Statement of Policy and Procedure	
Policy No.	FMB-001; Version 0
Department Ownership	Operations
Issue/Effective Date	November 16, 2019

Qalipu First Nation

Information Management Policy

Approved by Council on November 16, 2019; BCR 04-19-20

Qalipu
FIRST NATION

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 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 the Senior Manager, Senior Financial Officer, Tax Administrator or any other employee of the First Nation designated by the Council as an Officer;
"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 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 First Nation for business purposes or legal obligations, which enable and document decision-making, and support 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 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 First Nation's information systems will support its operational requirements and have appropriate safeguards and monitoring processes in place to adequately protect the 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 First Nation.

C. Scope

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

D. Responsibilities

(1) Council is responsible for:

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

(2) The Senior Manager 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 First Nation.

E. Procedures

(1) **Planning and evaluation**

a. The Council, with the assistance of the Senior Manager and input from information technology staff, will ensure that information systems are developed that support the 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 Senior Manager will seek advice from a qualified external individual or organization.

(2) **Outsourcing**

a. Subject to the Procurement Policy, the Senior Manager 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 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 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 First Nation's information technology systems must be periodically backed-up. Backups will occur incrementally on a daily basis, with full backups on a weekly and monthly basis.

c. Backup drives must be stored in a secure location with access limited to the Senior Manager and limited other staff as appropriate. Ideally, backup drives will be securely stored at an offsite location that is easily accessible to individuals with authorized access.

d. Backup drives will be retained for a period of 6 Weeks minimum before being overwritten or deleted.

(4) **Access management**

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

b. Requests for access to the 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 Senior Manager (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 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:

d. The antivirus program must not be disabled 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;

e. Antivirus files must be updated on the network at a minimum of every two weeks or whenever a new threat is identified.

f. 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 First Nation;

ii. Description and rationale for the new network, hardware, communication and systems software change and how it is consistent the needs of the 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 Senior Manager for substantive changes, minor changes can be approved by Program Directors. For greater certainty substantive changes include software changes, Platform changes, Hardware Changes, and other changes valued above $5000.00.

viii. Communication of changes to First Nation staff as appropriate.

(7) **Monitoring**

a. Only approved and authorized programs will be implemented onto 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 First Nation information systems will be maintained. On a quarterly basis, the internal Computing Specialist 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 tested on a regular basis.

(8) **Ownership and Access of Electronic Mail, Internet Access**

a. It is considered reasonably necessary to maintain or protect the integrity, security or functionality of the Nation's or other computer resources or to protect the QFN from liability;

(i) There is reasonable cause to believe that the user has violated this policy or otherwise misused computing

b. Employees should have no expectation of privacy when utilizing the Nation's computing resources, even if such use is for personal purposes.
c. QFN owns the rights to all data and files in any computer, network, or other information system used in the Nation. QFN owns the rights to all data and files sent or received using any Nation system. It also owns the rights for using the Nation's access to any computer network or software, to the extent that such rights are not superseded by applicable laws relating to intellectual property. The QFN also reserves the right to monitor electronic mail messages (including personal/private/instant messaging systems) and their content. Any and all use by employees of the Internet and of computer equipment used to create, view, or access e-mail and Internet content is also subject to inspection or monitoring by QFN.
d. Employees must be aware that the electronic mail messages sent and received using QFN equipment or Nation-provided Internet access are not private. This includes web-based messaging systems used with such systems or access. All mail messages are subject to viewing, downloading, inspection, release, and archiving by QFN officials at all times.
e. The QFN reserves the right to inspect, without notice, the contents of computer files, regardless of medium, the contents of electronic mailboxes and other computer systems all files stored in private or designated areas of the network or on individual computers or on storage media, systems outputs (such as printouts) and to monitor network communication if:
   (i) An account appears to be engaged in unusual or unusually excessive activity; and
   (ii) It is otherwise required or permitted by law. Additionally, the USER ID and computing services of the individuals involved may be suspended during any investigation of misuse of computing resources.
f. No employee may access another employee's computer, computer files, or electronic mail messages without prior authorization from either the employee or an appropriate QFN official.
g. Employees who wish to maintain their right to confidentiality or a disclosure privilege must send or receive such information using some means other than through the QFN systems or the Nation-provided Internet access. (QIT POLICY,pp. 4-5).

(9) **Confidentiality of Electronic Mail**

a. As noted above, electronic mail is subject at all times to monitoring, and the release of specific information is subject to applicable provincial and federal laws and QFN rules, policies, and procedures on confidentiality.
b. Existing rules, policies, and procedures governing the sharing of confidential information also apply to the sharing of information via commercial software. Since there is the possibility that any message could be shared with or without your permission or knowledge, the best rule to follow in the use of electronic mail for non-work-related information is to decide if you would post the information on the office bulletin board with your signature.
c. It is a violation of QFN policy for any employee, including system administrators and supervisors to access electronic mail and computer systems files to satisfy curiosity about

the affairs of others, unless such access is directly related to that employee's job duties. Employees found to have engaged in such activities will be subject to disciplinary action.

(10) **Electronic Mail Tampering**

a. Electronic mail messages received should not be altered without the sender's permission; nor should electronic mail be altered and forwarded to another user and/or unauthorized attachments be placed on another's electronic mail message.

(11) **Software**

a. The QFN has licensed the use of certain commercial software application programs for business purposes.
b. Third parties retain the ownership and distribution rights to such software. No employee may create, use, or distribute copies of such software that are not in compliance with the license agreements for the software.
c. No game or recreational software is to be loaded on any QFN computer.
d. Violation of this policy may lead to disciplinary action, up to and including dismissal.
e. Installation of any software requires IT staff approval.
f. Employees will be individually liable for any and all damages incurred as a result of violating QFN security

(12) **Policy Statement for Internet/lntranet Browser(s)**

a. The Internet is to be used to further the QFN's mission, to provide effective services of the highest quality to the Nation's members, clients, partners, customers and staff, as well as to support other direct job-related purposes. Internet/lntranet access is provided as a business tool to employees who may use them for research, professional development, and work-related communications.
b. When discussing job duties, the work plan and professional development, each Manager should work with each employee to determine the appropriateness of using the Internet for professional activities and career development.
c. All QFN policies and procedures apply to employees ' conduct on the Internet, especially, but not exclusively, relating to: intellectual property, confidentiality, Nation or Nation related business information dissemination, standards of conduct, misuse of Nation resources, anti-harassment, and information and data security.

(13) **Personal Use**

a. Limited personal use of Internet resources is a special exception to the general prohibition against the personal use of computer equipment and software.
b. Subject to the privacy policy above and the prohibited uses outlined below, the QFN permits limited personal use of staff computers subject to the following:
    i. Personal use will be on an employee' s personal time (before or after regularly scheduled work time, during lunch breaks);

ii. Personal use of computers must not interfere with any work-related activity;
iii. Personal use must not interfere with a co-worker's or client's time where such use is recreational;
iv. The email system should not be used to solicit or persuade either for personal commercial ventures, religious or political causes, outside organizations or other non-work-related solicitations;
v. Participation in social or recreational chat channels and bulletin boards is strictly prohibited;

(14) **Prohibited Uses of the Internet and QFN Computers**

a. Use of QFN computers, networks, and Internet access is a privilege granted by the Nation and may be revoked at any time for inappropriate conduct carried out on such systems, including, but not limited to:
   i. The use or installation of computer games is not permitted on any QFN computers.
   ii. Sending chain letters or participating in any way in the creation or transmission of unsolicited commercial e-mail ("spam") that is unrelated to legitimate Nation purposes;
   iii. Engaging in private or personal business activities, including excessive use of instant messaging and chat rooms;
   iv. Accessing networks, servers, drives, folders, or files to which the employee has not been granted access
b. or authorization from someone with the right to make such a grant;
   i. Making unauthorized copies of QFN files or other Nation data;
   ii. Destroying, deleting, erasing, or concealing QFN files or other data, or otherwise making such files or data
c. unavailable or inaccessible to the Nation or to other authorized users of QFN systems;
   i. Misrepresenting oneself or QFN;
   ii. The use of aliases while using the Internet is prohibited. Anonymous messages are not to be sent.
   iii. Violating the laws, regulations or policies of the federal or provincial government in any way;
   iv. Engaging in unlawful or malicious activities;
   v. Deliberately propagating any virus, worm, Trojan horse, trap-door program code, or other code or file
d. designed to disrupt, disable, impair, or otherwise harm either QFN's networks or systems or those of any
e. other individual or entity;
   i. Using abusive, profane, threatening, racist, sexist, or otherwise objectionable language in either public or
f. private messages;
   i. Sending, receiving, or accessing pornographic materials;

ii. Becoming involved in partisan politics or any other form of politically related activity;
iii. Streaming content that is large and cumbersome (video) and that is also non-work related causing congestion, disruption, disablement, alteration, or impairment of QFN networks or systems;

g. Streaming excessive or extreme content that slows the QFN connectivity thereby lowering or slowing the ability of other employees to do legitimate QFN business or work
h. Maintaining, organizing, or participating in non-work-related Web logs ("blogs"), Web journals, "chat rooms", or private/personal/instant messaging;
    i. Failing to log *off* any secure, controlled-access computer or other form of electronic data system to which
i. you are assigned, if you leave such computer or system unattended;
    i. Using games; and/or
    ii. Defeating or attempting to defeat security restrictions on QFN systems and applications.
j. Using the QFN systems to access, create, view, transmit, or receive racist, sexist, threatening, or otherwise objectionable or illegal material, defined as any visual, textual, or auditory entity, file, or data, is strictly prohibited. Such material violates the QFN anti-harassment policies and is subject to disciplinary action. QFN's electronic mail system, Internet access, and computer systems must not be used to harm others or to violate the laws and regulations of the federal, provincial or the Nation in any way. Use of QFN resources for illegal activity can lead to disciplinary action, up to and including dismissal and criminal prosecution. QFN will comply with reasonable requests from law enforcement and regulatory agencies for logs, diaries, archives, or files on individual Internet activities, e-mail use, and/or computer use.

(15) **Security Standards for Mobile Devices**

a. This policy defines appropriate security measures that must be implemented on Mobile Devices that are used to access the data and resources of the QFN The very features that make mobile computing devices (cell phones, USB drives, laptop computers, etc.) useful (portability, access, connectivity, data storage, processing power) also present security risks to QFN data and technology resources. For example, they can be easily lost, stolen, or misplaced because of their small size. In addition, most Mobile Devices provide weak, if any, authentication mechanisms that can be easily compromised by others or simply disabled by the user.
b. Cellular devices are not considered secure, as they traditionally do not contain options to increase their security. Despite lacking many safeguards, cellular devices today can contain many types of information such as phone numbers and contact information (perhaps contact information that should be kept confidential), email, calendaring functions, photographs, short notes or voice memos, etc.
c. Unauthorized access to confidential information such as passwords or client/member information could have significant legal consequences. Thus, it is critical that Mobile

Devices be used with the same level of concern as exercised when dealing with other individual and organizational confidential materials.

d. All mobile devices with direct connections to the QFN network system or access to a Qalipu e-mail account will require password, auto-lock after 10 minutes of inactivity, and have remote-wipe capabilities. All mobile devices must login to the "Qalipu Guest" network, with the exception of QFN owned laptops, which are permitted on the "Qalipu Wireless" network.
e. This Mobile Devices policy applies to any individual (employee or Council member) issued with and using a QFN Mobile Device. This policy applies to employees or Council members provided with login capabilities for QFN internet and websites regardless of the party issuing the device (i.e. applies when logged in using a personal mobile device). All individuals using Mobile Devices for QFN purposes must comply with this policy.

(16) **Security Standards for Mobile Devices**

a. Keep Mobile Devices with you at all times or store them in a secured location when not in use. Do not leave your Mobile Devices unattended in public locations (e.g. airport lounges, meeting rooms, restaurants, etc.).
b. Mobile Devices that are used to access QFN data and resources must be password protected. The password should block all access to the device until a valid password is entered. The QFN IT department will assist users to set passwords.
c. Mobile Device users shall not permit anyone else to use QFN-owned Mobile Devices for any purpose.
d. Mobile Device users will not install any software onto any QFN-owned Mobile Device except as required for the applications supported by the Mobile Device.
e. Users of QFN-owned Mobile Devices will immediately report the loss, theft, or unauthorized use of their Mobile Device to the IT department.
f. Any mobile device connecting to QFN systems used to access data and resources residing at or belonging to QFN must be cleared of such data prior to the employee's departure from the organization. The IT Department must be informed of the employee's departure and hereby has the authorization responsibility to remove such data before the device is returned to the department or individual. Removal of this data may involve a backup of the device, the device being wiped clean of all data (business and personal), and a best effort device restore of personal data excluding all email messages previously stored on the device.

(17) **Usage and monthly allowable limits for Cell Phones**

a. All QFN cell phone users must adhere to the restrictions regarding usage and monthly limits as set-out in the QFN Finance Policy. Expenditures by individuals that exceed the monthly allowable limit, will be reviewed and discussed to determine if any additional expenses can be recovered by the QFN. The individual cell phone user may be required to pay the QFN for the difference.

(18) **Care and Use of QFN Property and Equipment**

a. Any equipment, machines, computers, cellular telephones and other supplies that are used by employees are to be signed out with the Manager, particularly when such items are taken off site for use. A copy of the authorization forms will be placed in the employee's personnel file.
b. Any equipment broken or destroyed while in the care of an employee (apart from normal wear and tear) will be the responsibility of that employee to repair or replace.
c. In the event of theft, the Manager may review the circumstances to determine responsibility for replacement and to assess which notification procedures are required. Personal use of QFN property or equipment is not allowed. Abuse of this section will lead to disciplinary action.

(19)**Oversight of Information Technology, Management and Computer**

a. Oversight of this Information Technology, Information Management and Computer Use Policy shall be the responsibility of the Senior Manager and the IT Support Specialist and other key staff members that have valid or relevant education surrounding, connection to or involvement with Information Technology which enables them to administer and oversee this policy's adherence and observance.
b. All employees are bound by this Information Technology, Information Management and Computer Use Policy and are expected to abide by the policies herein. Failure to do so will lead to appropriate disciplinary action as presented and defined in the Human Resources Policy or Council Governance Manual. This description is not to be considered exhaustive or all-inclusive.
c. Council may amend this Information Technology Information Management and Computer Use Policy at any time. If amended, all employees will be informed in writing that changes have been approved. Employees will be informed where they can at any time, review a copy of the Policy (revised and amended).
d. If any provision of this Information Technology, Information Management and Computer Use Policy is found invalid, such provision is severable and shall not affect the validity of the Information Techno logy, Information Management and Computer Use Policy as a whole.

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 First Nation for business purposes or legal obligations, which enable and document decision-making, and support 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.

B. Purpose

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

C. Scope

This policy applies to all Council members, members of the Finance and Audit Committee, Committee members, Officers and employees of the 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 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 First Nation.

(2) The Senior Manager is responsible for:

a. Implementing appropriate Recordkeeping practices,

b. Ensure appropriate safeguards of the 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) 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 volunteer 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 volunteers 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. All important activities and decision making processes of the First Nation should be identified, including the records required to support those processes, to ensure accountability, preserve an audit trail, and protect the First Nation from liability.

b. 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.

c. The 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.

d. The 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.

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

f. The First Nation's records shall be legible, written in plain language and adapted to their specific audience.

(3) **Organization and Classification**

a. A Classification plan structure shall be implemented based on the First Nations functions and activities, with records stored in accordance with the activity and/or function that it supports. This Classification plan should be used to support the filing system for both electronic records and hardcopy paper-based records.

b. Records should be subject to a consistent naming convention, with the name of the record including the title, version (v. XX) and date (DD/MM/YYYY).

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. An official Repository shall be identified and designated for each record, in which the record must be stored. The number of record repositories should be limited and be consistent to support the format and type of record.

g. 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. Backups should be taken of all electronic records on a regular basis and stored in a physical location separate from the location of the original records.

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 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).
b. The location of each Department/Program records need to be recorded to ensure that records can be accounted for in the same way that other assets are maintained. Staff should update the record list when records locations are changed. Currently Departmental/Program records are maintained as follows:

(6) **Maintenance and Monitoring**

Department/Program	File Type	Location
Administration Finance	General Correspondence Band Council Activities Financial Human Resource Other	3 Church St., Corner Brook, NL
Membership	Membership Changes Secure Card	3 Church St., Corner Brook, NL 45 Spruce Ave., Glenwood, NL
Education	Student/Client Funding Agency	28 Hardy Ave., Grand Falls-Windsor, NL
Community Economic Development	Employment	3 Church St., Corner Brook, NL 28 Hardy Ave., Grand Falls-Windsor, NL
Health	Call Logs Client	3 Church St., Corner Brook, NL 45 Spruce Ave., Glenwood, NL
Aquatic Resource Management	Research Fishing Permits/Licenses River Guardians Funding Agency	1 Church St., Corner Brook, NL

Cultural Initiatives	General	3 Church St., Corner Brook, NL 1 Church St., Corner Brook, NL

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 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 provincial legislation, but also to ensure continued stakeholder confidence in the 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 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, Committee members, Officers and employees of the 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 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 First Nation; and

b. Program Director(s) are responsible to manage and oversee the First Nation's compliance with privacy requirements; and this policy for any and all files in their care and control.

(2) The Senior Manager is responsible for:

a. Ensuring compliance with the established information privacy policy.

(3) The Program Director(s) is responsible for:

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

b. Ensuring that all the activities of the 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 Program Director(s) 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 First Nation.

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

iv. Conduct periodic reviews of the 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 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. The 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 through electronic means, once their identity is confirmed using reasonable methods.

f. An individual may withdraw consent at any time, subject to legal or contractual restrictions and reasonable notice. The 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.

(4) **Limiting Collection**

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

(6) **Accuracy**

a. The 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 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.

d. Portable storage devices utilized to stored First Nation records will be password protected, and only used for the purposes intended when the data was collected, or if required for law enforcement.

(8) **Openness**

a. The 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 Senior Manager, who is accountable for the 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 First Nation; and,

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

(9) **Individual Access**

a. When requested, an individual must be informed if the 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 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. The requested information will be provided or made available in a form that is generally understandable.

d. Individuals who are given access to, or otherwise have knowledge of, 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 be notified of the correction or notation.

e. In certain situations, the First Nation may not be able to provide access to all the personal information it holds about an individual. In these situations, some information may be redacted or denied in its entirety. Exceptions to the access requirement will be limited and specific. The reasons for denying access or redacting information 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 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 First Nation must investigate all complaints. If a complaint is found to be justified, the First Nation will take appropriate measures, including, if necessary, amending its policies and practices.

5. Membership Database (Ginu)

QMFN has created a Membership Database (Ginu) using information with respect to members of the band. The database contains basic contact information on each member and will be used to generate the Band's official membership and voters list.

(11) **Consent**

a. Unless permitted by law, no personal information is collected used or disclosed without first receiving the concerned individual's consent to do so.
b. Members must give QMFN consent to use your personal information for any other purposes, besides developing and maintaining a membership list and creating the official voters list. You must give QMFN consent before the discloser of information to a third party.
c. Members must acknowledge that they are not entering any information you know is wrong or false. Members must also agree that they are not entering personal information about another member without their permission to do so.
d. If members are the legal guardian or parent (with legal custody status) of a member who is under 18 years of age or have the power of attorney over an adult member with a disability, members may update his/her information if agree to the same terms and conditions for accuracy and legal responsibility to update the information. To be able to enter information on behalf of a minor or an adult member with a disability, you must first sign a parent/guardian consent form and it must be on file with the Indian Registrar Assistant in the QMFN Band Office. To download a copy of the form, see "Membership" under the Programs and Services tab. Then mail/fax it to the QMFN Indian Registrar Assistant. Note: only once the form has been received will access to the minor or the adult member with a disability member database information be granted.

(12) **Website**

a. QMFN provides members and others with general access to our public website. Our web server tracks general information about visitors such as their domain name, time and duration of visit and which pages are being accessed. This information is used to help us:
   a. manage our site;
   b. diagnose any technical problems; and
   c. improve the content of our website.
b. The personal information provided to third parties whose websites have been accessed through links on our website will be protected by the privacy policy of that third party. We encourage everyone to read the privacy policy of every website they visit.

(13) **Receiving information Via Email**

a. When members log on to a personal member information form, there is an option to keep your email address. By inserting an email address, members will be agreeing to give permission to QMFN to send information to you electronically.

(14) **Inquiries and Complaints**

a. When a complaint or dispute regarding any of QMFN's privacy practices is received, an investigation will be initiated. The complexity of the investigation will be dependent on individual complaints or disputes. All investigations will include the documentation of the issue, who has asked it, the date the issue was communicated to QMFN and any response given. All complaints will be responded to as soon as possible. If the initial investigation does not lead to the resolution of the complaint or dispute, QMFN will take all reasonable steps necessary to resolve the issue.
b. If members have any questions or complaints concerning access to personal information or any information included within this policy; members will contact the Senior Manager by sending an email to kgoulding@qalipu.ca

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 First Nation governance records	
All First Nation bylaws, amendments to the bylaws, the 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 First Nation's Financial Administration Law	Permanent
The First Nation's Property Taxation Law or By-law	Permanent
The 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 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	2 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	2 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	2 years beyond the period to which it applies
Applications, resumes, and correspondence related to individuals not hired	2 years beyond the period to which it applies
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 Annual budgets Multi-year financial plans	8 years

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