Sipekne’katik

Information Management Policy and Procedures

Chief and Council Approved March 31, 2021

SIPEKNE'KATIK

Approved by Chief and Council March 31, 2021.

Signature print name	Signature print name
Signature print name	Signature print name
Signature print name	Signature print name
Signature print name	Signature print name
Signature print name	Signature print name
Signature print name	Signature print name
Signature print name	Signature print name

Date Approved by Council: March 31, 2021 (BCR number) Motion #3 of Meeting on March 31, 2021

Contents

1. DEFINITIONS

“Budget”	a plan or outline of expected money and spending over a specified period
“Capital Assets”	tangible capital assets (physical assets) such as buildings, land, and major equipment
“Capital Project”	the construction, rehabilitation or replacement of Sipekne’katik’s capital assets and any other major capital projects in which Sipekne’katik or its related entities are investors
“Classification”	process of categorizing records in an organized way
“Committee”	group of people appointed by Council for advising Council or conducting decision-making activities assigned by Council until or unless they are suspended or disbanded by Council
“Conflict of Interest”	situation of personal gain, or perceived personal gain, at the expense of others
“Contract”	legally binding agreement between two parties
“Control”	policy, procedure, or process put in place to manage Sipekne’katik’s administration
“Council”	elected or appointed official representatives of Sipekne’katik that includes Chief, Councillors and the equivalent terminology used by Sipekne’katik elected pursuant to the Indian Act
“Direct Supervisor”	employee responsible for managing and overseeing the work and development of other staff
“Director of Administration (DOA)”	member of Senior Management Group who leads the day to day administration of Sipekne’katik and is the direct supervisor to department managers. This position is the link between the Director of Operations and the Managers as well Sipekne’katik members
“Director of Finance (DOF)”	means the employee who manages the day to day financial transactions of all departments and supervises the employees in the Finance Department. This position is a member of the Senior Management Group, reports to the Executive Finance Officer and is the first point of contact for Program Managers/Directors regarding financial transactions.

“Director of Operations (DOO)”	means the most senior member of the Senior Management Group who directly reports to Chief and Council. This position leads the vision, mission and strategic priorities of Sipekne’katik. The Director of Operations works closely with and may delegate responsibilities to the Director of Administration.
“Executive Financial Officer (EFO)”	means the most senior Financial position for Sipekne’katik, responsible for overseeing all financial activities, including Budget and Financial Reporting. The EFO has signing authority for Sipekne’katik, as approved by Council and is responsible to report on financial matters to Chief and Council regularly. The EFO is a member of the Senior Management Group and works closely with and may delegate some responsibilities to the Director of Finance. “Financial Statement” formal record of all money and property of Sipekne’katik within a specific period
“Information”	knowledge received and any documented material regardless of source or format
“Information Security”	way Sipekne’katik protects information from unauthorized access, use, modification, or destruction
“Investment”	an asset or item bought with the hope that it will gain value or provide income in the future
“Local Revenues”	term used to describe property taxes under *First Nations Fiscal Management Act*
“Misconduct”	breach of the Sipekne’katik’s Financial Administration Law including conflict of interest provisions, code of conduct, Council-approved policies and administrative procedures
“Officer”	means an employee of Sipekne’katik designated by Council to perform official duties as outlined in Sipekne’katik’s Financial Adminsitration Law and is limited to such duties assigned to the Director of Operations, Director of Administration, Executive Finance Officer, Tax Administrator and any other employee of Sipekne’katik government designated by the Council to perform similar duties

“Organization Chart”	visual representation of the different positions in Sipekne’katik that clearly shows reporting relationships (who reports to who)
“Personal Information”	information about a specific individual. In addition to common items such as an individual’s name, gender, physical characteristics, address, contact information, identification and file numbers - it also includes criminal, medical, financial, family and educational history as well as evaluative information and other details of an individual’s life
“Privacy Protection”	rules a Sipekne’katik government puts in place to collect, create, use, share/disclose, retain, protect and dispose of the Personal Information that it needs for its administration
“Purchasing”	buying an asset or item. Also referred as “procurement” per the Sipekne’katiks Financial Management Board Standards
“Record”	information created, received, and maintained by the Sipekne’katik for operational purposes or legal obligations. A record may be electronic, or hardcopy paper based
“Recordkeeping”	how an organization creates, obtains, and manages records
“Risk”	possibility of a loss or other negative event that could threaten the achievement of Sipekne’katik’s goals and objectives
“Special Purpose Report”	financial report on a specific activity
“Tax Administrator”	person responsible for managing the local revenues and local revenue account on a day-to-day basis, if Sipekne’katik is collecting local revenues
“Virtual Private Network”	VPN is a way to use public telecommunication infrastructure, such as the internet, to provide remote offices or individual users with secure access to the Sipekne’katik’s virtual network

2. INFORMATION TECHNOLOGY

POLICY

Policy Statement

It is Council's policy to establish a process around Sipekne'katik's information systems to support its operational requirements and have appropriate safeguards and monitoring processes in place.

Purpose

The purpose of this policy is to make sure that Sipekne'katik's information is adequately protected and that the information system has integrity to maintain and support the strategic and operational requirements of Sipekne'katik.

Scope

This policy applies to all staff involved in the selection, implementation, operations, and ongoing maintenance of Sipekne'katik's information systems.

Responsibilities

Council is responsible for:

- approving the information technology policy used by Sipekne'katik

The Director of Operations is responsible for:

- ensuring that controls are in place over information technology, whether performed by an internal staff member or outsourced
  establishing and implementing documented procedures for information technology used by Sipekne'katik

The Director of Administration is responsible for:

- monitoring the performance of internal and/or external information technology professionals

The IT Manager (internal and/or external) is responsible for:

- maintaining the integrity of information systems within Sipekne'katik

ADMINISTRATIVE PROCEDURES

Procedures

2.1 Planning and Evaluation

The Director of Operations, with input from IT Manager (internal and/or external), will make sure that information systems are developed that support Sipekne'katik's strategic plan and operations.

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

2.2 Outsourcing

Subject to the purchasing section of the finance policy, the Director of Operations, in consultation with IT Manager and any other relevant department Managers/Directors, 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.

Specific items which should be included in the procurement of IT services and final contract with the chosen provider include:

- a requirement that the service provider submits regular reports of all work performed on Sipekne'katik's information systems
- a requirement that outsourced parties are responsible to comply with legal and regulatory requirements, including the protection of confidential and private information
- access by outsourced parties to Sipekne'katik information is provided on a 'need to know basis' only

2.3 Data Management

Subject to the Records Information Management section of this policy, data retention allows access to appropriate data to specified personnel where required, depending on the type of data retained.

All sensitive, valuable, or critical data stored on Sipekne'katik's information technology systems must be regularly backed-up.

The back-up of the server/shared drive is completed by the external consultant and stored off-site. Accounting information is automatically backed up by the accounting software provider each night and stored off site.

2.4 Access Management

All individuals requiring access to Sipekne'katik information systems will have unique user identification. Employees are required to change their password regularly, when prompted by the system. Shared user IDs or passwords will not be permitted.

Requests for access to Sipekne'katik's network, accounting system, or other access restricted information system must include a description of an employee's role and rationale for the level of access required. Signed approval must be obtained from the Executive Finance Officer for accounting system and the Director of Administration for all other information systems.

User ID and password are required for access to the network and other critical programs/areas such as the accounting system.

Individuals will be given revocable 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.

When an employee's employment is terminated, their user IDs must be disabled immediately.

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.

Only Sipekne'katik's IT Manager is authorized to provide any downloads of any software onto any computer or system of Sipekne'katik.

The following applies with respect to Sipekne'katik computers:

1. Computers belonging to Sipekne'katik are not to be used for personal use;
2. Internet use is only to be conducted during work hours and only for work related activities. Internet use brings the possibility of breaches to the security of confidential organizational information. Internet use also creates the possibility of contamination to Sipekne'katik system via viruses or spyware.
3. Individuals using Sipekne'katik equipment to access the Internet are subject to having activities monitored by system or security personnel. **Use of this system constitutes consent to security monitoring, and employees should remember that most sessions are not private.**
4. No personal information shall be placed onto the computer;

The Sipekne'katik email address is to be used for Sipekne'katik business only and not for personal use.

Employees are only permitted to use Sipekne'katik assigned emails. No personal email addresses can be used by employees during work to conduct Sipekne'katik business. Note: if an employee uses their personal email during work and/or to conduct Sipekne'katik business, those emails automatically become the property of Sipekne'katik.

2.5 Information System Security

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

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

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

- 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
- antivirus files must be updated on the network regularly or whenever a new threat is identified

Staff are required to report to the IT professional and their immediate supervisor if they receive any spam emails, suspect they have a virus, have been hacked, or any other potential security breach.

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:

- firewall and proxy servers must be securely installed
- detailed firewall logs must be maintained
- alerts must be raised if important services or processes crash

2.6 Change Management

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

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:

- data structure is consistent with the needs of Sipekne’katik
- description and rationale for the new network, hardware, communication and systems software change and how it is consistent with the needs of Sipekne’katik
- it falls within the approved budget
- assessment of any risks involved with the change
- roll-back considerations
- implementation considerations
- description of required testing
- approval from the relevant Officer
- communication of changes to Sipekne’katik staff as appropriate
- changes to the accounting software (i.e. new system or major changes to the current system set-up) require authorization from the Council and the Executive Financial Officer with consultation and communication with the Finance and Audit Committee. Changes such as

the addition/deletion/ modification of general ledger accounts, customer/member accounts, or vendor accounts require approval from the Executive Financial Officer or designate.

2.7 Monitoring

Only approved and authorized programs will be implemented onto Sipekne'katik's information management systems. The IT Manager will conduct periodic reviews of the workstations and the system to monitor compliance with this requirement.

A log of staff, their user IDs, and their access levels within Sipekne'katik's information systems will be maintained. On a periodic basis, the IT Manager, in consultation with the Director of Administration will review the log to make sure users and the associated access rights are appropriate. Access rights that will be monitored include the following:

- user access management (i.e. the accounting system)
- third party access (i.e. outsourced information technology professionals)
- network access and file sharing
- remote and VPN access
- email

Network system performance is monitored on a regular basis.

The firewalls must be monitored regularly.

3. RECORD INFORMATION MANAGEMENT

POLICY

Policy Statement

It is Council's policy to establish a process around the creation, collection, organization, retention, and safeguarding of records for long term availability, understandability and usability.

Purpose

The purpose of the policy is to provide guidance on effective recordkeeping practices to create, manage and protect the integrity of Sipekne'katik's records that support its decision-making, reporting, performance and accountability requirements.

Scope

This policy applies to all Council members, members of the Finance and Audit Committee, Officers and employees of Sipekne'katik 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 Sipekne'katik regardless of format (i.e., both electronic and paper records).

Responsibilities

Council is responsible for:

- approving the policy for records management

The Director of Operations is responsible for:

- establishing and implementing documented procedures for records management
- implementing appropriate recordkeeping practices
- make sure appropriate safeguards of Sipekne'katik's records

The Director of Administration is responsible for:

- ensuring compliance with the established records retention and disposition schedule and overseeing the disposition process
- ensuring that employees and any contractors, agents, or volunteers performing services on behalf of the Council are fully knowledgeable of their responsibilities as they relate to recordkeeping practices

Employees, contractors, agents, and volunteers are responsible for:

- complying with the established policy
- immediately reporting to their supervisor any potential breach related to compliance with the recordkeeping policy

ADMINISTRATIVE PROCEDURES

Procedures

3.1 Accountability

Each record will have a designated employee that makes sure the recordkeeping framework outlined in this policy is applied to the record. All employees, contractors, agents, or volunteers that are in custody of a record must make sure it is managed in accordance with this policy. Any individual who breaches this policy may be subject to progressive discipline in accordance with Sipekne'katik's Human Resources Policy.

Permanent records such as policies and procedures will be reviewed and updated by the Director of Operations on a regular basis.

Records under the safekeeping of a departing employee, contractor, agent, or volunteer 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 location the records are kept, and required safeguards.

All records produced, used, or received by Sipekne'katik remain the property of Sipekne'katik.

3.2 Creation and Collection

Key activities and decision-making processes of Sipekne'katik should be identified, including the records required to support those processes, to ensure accountability, preserve an audit trail, and protect Sipekne'katik from liability.

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

The record will contain information necessary to achieve the objectives for which each record is created and will be limited to only what is necessary to achieve those objectives.

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

Sipekne'katik's records will be legible, written in clear language and adapted to their specific audience.

3.3 Organization and Classification

Records stored in accordance with the activity and/or function that it supports.

The title of the document should be short and descriptive. The title should include the date when appropriate.

An official storage location will be identified and designated for each record. The number of storage locations should be limited and be consistent to support the format and type of record.

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

Whenever possible, no information should be saved on the individual's personal computer (desktop). Instead, all electronic records should be stored on the personal or shared drive which is saved on the server. Confidential information stored in a share drive should only be stored in a folder that has limited access to individuals who are privy to that information.

3.4 Maintenance, Protection and Preservation

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

Backups will be taken of all electronic records on a regular basis and stored off-site by the IT Manager or external provider.

The Xyntax server is backed up every night.

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 protect their long term availability.

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.

Confidential records should be protected with appropriate safeguards to make sure only those with a need to know will have access to the records:

- 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 storage location in which the record is stored
- for hardcopy paper-based records, confidential records will be stored in secure filing cabinets at all times unless being used, and transported in a secure manner if required to be offsite

3.5 Retention and Disposition

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

Attachments

1. Document Retention Periods

DOCUMENT RETENTION PERIODS

Record or information	Duration
General Sipekne'katik governance records	
Sipekne'katik laws, bylaws, legislative amendments, regulations, codes, directives, constitution, and membership resolutions	Permanent
Appointments and terms of appointments	Permanent
Agreements, funding arrangements, Council commitments	Permanent
Council meeting minutes, Council committee meeting minutes, annual reports, debenture records, 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 Sipekne'katik 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 related to the purchase, sale or lease of property	Permanent
Documents related 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	Minimum 2 years after termination of the employee
Signed Code of Conduct obligations and signed Conflict of Interest declarations	Minimum 2 years after termination of the employee
Attendance records	Minimum 2 years after termination of the employee
Financial information such as payroll history including RRSP contributions, commission and bonus history	Minimum 2 years after termination of the employee
Medical information	Minimum 2 years after termination of the employee
Job descriptions	Minimum 2 years after termination of the employee
Performance evaluations and/or Progressive Discipline documentation	Minimum 2 years after termination of the employee
Applications, resumes, and correspondence related to individuals not hired (recruitment files)	Minimum 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 • special purpose reports • internal audit reports	Minimum 10 years unless otherwise specified by authoritative bodies
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 working papers • financial institution account statements and reconciliations	Minimum 8 years unless otherwise specified by authoritative bodies

• cancelled cheques and cash register tapes • invoices • annual budgets • multi-year financial plans	
Asset management documentation, including but not limited to: • tangible capital asset register • reserve fund reports • life cycle planning • capital project budgeting • contract and tendering provisions	Minimum 8 years beyond completion of the project or asset utilization unless specified by authoritative bodies
If applicable, property taxation related documentation, including but not limited to: • property tax working papers • tax roll • tax filings	Minimum 8 years unless specified by authoritative bodies
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
Backup drives	
Backup drives before being overwritten or deleted.	3 months
All Sipekne’katik Records	
As a result of the forensic audit completed in 2013, ALL records of Sipekne’katik must be retained	15 years from 2013
Sipekne’katik Health Records	

4. INFORMATION PRIVACY

POLICY

Policy

It is Council's policy to establish a process around ensuring the privacy of personal information provided to Sipekne'katik in compliance with legislative requirements such as those outlined in the Personal Information Protection and Electronic Documents Act or similar federal and provincial legislation.

Purpose

The purpose of this policy is to provide guidance on the implementation and maintenance of appropriate information privacy practices within Sipekne'katik related to the collection, use, disclosure, retention, and safeguarding of personal information.

Scope

This policy applies to all Council members, members of the Finance and Audit Committee, Officers and employees of Sipekne'katik 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 Sipekne'katik regardless of format (i.e., both electronic and hardcopy paper records).

Responsibilities

Council is responsible for:

- approving and complying with the policy for privacy and the management of personal information

The Director of Operations is responsible for:

- establishing and implementing documented procedures for privacy and the management of personal information
- recommending changes to policies, procedures and practices in response to the issues raised in the complaints

The Director of Administration is responsible for:

- designating an employee to manage and oversee Sipekne'katik's compliance with privacy requirements and this policy
- ensuring compliance with this policy
- 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 supervisor and, where warranted, to Council

- responding in writing to the requests for access to, and correction of personal information submitted by employees and community members within 10 business days from the date of the receipt

The designated employee who manages and oversees information privacy function is responsible for:

- developing and maintaining standards, policies and procedures that support the objectives of Sipekne'katik's privacy program
- making sure that all the activities of Sipekne'katik are conducted in compliance with the established privacy standards, policies and procedures and in accordance with the generally accepted privacy principles. For this, the employee will:
  - provide training and awareness on privacy protection
  - make sure 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 Sipekne'katik
  - act as an expert resource on privacy matters
  - conduct periodic reviews of Sipekne'katik's activities that involve the collection, use, disclosure, retention, and safeguarding of personal information

Employees, contractors, agents, and volunteers are responsible for:

- complying with the established policy
- immediately reporting to their direct supervisor any privacy breaches

ADMINISTRATIVE PROCEDURES

Procedures

4.1 Accountability

The Director of Operations, or designate, will make sure the principles outlined in this policy are implemented.

4.2 Identifying Purpose

The purposes for the collection of personal information should be communicated to individuals at or before the time of collection, either verbally or in writing. 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.

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

4.3 Consent

With limited exceptions, Sipekne'katik must obtain consent, verbal or written, 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 used and disclosed.

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.

Personal information can be collected, used, or disclosed without the knowledge and consent of the individual in only limited circumstances, such as legal or security reasons which may make it impossible or impractical to seek consent.

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.

Individuals can give consent in many ways. For example:

- 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
- consent may be given orally (the collector should document in writing the details of the oral consent received)
- consent may be given through electronic means

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

4.4 Limiting Collection

Sipekne'katik cannot collect personal information unethically. Both the amount and the type of information collected must be limited to that which is necessary to fulfill the purposes identified.

4.5 Limiting Use, Disclosure and Retention

Personal information will only be used or disclosed for the purpose for which it was collected, specifically:

- consistent with the original collection of the personal information
- when consent of the individual is obtained
- for 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

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.

Identifiable personal information must only be used and disclosed if required.

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

4.6 Accuracy

Sipekne'katik will take all reasonable steps to make sure 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.

4.7 Safeguards

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

- 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 storage location in which the record is stored
- 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

Sipekne'katik must make its employees, contractors, and volunteers aware of the importance of maintaining the confidentiality of personal information.

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

4.8 Openness

Sipekne'katik must be open about its policies and practices with respect to the management of personal information. Individuals will be able to easily acquire information about its policies and practices, including all policies and practices that comprise the Financial Management System. This information must be made available in a format that is generally understandable.

The information made available should include:

- the name or title, and the address, of the designated employee overseeing information privacy, who is accountable for Sipekne'katik's policies and practices, and to whom complaints or inquiries can be forwarded
- the means of gaining access to personal information held by Sipekne'katik

4.9 Individual Access

When requested, an individual must be informed if Sipekne'katik 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.

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

When requested, Sipekne'katik 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. All access to personal information will only be conducted on-site in the presence of the appropriate Program Director/Manager or designated personnel. Original copies will remain the record of Sipekne'katik.

Individuals who are given access to their personal information may:

- request correction of the personal information where the individual believes there is an error or omission therein
- require that a notation be attached to the information reflecting any correction requested but not made
- require that any person or body to whom that information has been disclosed for use for a decision-making process, within a reasonable time that a correction or notation is requested, be notified of the correction or notation

Individuals who are given access to their personal information may not, under any circumstance, make a correction to the original record. Requests for corrections must be made in writing to the Director of Administration.

In certain situations, Sipekne'katik 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:

- contains references to other individuals
- cannot be disclosed for legal, security, or commercial proprietary reasons
- is subject to solicitor-client or litigation privilege or investigation
- cannot be accessed as they are stored at a separate location (ie. ISC office)

4.10 Challenging Compliance

Sipekne'katik will make sure 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. Please consult the Director of Administration (members) or direct supervisor/Manager (employees) if you would like additional information on this process.

If a complaint is found to be justified, Sipekne'katik will take appropriate measures, including, if necessary, amending its policies and practices.