Information Technology Policy

Policy

Nipissing First Nation's information systems will support its operational requirements and have appropriate safeguards and monitoring processes in place to adequately protect Nipissing First Nation's information.

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 Nipissing First Nation.

Scope

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

Definitions

"***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.

Responsibilities

Council is responsible for:

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

The Chief Executive Officer is responsible for:

- Ensuring that controls are in place regarding information technology, whether performed by an internal staff member or outsourced to an external organization;
- Monitoring the performance of internal and/or external information technology professionals.

The information technology technician(s) are responsible for:

- Maintaining the integrity of information systems within Nipissing First Nation.

Procedures

Planning and evaluation

The Council, with the assistance of the Chief Executive Officer and input from information technology staff, will ensure that information systems are developed that support Nipissing First Nation'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 Chief Executive Officer will seek advice from a qualified external individual or organization.

Outsourcing

Subject to the Procurement Policy, the Chief Executive Officer is responsible for the selection of contractors providing information technology services, the definition of services in their contracts and the administration of the contracts.

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

- A requirement that the service provider submits regular reports of all work performed on Nipissing First Nation'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 Nipissing First Nation information is provided on a 'need to know basis' only.

Data management

Data retention allows access to appropriate data to specified personnel where required, depending on the type of data retained.

All sensitive, valuable, or critical information / data residing on Nipissing First Nation's information technology systems must be periodically backed-up. Backups will occur incrementally on a daily basis, with full backups on a weekly and monthly basis.

USB drives must be stored in a secure location with access limited to the Chief Executive Officer and limited other staff as appropriate. Ideally, USB drives tapes will be securely stored at an offsite location that is easily accessible to individuals with authorized access.

USB Drives will be retained for a period of one (1) year, according to applicable legal requirements.

Access management

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

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

A 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.

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

When an individual or contractor is terminated or ends employment with Nipissing First Nation, 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.

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 ("AV") program installed. The following standards must be met:

A. The AV program must not be disabled and must be configured to scan all programs and files upon execution and must have real time protection enabled. If encrypted and password protected files cannot be virus checked, it is the responsibility of the user to ensure that virus checking takes place whenever this protection is removed;

B. Antivirus files must be updated on the network every two weeks or whenever a new threat is identified.

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

Additionally, the following Firewall standards must be addressed:

i. Firewall and proxy servers must be securely installed;
ii. Detailed firewall logs will be reviewed as needed and stored for a period of two(2) weeks;
iii. Alerts must be raised if important services or processes crash.

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:

1. The data structure is consistent with the needs of Nipissing First Nation;
2. Description and rationale for the new network, hardware, communication and systems software change and how it is consistent the needs of Nipissing First Nation;
3. An assessment of any risks involved with the change;
4. Roll-back considerations;
5. Implementation considerations;
6. A description of the testing required;
7. Approval from the Chief Executive Officer;
8. Communication of changes to Nipissing First Nation staff as appropriate.

Monitoring

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

(2) A log of staff, their user IDs, and their access levels within First Nation information systems will be maintained. On a quarterly basis, the Chief Executive Officer, or his designate, will review the log to ensure users and the associated access rights are appropriate. Access rights that will be monitored include the following:

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

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

(c) Network access and file sharing;

(d) Remote and VPN access.

(3) Network system performance is monitored on a regular basis.

(4) The firewalls must be monitored daily and their functionality audited semi-annually.