Upper Nicola

Information Management Policies

To be approved March 19, 2018

Mission Statement:

Upper Nicola is a proud, inclusive Syilx community working together to promote SuxwtxtEm, teach our Captikw and committed to building foundations through En'owkin'wixw.

Vision:

A strong, flourishing community in harmony with our Tmixw.

Upper Nicola

Band Council Resolution

The Council of the **Upper Nicola Band**	BCR Chronological No.: 2018– 03 – 19 – 01
Physical: 2225 Village Road, Douglas Lake, BC **Mailing:** Box 3700, Merritt, British Columbia V0K 1B8	File Reference (if applicable):
Date: **March 19, 2018**	

WHEREAS the Upper Nicola Band approved the Upper Nicola Band Financial Administration Law on March 20, 2014.

WHEREAS the First Nations Finance Management Board provided compliance review of the UNB FAL on March 31, 2014.

WHEREAS Upper Nicola Band has been:
a) Working to implement the UNB Financial Administration Law.
b) Working with Administration to review policies that will support the implementation of the UNB Financial Administration Law.

WHEREAS, Upper Nicola Band is seeking Financial Management System certification and has identified a need to update the Financial Administration Law and policies.

WHEREAS Upper Nicola Band Chief and Council approved the Governance Policy Finance Policy on November 20, 2017.

THEREFORE, BE IT RESOLVED that we accept the following Upper Nicola Band Policies: Information Management.

A quorum for this Band consists of **(4) FOUR**

Chief Harvey McLeod	Councillor Brian Holmes	Councillor David Lindley
Councillor Dennis MacDonald	Councillor Wallace Michel	Councillor Clarine Paul

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 Upper Nicola Band. 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 Band Administrator, Chief Financial Officer, Tax Administrator or any other employee of the Upper Nicola Band 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 the Upper Nicola Band 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 Upper Nicola Band for business purposes or legal obligations, which enable and document decision-making, and support Upper Nicola Band 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 Upper Nicola Band.
“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.

INFORMATION MANAGEMENT

Policy #:	**2. Information Technology**
Date Approved:	Dates of Amendment:
Cross Reference:	

A. Policy

The Upper Nicola Band's information systems will support its operational requirements and have appropriate safeguards and monitoring processes in place to adequately protect the Upper Nicola Band'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 Upper Nicola Band.

C. Scope

This policy applies to all staff involved in the selection, implementation, operations, or ongoing maintenance of the Upper Nicola Band's information systems. This includes the Band Administrator, and information technology staff.

D. Responsibilities

(1) Council is responsible for:

a. Establishing and implementing documented protocols for information technology used by the Upper Nicola Band in its operations.

(2) The Band 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 IT and Communications Coordinator is responsible for:

a. Maintaining the integrity of information systems within the Upper Nicola Band.

E. Protocols

(1) Planning and evaluation

a. The Council, with the assistance of the Band Administrator and input from information technology staff, will ensure that information systems are developed that support the Upper Nicola Band'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 Band Administrator and other managers as needed will seek advice from a qualified external individual or organization.

(2) Outsourcing

a. Subject to the Procurement Policy, the Band 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 outsourced parties are responsible to comply with legal and regulatory requirements, including the protection of confidential and private information;

ii. Access by outsourced parties to Upper Nicola Band information is provided on a 'need to know basis' only.

(3) Data management[A1]

a. Upper Nicola Band is responsible for the protection and accessibility of the work that is completed by its staff. The purpose of this clause is to provide guidelines for the management and access to data, which is critical to effective administration of our programs and services.

b. Upper Nicola Band realizes that this data is to be used with appropriate and relevant levels of access and with sufficient assurance of its reliability in compliance with existing laws, rules and regulations.

c. Upper Nicola Band is the sole owner of the data prepared or acquired by a staff member for use under their job description.

d. Staff will ensure adequate protection and control procedures for data to which they have been granted the ability to create, modify, view, copy, download or delete.

e. Only individuals with proper authorization may access data pertinent to their daily job. IT staff must ensure staff only have access to data they require for their job.

f. The ongoing availability of data is vital to the successful delivery of our programs and services. Data can be destroyed by various means such as systems malfunctions, accidental or even intentional means. Adequate scheduled backups will allow data to be readily recovered as necessary. In order to minimize possible loss or corruption of data, we must ensure that data is adequately backed up by performing at least a minimal data backup periodically using external hard drives, CD-ROMs or other means of offsite storage. Copies of your backup must be stored offsite.

g. 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.

(4) Access management

a. All individuals[A2][A3][A4] requiring access to Upper Nicola Band information systems will have unique user identification. Shared user IDs or passwords will not be permitted.

b. Requests for access to the Upper Nicola Band's network, accounting system, or other access restricted information system (ie. Xyntax) must include a description of an employee's role and rationale for the level of access required. Signed approval must be obtained from the Band Administrator or employee supervisor on the authorization form.

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. Privileged access is restricted to the IT Communications Coordinator and third party for the operating system/network and database. Privileged access to the Xyntax application is restricted to the Chief Financial Officer. [Privileged access may be required for identified databases or programs.]

e. When an individual or contractor is terminated or ends employment with the Upper Nicola Band, their user IDs will be disabled upon notification of termination.

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 will be installed with an antivirus program prior to the computer being given to the staff member.

d. Antivirus files must be updated on the network periodically.

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 is limited to the third-party service provider and those personnel with specific training and authorization to manage the device. Additionally, the firewall and proxy servers must be securely installed.

(6) Change management

Upper Nicola Band has outsourced change management procedures to a third party.

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 Upper Nicola Band;

ii. Description and rationale for the new network, hardware, communication and systems software change and how it is consistent with the needs of the Upper Nicola Band;

(7) Monitoring

a. Only approved and authorized programs will be implemented onto Upper Nicola Band 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 Upper Nicola Band information systems will be maintained. On an annual basis, the Band 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 access.

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

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

(1) **Appendix A** – Access Request Form

INFORMATION MANAGEMENT

Policy #:	**3. Record Information Management**
Date Approved:	Dates of Amendment:
Cross Reference:	

A. Policy

Records are a special form of information that is created, received, and maintained by the Upper Nicola Band for business purposes or legal obligations, which enable and document decision-making, and support Upper Nicola Band 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 Upper Nicola Band to create and acquire; manage; and, protect the integrity of its records that support its decision-making, and support Upper Nicola Band 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 Upper Nicola Band 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 Upper Nicola Band 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 Upper Nicola Band.

(2) The Band Administrator is responsible for:

a. Implementing appropriate Recordkeeping practices,

b. Ensure appropriate safeguards of the Upper Nicola Band's records;[A5]

c. 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) Department Managers are responsible for:

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

(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. Protocols

(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 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 Upper Nicola Band should be identified, including the records required to support those processes, to ensure accountability, preserve an audit trail, and protect the Upper Nicola Band 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 protocols outlined within this policy.

c. The Upper Nicola Band's records shall be legible.

d. Only one copy of each record should be created or collected and the records should be maintained on a shared drive. 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 in accordance with the requirements of this policy.

(3) Organization and Classification

a. A Classification plan structure shall be implemented based on the Upper Nicola Band's 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 (YYYY/MM/DD).

c. Common words such as 'draft' should not be at the start of the title of records, including permanent records.

d. 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.

e. 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 stored on the shared drive 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. All permanent hardcopy records will be scanned and uploaded to the shared drive or to Xyntax.

d. Files containing records that have 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 Upper Nicola Band records shall be retained for the period specified in the records and information retention and disposition schedule, as outlined in Appendix B 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 B** – Document Retention Periods

INFORMATION MANAGEMENT

Policy #:	**4. Information Privacy**
Date Approved:	Dates of Amendment:
Cross Reference:	

A. Policy

Ensuring the privacy of Personal Information provided to the Upper Nicola Band 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 Upper Nicola Band 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 Upper Nicola Band 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 Upper Nicola Band 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 Upper Nicola Band 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 Upper Nicola Band.

(2) The Band Administrator is responsible for:

a. Ensuring compliance with the established information privacy policy.

b. Developing and maintaining standards, policies and protocols that support the objectives of the Upper Nicola Band's privacy program;

c. Ensuring that all the activities of the Upper Nicola Band are conducted in compliance with the established privacy standards, policies and protocols and in accordance with the generally accepted privacy principles. For this, the Band Administrator 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 Upper Nicola Band.

iii. Be accountable for privacy matters within the Upper Nicola Band.

iv. Conduct periodic reviews of the Upper Nicola Band's activities that involve the collection, use, disclosure, retention, and safeguarding of Personal Information.

d. 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;

e. Recommending changes to policies, protocols and practices in response to the issues raised in the complaints; and

f. Responding in writing to 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.

(3) 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. Protocols

(1) 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.

(2) Consent

a. With limited exceptions, the Upper Nicola Band 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 Upper Nicola Band 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.

(3) Limiting Collection

a. The Upper Nicola Band 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.

(4) Limiting Use, Disclosure and Retention

a. The Upper Nicola Band 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 Upper Nicola Band's retention and disposition schedule.

(5) Accuracy

a. The Upper Nicola Band 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. Change forms are available for members to use to update their information as needed.

(6) Safeguards

a. Personal information (HR and payroll files) 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 are stored in a restricted folder on the shared drive and/or in Xyntax (which has user access controls in place).

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 Upper Nicola Band 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.

(7) Openness

a. The Upper Nicola Band 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 Band Administrator, who is accountable for the Upper Nicola Band'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 Upper Nicola Band; and,

   iii. a description of the type of personal information held by Upper Nicola Band, including a general account of its use.

(8) Individual Access

a. When requested, an individual must be informed if the Upper Nicola Band 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 Upper Nicola Band 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 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 Upper Nicola Band 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.

(9) Challenging Compliance

a. The Upper Nicola Band 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 Upper Nicola Band must investigate all complaints. If a complaint is found to be justified, the Upper Nicola Band 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

[A6]Appendix A – Access Request Form

Network / Application Access Request Form

New / Change to User Account

Please complete this form, send it to and copy the applicable department/person

Date: _____ **Location:**

☐ **New Addition** ☐ **Termination** ☐ **Change**

☐ **New Employee** ☐ **Existing Employee** **Employee Number:**

☐ **New Contractor** ☐ **Existing Contractor** **Vendor Number:**

Hire Date: _____

Required Date: _____

Replacing (Position or Person): _____

Account for (Employee's Full Name): _____

Email (If Existing Employee): _____

Phone #: _____

Job Title: _____ **Department:**

Temporary position: No ☐ **Yes** ☐ **If YES – Expiry Date:**

Personal Computer Required: No ☐ **Yes** ☐ **If NO - Is common computer being used?_____**

Desk Location: _____ **Computer Name:_____**

Cell Phone Required: ☐ **No** ☐ **Yes**

Network Account: _____

List Shared Drives that User Requires Read/ Write access to:

_____

Email Access required? ☐ **No** ☐ **Yes**

List of Email Groups to be a Member of:

_____

Application Access:

Application 1 Role/Rights: _____

Application 2 Role/Rights: _____

Application 3 Role/Rights:

Additional Comments:_____

Requested By (Name, Date): _____

Authorized By (Name, Date): _____

To be completed by IT Department:

Network Username:_____

Email Address: _____

Cell phone:_____

BB/ Android/ Apple ID: _____

Location/ Desk Extension:_____

Computer Name:_____

Application Usernames:_____

Other requirements: _____

Appendix B – Document Retention Periods

Record or information	Duration
General Upper Nicola Band governance records	
All Upper Nicola Band bylaws, amendments to the bylaws, the Upper Nicola Band 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 Upper Nicola Band's Financial Administration Law	Permanent
The Upper Nicola Band's Property Taxation Law or By-law	Permanent
The Upper Nicola Band'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 Upper Nicola Band 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