicable, property taxation related documentation, including but not limited to: Property tax working papers Tax roll Tax filings	8 years
Operational records	
Operations manuals, policies and procedures	Permanent
Original patents, trademarks, and copyrights	7 years after the expiration of the right
Customs documents	7 years
Annual physical inventories	Permanent
Safety committee minutes, inspection reports and related action reports	10 years
Housing records	
Summary chart of applications for rental units	7 years after applications close
Individual applications for rental units	2 years after applications close
Lease agreements and other documents associated with leases (including Notice to Terminate Tenancy)	7 years after tenancy ends
Consultation records (within Treaty, Lands, Environmental Department)	
Traditional land use studies, community surveys and maps	Permanent
Environmental studies or reports with general applicability	Permanent
Maintenance and production reports for completed infrastructure (for any level of concern)	2 years after report is issued
Examples of other consultation documents include (but are not limited to): Regulatory applications and responses to information requests; Environmental impact assessments; Proponent reports; Correspondence between proponents, COTTFN, and other governments (First Nations, municipal, provincial, federal). Document retention based on project classification matrix (and subject to the qualifications below):	
Minimal concerns	2 years after project is completed, cancelled,

	withdrawn or denied by regulatory authorities
Moderate concerns	5 years after project is completed, cancelled, withdrawn or denied by regulatory authorities
Extensive concerns	20 years after project is completed, cancelled, withdrawn or denied by regulatory authorities
The above schedules (under Consultation Records) are subject to the following qualifications: The Treaties, Lands and Environment Department and Consultation staff are under no obligation to dispose of files according to this schedule if they see value in keeping the documents. Public documents without any confidential information (e.g. proponent applications to regulatory bodies) may be recycled without shredding. Other documents will be shredded. If environmental studies or reports by proponents have broader applicability for COTTFN, those documents will be retained permanently. Studies of limited applicability may be disposed of subject to the above schedules. Staff should err on the side of caution when considering the management of written correspondence or meeting notes that document interactions between COTTFN and proponents. Unlike regulatory applications, duplicates of letters and meeting notes may not be available from other sources. At times, proponents may make commitments in letters or meetings that are not repeated elsewhere. Documentation of these types of negotiations, especially with companies that COTTFN may foreseeably deal with again in the future, should be retained for a longer period. This also applies to cancelled or denied projects that may be reintroduced at a later date. Maintenance or production reports that could foreseeably be useful in case of company non-compliance should be retained for longer than 2 years. For example, reports on pipeline integrity digs could be useful in a legal action if there is a breach. Information inputted into software (e.g. Community Knowledge Keeper) may also deviate from the above schedule. All discretionary decisions to retain documents for longer than the scheduled time shall be made by the Consultation Coordinator.	