Information Management Policy

Approved by Chief and Council: May 11, 2021

Implementation Date: May 11, 2021

Band Council Resolution Number: 51
Band Council Resolution Date: 05/11/2021
Last Amended: 05/11/2021

Table of Contents

Appendices

1) INTRODUCTION AND PURPOSE

1.1) The Government of Peguis First Nation, elected by its membership, is responsible for programming and service delivery, policy making and decision making on behalf of and for the benefit of the Band membership it represents and the community of Peguis First Nation.

1.1.1) The Government of Peguis First Nation, as elected officials, are responsible and accountable to the membership of Peguis First Nation.

1.1.2) Peguis First Nation, along with its government, receives financial resources from Indigenous Services Canada (formerly Indigenous and Northern Affairs Canada) the Province of Manitoba and through local revenue generation.

1.1.3) The mission of the government of Peguis First Nation is to work with the Band's membership, the community, and various levels of government to help grow and enhance the community as it moves along a path to prosperity and sustainability.

1.2) Purpose

This *Information Management Policy* has been established and written under the authority of the Financial Administration Law (FAL), enacted by the Government of Peguis First Nation in May 2016, and under the direction, guidance, and authority of the Government of Peguis First Nation, and in conjunction with the *Governance Policy* and the *Finance Policy*.

1.2.1) The purpose of this *Information Management Policy* is to help guide the Peguis First Nation government, its administration and staff plan how its information will be used, maintained, kept safe and how users of the system may access it.

1.2.2) This *Information Management Policy* will also serve the purpose of outlining the importance of the Administration along with Chief and Council in planning for information management and how each body contributes to the efficient and effective management of the government's operations and managing the resource available to it.

1.2.3) This *Information Management Policy* will do this by providing guidance in the following key areas:

1.2.3.1) By outlining the roles and responsibilities of the staff, the Administration and the government of Peguis First Nation in information management.

1.2.3.2) It will outline policy, tools and resources that are available, including the development of business plans, and various committees to help guide the decision-making surrounding activities or transactions that, by their very nature, are risky, including interest rate exposure and disaster management.

1.3) This *Information Management Policy* is not intended to deal with and address all possible types of information management issues that may face the Peguis First Nation and its Government.

1.3.1) This policy is therefore meant to be a guideline and to set forth expectations of how and when, Peguis First Nation's Government can and should take reasonable steps to plan for and decide how the information it collects, and processes might be used.

2) DEFINITIONS

The Government of Peguis First Nation – shall be referred to as "Chief and Council" throughout the remainder of this Policy. The Chief and Council of Peguis First Nation is made up of seven (7) members, elected by membership once every four (4) years. Chief and Council is currently comprised of one (1) elected Chief and six (6) elected Councillors.

Financial Administration Law- a Law enacted by Chief and Council on behalf of the Peguis First Nation, to allow for greater transparency in its accounting and financing, in the way it reports to its membership and its funders, increased controls on resource use. It will hereinafter be referred to as FAL.

Indigenous Services Canada – shall be referred to as ISC throughout the remainder of this Policy. ISC is the federal government department that provides for the delivery of funding services to First Nations, Metis and Inuit populations in Canada living both on and off Reserves in Canada

The First Nation – for the remainder of this Policy will refer to the membership of Peguis First Nation- of speaking directly of the membership.

PFN Employees- In speaking to, of, or about the Peguis First Nation's employees, they will be referred to throughout the remainder of this Policy as PFN employee(s).

PFN Management- PFN employees hired, directly or indirectly, by Chief and Council and which Chief and Council may hold responsible and accountable for the Operations and Performance of Departments which constitute the functional areas of the Government. This can be interpreted to mean: Directors, Managers and/or Supervisors, or their designates, as may be named from time to time.

Senior **Management-** PFN employees that hold the position/role/level of responsibility that make her/him either the Chief Operating Officer or the Chief Financial Officer, or both as the case may be from time to time.

- In relation to financial administration or the delegation of financial authority on behalf of Chief and Council, as the case may be, in this policy, the reference to Senior Management, can be taken to mean the ***Chief Financial Officer*.**

- In relation to operational administration, or the delegation of operational authority on behalf of Chief and Council, as the case may be, in this policy, the reference to Senior Management can be taken to mean the ***Chief Operating Officer*****.**
- When both the ***Chief Operating Officer*** and the ***Chief Financial Officer*** are referenced collectively and together as one person, they will be referred to as **Executive Management**.

Risk- The possibility that a negative event will happen.

Risk Management- Is hereby defined as the process used to plan for negative events and how best to avoid them or to minimize the exposure, or the effect, the negative event may have.

Information- knowledge received or documented material regardless of source of format.

Information Management- will hereby be defined, and for purposes of this policy come to mean; the cycle of organizational activity concerning the acquisition of information from one or more sources, how it is maintained and eventually accessed, processed and distributed to those that require it, and then eventually how it will be disposed of.

Wisdom- will be taken to mean and will come to mean throughout this policy as the application of knowledge.

*** The above list of definitions is not meant to be exhaustive, however specific to this policy. For all interpretations or definitions of words or phrases, or terminology that might not be addressed in the above list, that might be used throughout this policy, such as nepotism, please refer to definitions in other Policies, such as the Human Resources and Procedure Manual that have been implemented by Chief and Council.*

3) DISTRIBUTION AND APPLICABILITY OF THIS POLICY

This policy is intended for use and distribution to the following users within Peguis First Nation:

3.1) In their governance capacity for Peguis First Nation, and to assure Chief and Council that effective policy has been developed and implemented which ensure a sound organizational decision-making system exists, and that Chief and Council's ability to govern and make decisions for the First Nation is assured.

3.1.1) As Chief and Council are elected officials and are not considered employees of the First Nation, or for purposes of this *Information Management Policy*, users, certain parts of this policy shall not pertain to them.

3.2) Peguis First Nation's Chief Financial Officer (CFO) and her/his Finance Department to provide it with tools necessary to ensure the stewardship and proper use of the First Nations' resources, as charged by Chief and Council and the FAL, are met and carried out

and that any financial risk the First Nation may be exposed to is identified and managed out as much as possible.

3.2.1) In distributing this policy to the department, the Finance department has been given the authority, through both Chief and Council and the FAL to enforce, if necessary, and carry out the terms set out in this policy, and the requisite authority to enforce and ensure Chief and Council's direction is carried out as set forth in Band Council Resolutions, Minutes of Chief and Council Meetings or Letters of Direction from Chief and Council.

3.3) Peguis First Nation's Chief Operating Officer (COO) for the same underlying reasons as distribution to the Finance Department, namely so that she/he may follow the terms and conditions as set forth in this *Risk Management Policy* as she/he implement the Direction and Goals of Chief and Council through its operations.

3.4) The Peguis First Nation Information Technology (IT) department so that it might carry out the implementation, maintain and any enforcement of this policy, that may from time to time be necessary.

3.5) PFN Employees so they may know how the Chief and Council and their administration plan to use, maintain and keep current their Information Management System.

3.6) PFN's Management, namely "the Directors" so they may effectively and efficiently manage the Human Resources available to their department and their departmental budgets and manage how those same employees may be governed in relation to the management of Information available to the Administration.

4) INFORMATION MANAGEMENT

4.1) Throughout this policy information management shall be limited in reference to the definition as outline in Section **2)** of this policy.

4.2) Information shall be limited in reference to its meaning as set out in Section **2)** of this policy.

4.2.1) Should the definition or use of either Information or Information Management change or be modified, or taken to mean something different, it will be defined in that section along with its applicability.

5) RECORD KEEPING AND MANAGEMENT

5.1) The Peguis First Nation, through its Administration has certain key activities and decision-making processes that require documentation which supports those processes,

to ensure there is accountability in the First Nation's record keeping processes, and that it will effectively manage and steward those documents.

5.1.1) A record will come to mean a piece of information, that at its time of collection should be used, or could have been used to support Chief and Council's business purposes or other legal obligations or that enabled decision-making by Chief and Council or its Administration, as the case may be.

5.1.2) If a piece of information is determined to be a record, or to form part of the book of record, the information shall the be considered to be a record and will be collected, recorded and maintained according to this policy.

5.2) The records will contain information necessary to easily extract what the objective(s) of each record created is and what, if anything, it will be limited to.

5.3) To facilitate ease of retention, collection, classification, organization, all records will contain information about one (1) function or activity.

5.3.1) The First Nations records will be kept and recorded in a legible fashion and will be written in plain language.

5.3.2) The First Nation shall only keep and maintain one (1) record of the information collected. Should there be more than one (1) copy on file, the additional copies should be disposed of in accordance with this policy.

5.4) Employees, as part of her/his responsibilities of employment, may from time to time, be charged with collecting or maintaining records on behalf of the First Nation.

5.4.1) Therefore, it will be incumbent upon the employee(s) to ensure that record collection and management is done so in accordance with this policy.

5.4.2) Permanent records, such as policies and procedure manuals are subject to periodic review and updates. These records will be kept by the COO or her/his designate.

5.4.3) Any records that are the responsibility of employees exiting the department or the First Nation's employment will be required to transfer the knowledge of the record and the record to an employee designated by her/his Program Director.

6) ORGANIZATION OF RECORDS

6.1) Records will be organized according to this policy and will be done so in the most efficient and effective manner possible.

6.2) Records will be subject to a consistent naming convention and strategy, consisting of at minimum, the name of the record, the date of the record and the title of the record.

6.3) All records, should be shared, re-used, and made accessible to the greatest extent made possible by this policy or by best practices, legal standards, and security practices.

7) RETENTION AND STORAGE OF RECORDS

7.1) The Peguis First Nation, its government and its administration shall keep, make available and maintain an accurate (book of) record for planning, forecasting, institutional memory and for reasons of accountability.

7.2) All hard copy and printed materials forming the record will be protected and stored in an appropriate storage location that will allow for their long-term preservation, comprehension and use.

7.3) All electronic records, including journal entries (for the accounting book of record) will be saved, stored and otherwise "backed-up" and maintained at a location that is not the Peguis First Nation, and which is separate from its original records.

7.4) All confidential information, including information that may contain personal information about an individual(s), should be marked as CONFIDENTIAL and treated as such.

7.4.1) Once these confidential records are processed for retainment, they should only be accessed by those individuals that "need to know."

7.4.1.1) The "need to know" basis will be defined by Chief and Council, the COO, and in the case of financial information, the CFO.

7.4.2) To access this confidential information, or any confidential information, once retained, the individual requesting the information, regardless of who that individual might be, will require approval, in writing from Executive Management.

7.4.3) Once the confidential information is approved for release, and prior to receiving said information, the individual making the request must sign a release of information, including conditions of its use and any consequences that might result in the event the information is used in a manner contrary to its intended use.

7.5) All records will be kept and maintained as per Appendix 'A' *Record Retention Strategy* attached to this policy.

7.5.1) "Back-ups" that are taken will be maintained and stored regularly at a frequency as determined by Appendix 'A' and the IT Department.

7.6) Records, may, from time to time, be destroyed. When destroying these records, the employees of the Peguis First Nation will dispose of them in a manner that is in accordance with this policy and as per Appendix 'B' - *Document Destruction.*

Nothing that may be set out in this policy, will prevent or preclude the First Nation and it's administration from moving its record keeping, record maintenance or archival system to a digital environment, or a cloud based storage environment, so long as the strategy behind this move does not violate this Information Management Policy or any other policies in place and approved by Peguis First Nation's Chief and Council, or the Peguis First Nation Financial Administration Law.

8) ACCESS TO INFORMATION- EXTERNAL REQUESTS

8.1) For purposes of this policy, and all other policies and daily operations for the First Nation, the CFO for the Peguis First Nation, shall also serve the function of Privacy Officer.

8.2) With the exception of all internal requests for information, any requests for information from sources outside Peguis First Nation must be approved for their release by the CFO (for the reasons above) and Chief and Council.

8.3) All requests for information will be done so in writing. And will follow the steps below prior to any information being released to the general public.

8.3.1) The person requesting the information must complete and submit through regular mail, facsimile or email, the form attached to this policy and marked as Appendix 'C' - *Request for Information - External*.

8.3.2) Once the request has been received it will be forwarded to the CFO for her/his review.

8.3.3) The CFO will then work with the individual departments that might be providing the information requested.

8.3.4) Once the information is compiled and the response from the First Nation is drafted, the response and the documentation will be forwarded to Chief and Council for their review and approval.

8.3.5) From time to time, and depending on the nature of the request, the response may have some items redacted by the CFO.

8.3.6) Redaction will be reserved only in situations where the information requested is considered confidential and/ or has been filed and marked as confidential.

8.3.7) Once the information and the response from the First Nation has been approved for release by the CFO and Chief and Council, the requested information and the response will be saved and stored as per this policy.

8.3.8) For purposes of this policy any responses and the provision of information, when requested and approved will be maintained and considered to be a 'Special Purpose Report' and will be treated and filed as such.

8.4) From time-to-time financial information of the Peguis First Nation, other than its Annual Report and its annual audited financial statements may be requested.

8.4.1) Every year, within one hundred eighty (180) days of the close of the fiscal year, and in following the Peguis First Nation *Finance Policy*, the Annual report will be published to the Peguis First Nation website and will be available in hard copy format.

8.4.2) Every year, and within thirty (30) days of the approval of the annual audited financial statements, and no longer than one hundred thirty-three (133) days after the close of the year end, these same statements will be published in hard copy format and will be made available to the public upon request.

8.4.2.1) Once the annual audited statements are final, they will be published to the Peguis First Nation's website and will be provided to all external stakeholders that require them.

8.4.3) Other than the financial information indicated above, which after the deadlines indicated above have passed and the information contained in those reports becomes freely available, all other requests for financial information will be considered and treated as unique and non-recurring in nature and will be treated in a fashion similar to any other request(s) for information.

8.4.3.1) The types or items of information that **will not** be released by the finance department are the following:

- journal entries and internally created source documentation
- any banking information for the First Nation's bank accounts
- any personal financial information that may be maintained and kept on file for any of the PFN employees.
- Any specific details on contracts awarded by the Peguis First Nation, such as addresses, etc., that may otherwise be used for their unintended purposes.
- Remuneration of any of the employees of the Peguis First Nation that are not included on the annual 'Statement of Remuneration for Unelected Senior Officials.'

8.4.3.2) Until such time as it is approved for release and released to the general public, all financial information will be considered confidential and will be treated as such.

8.5) The types of information that require formal (in writing) requests for information and the type of information that do not require a formal request for information are outlined in Appendices 'E' and 'F'.

8.6) ***At no time***, *within sixty (60) days of an election campaign for Chief and Council* will the Administration or the Finance department of the First Nation entertain or fulfill, in any way requests for information of any kind.

8.7) The purpose of this part of the Peguis First Nation *Information Management Policy* is to replace the previous *Access to Information Policy* first adopted by Chief and Council is 2009.

9) REQUSTS FOR INFORMATION- INTERNAL

9.1) From time-to-time employees may be in need of information or records from other government departments in order to fulfill her/his responsibilities, or internally from within her/his own department, to which she/he may have at the time no access to.

9.2) All requests for information must be done so in writing and all employees must complete the form as shown in Appendix 'D' - *Request for Information - Internal*.

9.3) Other than financial information, including payroll information, the Program Director shall be responsible for granting access to the information the employee is requesting, including placing limitation on its use.

9.4) Requests for financial information from PFN employees must be done so in writing and will be made to the attention of the CFO or her/his designate.

9.4.1) Once the internal request for information has been fulfilled and should her/his designate be the individual in the Finance Department to fulfill the request, the CFO will approve the release of information to the employee requesting the information.

9.4.2) Should the CFO be the employee fulfilling the request, then the COO will be the one to approve the release of information to the employee requesting the information.

9.4.3) In any case, once the request has been fulfilled and approved for release, the information will be placed in internal mail and delivered to the employee in that manner, or it may be sent through secure, confidential email.

9.5) All internal requests for information, once fulfilled and approved for release, will be treated the same, in as far as documentation and filing the request, as it would be if the departments were fulfilling external requests for information.

9.6) ***At no time****, within sixty (60) days of an election campaign for Chief and Council* will the Administration or the Finance department of the First Nation entertain or fulfill, in any way requests for information of any kind.

10) INFORMATION MANAGEMENT- ROLES OF THE COO AND CFO

10.1) The role of Peguis First Nation's COO in Information Management will be

a) Establishing and maintaining a set of controls to document procedures for records management and for appropriate record keeping within the government's administration and its operations.

b) Take the lead in ensuring that, at all times, there are appropriate safeguards in place that will protect and keep safe the records of the First Nation.

c) Ensure compliance with any established record retention and disposition schedules that are in place and overseeing the disposition and destruction process of same.

d) The COO will ensure that all contractors, suppliers, vendors, and/ or third-party contractors or service providers are fully knowledgeable and adhere to all parts of this policy on Records Retention and their subsequent destruction.

10.2) The role of Peguis First Nation's CFO in Information Management will be the same as the COO's responsibilities and role, however, the CFO, in her/his capacity as Privacy Officer, will also ensure that all requests for access to information follow the appropriate processes.

10.2.1) The CFO will also ensure these same responsibilities to safeguard and preserve the First Nation's accounting book or record is kept safe, confidential and secure at all times.

11) ANNUAL REVIEW

11.1) To ensure this *Information Management Policy* remains current and that it is following best practices and continues to work with the five (5) year strategic plan, it will be reviewed annually by Executive Management and Chief and Council.

12) CONFLICT OF INTEREST

12.1) A conflict of interest, in terms of this, the Peguis First Nation *Information Management Policy,* will come to mean nothing different than how a conflict of interest is defined in either of the following two (2) Peguis First Nation policies, *Governance Policy and Human Resources Policy and Procedure Manual.*

12.2) However, in the case of the provision and management of information, the common definition of a conflict of interest in the Peguis First Nation, will be amended to include

that "at no time shall family members, immediate or otherwise, take on, fulfill, or otherwise work on a request for information, or other type of record keeping as it may relate to members of that person's family."

13) INFORMATION TECHNOLOGY

13.1) The Peguis First Nation maintains an internal information technology network of communication, including email, electronic storage and filing that will hereby be called their network.

13.1.1) This network is maintained on premise.

13.1.2) The purpose of this network is to ensure that data, records and other types of information can be stored and easily retrieved and that it is kept stored and safe following this policy and any Peguis First Nation Laws that may be created regarding Information Management.

13.1.3) The secondary purpose of this policy is to ensure that the data Peguis First Nation uses and generates is organized and maintained in a way that is in the best interests of Peguis First Nation, its Chief and Council and its Administration.

13.1.4) Nothing in this policy will prevent the Peguis First Nation or its Administration from transitioning its network to the internet and taking part in "cloud-based computing" providing nothing in the transition to "the cloud" violates this *Information Management Policy*, in whole or in part, or violates any other policy approved by the Chief and Council for Peguis First Nation, now and in the future.

13.1.4.1) Any new network introduced by the Peguis First Nation, its Chief and Council and its Administration must meet the current needs and the future needs of the network and this policy.

13.2) Any vendors, third- party contractors, or third- party consultants the Peguis First Nation hires that might be used to work on, upgrade or enhance performance of the network must sign the applicable confidentiality forms as prescribed by the Peguis First Nation *Human Resources Policy and Procedures Manual.*

13.2.1) When vendors, third-party contractors, or third-party consultants are hired by the Peguis First Nation, the scope of work and the services being performed must be identified and included in any service agreements or contracts.

13.3) The CFO, COO and the IT Department will, at all times, ensure that only approved software and other type of technology are use on the network.

13.3.1) The CFO, COO and the IT Department will, at all times, ensure the hardware that is used on the network is approved of beforehand and is the best solution for the circumstances.

13.4) For purposes of the remainder of this policy, the CFO will also be considered the Director for the Information Technology function of Peguis First Nation and will remain so until such time as the Peguis First Nation deems it appropriate to employ an individual at the Director level in this department.

14) NEW USER ACCESS TO THE NETWORK

14.1) At the request of the Program Director, all employees who require access to the network to perform her/his responsibilities of employment and discharge her/his duties will be provided access to the network, including an email.

14.1.1) All requests for access to the network must be done so in writing by the Program Director, and the Program Director must fill out the form called *"New User Access- PFN Network"* and has been included with this policy as Appendix 'G' for reference.

14.1.2) The IT Department and only the IT Department will be responsible for granting access to the network on behalf of the requesting department.

14.1.2.1) The Director of IT must approve of the request prior to it being fulfilled.

14.2) In order to fulfill her/his responsibilities of employment and discharge her/his duties, should an employee require access to any software that is available on the network, the Program Directors will be required to make that request on behalf of the employee.

14.2.1) Once the employee has been given access to the software required, and should the software required be generic in nature, such as email software or Microsoft Office software, the IT Department will provide the necessary training on the software.

14.2.1.1) Once access is granted, employees, as users, will be granted only the permissions and access that is directed by the Program Director and that she/he are in need of by virtue of her/his position.

14.2.2) Once the employee has been given access to the software required, and should the software required be specific to the program or service area the employee works in, such as the CRW System in Income Assistance, the department or service area the employee works in shall be responsible, and only her/him, to ensure the employee receives the necessary training to use the software.

14.2.2.1) Once access is granted, similar to section **14.2.1.1)** employees, new users of the network will only be given the permissions and access she/he needs by virtue of her/his position. Those permissions will be directed, in writing, by the Program Director.

14.3) New users of the system will be given unique log in credentials for her/his profile on the network server. These credentials, including usernames and passwords will be provided directly to the new user (employee) by the IT Department.

14.3.1) The IT Department will be responsible for maintaining a list of usernames, both active and inactive, and ensuring they are kept safe and not re-used by the system.

14.3.2) The unique log in credentials assigned to the user by the IT Department will, once logged into the system, provide the user with access to all the software applications the user has been granted permission to access.

14.3.2.1) The IT Department will provide the new user with any and all user agreements/acknowledgements that might be required to be reviewed and acknowledged by the new user prior to the new user being given access to the system.

14.3.2.2) At the very least, the new user will be required to review and sign off on these acknowledgements/user agreements within the first week of employment or within one (1) business week of being given access to the system.

14.3.2.3) The acknowledgement/agreement, is a required form of employment that needs to be reviewed, signed, and then placed in the employee's/users Human Resources file.

14.3.2.4) The new user acknowledgement/agreement form will take the form Appendix 'H' attached at the end of this policy.

15) EXISTING USERS OF THE NETWORK

15.1) At the time of writing, there are many current users of the Peguis First Nation Network, each of which have already been assigned usernames, passwords, and access to the software/applications she/he need to carry out the duties and fulfill her/his responsibilities of employment.

15.1.1) As such, the above employees will be grandfathered into this *Information Management Policy* and will not be considered new users to the existing network. At the time of implementation these existing users will not be required to sign any documentation, other than what is already filed for her/his continued access to the existing network.

15.1.2) However, in the event that Peguis First Nation transitions to a new network, each employee, existing or new, will be required to renew or re-establish her/his access to the network following the process described in this *Information Management Policy.*

15.1.3) However, and due to ongoing confidentiality concerns and ongoing issues with access to information, the Chief and Council, and Executive Management, may make it a condition of ongoing employment for all users of the network, including existing users, have ongoing access to the network which is confirmed as per this policy.

16) UNAUTHORIZED ACCESS TO THE NETWORK

16.1) Unauthorized access to the network, in any way shape or form, either by new or existing users of the network, will be considered a breach of confidentialities and a breach of trust, and will be subject to disciplinary actions, up to an including termination of employment, and as per the Peguis First Nation *Human Resources Policy and Procedure Manual.*

17) STANDARD EQUIPMENT

17.1) Peguis First Nation will employ a standardized set of hardware and other tools that users will have available to it with which they can use to access the network.

17.2) The standardization of the hardware and other tools that will be used to gain access to the network will be at the discretion of the IT Department, as determined by its Director, and must be within the constraints of the annual IT budget and will not violate this *Information Management Policy* in any way whatsoever.

17.3) The above standardization of equipment includes the mobile devices that are used by the government's administration, its Executive Management and its Chief and Council.

17.4) The standardization of equipment, hardware and other tools will be done so in general, however specific users of the network may have different IT needs depending on what function she/he may perform for the Administration of the First Nation.

17.4.1) Users of the system that have specific IT needs which may be due to compatibility or performance issues, may make requests of the IT department to have her/his specific needs addressed.

17.4.2) Providing a business rationale for non-standardized equipment, tools or hardware is approved, and that it is the budget for the IT Department, or any other applicable government department, the non-standard hardware can be purchased and will be made available for use the network.

17.4.2.1) Any non-standardized equipment, tools or hardware that is needed by users, will be rolled out to the required users according to this *Information Management Policy.*

17.4.3) Under this policy, users of the Information Management System, including the technology employed, may not access the Information Management System using her/his own personal devices.

18) PASSWORD RENEWAL AND HARWARE

18.1) Access to the network and all of the software applications the Peguis First Nation subscribes to will, as part of the user credentials, have passwords assigned to them to allow controlled access to the software application, including the Peguis First Nation server(s).

18.2) The IT Department, at its discretion, and with the approval of its Director, will ensure that all passwords for the above types of software applications will be, as part of the secure access requirements, reset once every sixty (60) days.

18.3) The type of hardware that is deployed at a user's workstation will be at the discretion of the IT Department and its Director.

18.3.1) At all times, the hardware deployed to the users will be in line with the requirements of this policy and will always allow the users to faithfully do her/his work and will always allow for access to the software and the server(s) she/he require access to perform her/his duties.

18.3.2) An acceptable mix of thin clients, personal desktop computers and laptops computers, along with mobile tablets that are compatible with Peguis First Nation server's operating system will be tolerated and be considered.

18.4) All hardware deployed under the IT strategy for the Peguis First Nation's Administration will have installed on them, the usernames, serial numbers and other tracking mechanisms the IT Department and its Director decide are acceptable for controlling the use of Peguis First Nation owned hardware and technology.

18.4.1) Due to the confidentiality surrounding the types of devices that are used by ***Chief and Council***, and providing the members of the governing body use hardware that is provided to them, by virtue of their elected position, through the Peguis First Nation IT Department, the tracking tools and other kinds of identifiers the IT Department may use to monitor the use of these devices will be documented and kept, at all times, confidential.

18.4.2) For greater clarity, the identifiers used for Chief and Council will be stored and kept confidential and will, at all times, remain in the possession of the following three (3) individuals: the COO, the CFO and the Director of IT.

18.4.2.1) This will include, serial numbers, usernames, passwords, phone numbers and anything else that could be used to identify may be using the device.

18.4.3) When their term in office comes to an end, each member of Chief and Council will be required to return any of the equipment or devices in their use that are the property of Peguis First Nation.

Chief and Council will be required to sign and agree to the various terms and conditions of the use of the hardware that has been assigned to them, however those user agreements will be kept confidential and maintained by the COO, the CFO and the Director of IT.

19) USE OF THE INTERNET

19.1) Access to the internet maybe granted to employees to facilitate aspects of an employee's ability to discharge her/his duties and fulfill her/his responsibilities as employees of the Peguis First Nation.

19.1.1) In case of certain employees, who, through responsibilities of her/his employment, may be required to use the internet to access and use social media accounts such as LinkedIn, Twitter or Facebook, may do so, and in this case, and based on approval of use of social media accounts to carry out Peguis First Nation business, and only Peguis First Nation business, may be excluded from section **19.2)** of this policy.

19.1.2) Those certain employees, as indicated in above **19.1.1)**, may only use social media accounts owned and managed by the Peguis First Nation, providing the messages communicated are in accordance with this policy and any other policy that may be adopted, from time to time, by Chief and Council, including the Peguis First Nation *Social Media Policy*.

19.1.3) The Peguis First Nation *Social Media Policy* can be found in Appendix 'I' of this *Information Management Policy*.

19.2) In this case, the internet, and access to it, is being provided for business purposes only. It is not being provided to users as a means to allow for personal communication, as such the IT Department reserves the right, on behalf of Chief and Council, to restrict the use of the internet connection provided to just this, business purposes.

19.2.1) As such, and at the direction of the IT Director, the IT Department will restrict access to, or effectively "block", and in conjunction with the Peguis First Nation *Social Media Policy*, prevent users from using her/his workstations and the corresponding internet connection to gain access to or use any social media websites that are considered personal in nature.

19.2.2) Should an employee, or user, be found to be using the internet connection for use other than its intended purpose, that user or employee will be found to be in violation of this *Information Management Policy* and may be subject to disciplinary action, as per the Peguis First Nation *Human Resources Policy and Procedure Manual.*

20) TYPE OF NETWORK AND NETWORK MONITORING

20.1) At the direction of the Chief and Council, and Executive Management, the IT Department will at all times maintain a type of network that will allow for ease of access and secure access to the servers and the file storage areas.

20.1.1) This can be achieved through, but will not be limited to, the employment of a Local Area Network (LAN), a Wide Area Network (WAN) or a Virtual Private Network (VPN), "cloud-based computing" or some combination of all of these, so long as it meets the requirements and objectives of this policy.

20.2) At all times, and to allow for future upgrades and enhancements, the IT Department will create, develop, and maintain accurate documentation of the network and its systems.

20.3) The IT Department will ensure that regular monitoring of the network, which will include its performance, ongoing accessibility, its file storage capabilities and how it is accessed, along with the frequency of access is maintained and followed.

21) APPROVED SOFTWARE APPLICATIONS

21.1) All software applications and any hardware that is used as part of the network must be pre-approved and meet standards as determined by the IT Department.

21.1.1) The CFO, or her/his designate, will ensure, through periodic reviews, that workstations and the network are effectively monitored and are only operating with applications or hardware that meet the requirements of this policy, or any documented procedures the IT Department may keep.

21.1.2) All firewalls, whether they be software or hardware, are monitored regularly as part of the security requirements of the network.

22) NETWORK SECURITY

22.1) The IT Department and its Director, will ensure that proper security mechanisms are in place and functioning that will prevent unwanted access and malicious attacks to the network.

22.1.1) Other than mobile devices, and more specifically cellular telephones, each workstation will have a recommended version of an anti-virus software installed, functioning, and kept current on her/his workstation.

22.1.2) The protection contemplated in the above section **22.1.1)** may or may not be applicable to any "tablet" type devices that are employed as part of the overall Peguis First Nation IT strategy.

22.1.2.1) Should the Peguis First Nation choose to employ devices with an Android based operating system, then section **21.1.1)** is applicable.

22.1.2.2) Should the Peguis First Nation choose to employ a standard set of devices such as iPads, or another version of an Apple tablet, then section **21.1.1)** will not apply.

22.1.3) Any anti-virus software that is installed must meet the following specifications:

- Must be configured to scan all programs and files upon execution and have real time protection enabled.
- The anti-virus software must be able to update itself automatically, or when new threats to the security of the network are identified.

22.2) Network firewalls will be installed on each device that may be used to allow for external communication with the network.

22.2.1) Each firewall will be configured to support and allow for specific systems, services, and protocols to enter the network through its perimeter.

22.2.2) Physical access to the network will be limited to only those individuals that have specific training and which are authorized to manage the device on behalf of the Peguis First Nation.

22.2.3) At all times, the following standards regarding firewalls must be met:

- Firewall proxy servers must be securely installed
- Firewall logs shall be kept, and maintained
- Alerts will be raised in the event important processes or services fail.

23) NETWORK CHANGES

23.1) In the event the Chief and Council, the COO, the CFO, and the IT Department plan to make changes to the network, any new modifications will be planned out and tested prior to implementation happening.

23.2) All computers, other hardware, or software and any of the communications systems in the network that are being changed, modified, or upgraded shall have the appropriate documentation of said changes made.

23.3) Any planned changes to the network should be rational and will have the rationale for the change stated in writing, along with:

- any assessments of the risk associated with the change

- the description of any testing that might be needed
- any implementation considerations, including challenges that might need to be overcome should be stated.
- A plan for the communication to the affected employees must be stated.

23.4) Any planned changes to the network must be within budget and must, at the least, be signed by the Director of the IT Department and the CFO or her/his designate.

23.5) Any planned changes to the network must be communicated to Chief and Council.

24) TERMINTATION OF EMPLOYMENT

24.1) By virtue of this *Information Management Policy*, the Peguis First Nation IT Department will be hereby placed on notice that when an employee's (users) employment with the Peguis First Nation has been terminated, whether voluntarily or involuntarily:

- In the event of termination of employment by Peguis First Nation, the IT Department will be instructed to disable her/his network access effective immediately
- Or, if the employee leaves voluntarily, on the employee's last day of work.

24.2) For whatever reason, and upon termination of employment, all employee's (users) will be required to provide the following to either the Director of the IT Department, the CFO, or the COO (depending on the position of the employee):

- All username and passwords required to access software applications
- Any fobs, key cards, or other tools she/he may require accessing the network
- Any and all devices or pieces of hardware that are the property of the Peguis First Nation.

25) CHIEF AND COUNCIL - END OF TERM

25.1) One (1) week prior to the end of Chief and Council's term in office each member of Chief and Council that has, in their possession, any devices, hardware, usernames or passwords that are the property of the First Nation, must surrender the belongings, and upon surrender the IT Department's Director, and the Director alone, will either temporarily or permanently disable their access to the network, as the case may be.

26) OUTSOURCING OF WORK RESPONSIBILITIES

26.1) Nothing in this policy will prevent or preclude the Peguis First Nation's Administration from outsourcing any part(s), or the whole of this *Information Management Policy* to an independent third-party contractor, providing that contractor is provided with a copy of this policy and all other policies that will be necessary for that contractor to fulfill the

terms and conditions of their engagement with the Peguis First Nation and that contractor agrees to follow these policies.

26.2) Once outsourced to a third-party contractor, should the third-party contractor violate this *Information Management Policy,* or any other of the Peguis First Nation policies, the violation of policy, may be grounds for termination of the contract.

27) INFORMATION TECHNOLOGY- ROLES OF THE CFO AND THE COO

27.1) The CFO, in her/his capacity as the Privacy Officer in addition to her/his responsibilities as CFO, will hold the responsibility for and take overall accountability for the effective, efficient, and robust management of the IT Department for the Peguis First Nation, including its network.

27.2) The CFO will ensure at all times, this *Information Management Policy* remains current, is in line with Chief and Council's mandate and its strategic vision, and the proper and accurate enforcement of this policy.

27.3) The COO will share this responsibility with the CFO, and will in fact be the CFO's support, respite provider and coverage when the CFO may not be available.

28) PERSONAL INFORMATION COLLECTION AND RETENTION

28.1) In the course of regular business Peguis First Nation is required to collect information that may be considered to be either personal or proprietary in nature, such as personal identifiers or business numbers.

28.2) Under this policy, Peguis First Nation, for employment reasons, may ask for a new employee or its existing employees to provide her/his social insurance number (SIN) and her/his Certificate of Indian Status card (Status Card) or proof of status.

28.2.1) In the case of Status Cards, the request will be made for employment reasons only, and shall only be used for this intended purpose.

28.2.2) At its discretion, and as part of building a robust employee file, Peguis First Nation, may retain a copy of the Status Card for the length of time the employee is employed and for a period of time, post-employment, and in accordance with this *Information Management Policy*.

28.3) For employment purposes, Peguis First Nation, may ask, as a condition of employment, for a new or an existing employee for her/his SIN.

28.3.1) Should an employee provide Peguis First Nation with her/his SIN as a matter of securing ongoing employment, Peguis First nation shall retain this information in the strictest of confidence and will make every effort to maintain this information in a safe and secure environment.

29) DELEGATION OF RESPONSIBILITIES

29.1) Nothing in this policy will prevent or preclude the CFO or the COO from delegating some, or all of the responsibilities in this *Information Management Policy* to any employee, or member of the Executive Management Team, providing the delegation of responsibilities does not violate this *Information Management Policy* or any other policy that has, or will be implemented by the Peguis First Nation.

END OF POLICY