

First Nation or Organization Security Policy

Introduction

(First Nation or Organization) is responsible for the actions of its staff and the legal implications of unethical use and access of its systems.

The purpose of this policy is to provide guidelines so that **(First Nation or Organization)** staff may utilize these resources in ways that maximize employee productivity and minimize security gaps.

1. General Policy

(First Nation or Organization) has realized that to effectively protect their Systems from unauthorized access, alteration, disclosure or destruction, and to guarantee that data and programs are readily available to all authorized members of staff; they require a level of protection. **(First Nation or Organization)** also realizes that while no procedures will provide total security, all staff has the responsibility to minimize the risks.

2. System Access

You may not attempt to access information for which you have no authorization including, but not limited to, data and email.

To ensure your workstation is secure in your absence from your office, logging off, a password protected screensaver, or turning off your monitor should be considered when you leave the room.

3. Passwords

In the cases where a password is important such as email systems or workstation access, including screensavers, individuals should ensure the passwords are difficult to guess but easy to remember. If a password has been assigned to you as a temporary password, you must change it before continuing use of the system. To aid in the creation of a password here are some guidelines.

- Use 5 or more characters, including mixed case
- Deliberately misspell words
- Take the first letter from each word of a phrase
- Include at least two numbers, you can substitute letters for number (ie 3 for E)

Individuals should make sure their password is safe, this includes making sure not to write passwords down, let anyone see you entering

your password. Change your password every few months and never reuse an old password.

4. System Updates

Whenever possible, the installation of approved software updates must be performed. This may be setup as a automated feature and it should be set to be completed outside office hours to minimize any disruptions.

5. Virus Protection

Virus protection is most effective if every workstation and server in the office has up to date anti-virus software installed and is actively monitoring all incoming and outgoing activities to help control infection.

Viruses are able to enter the computer in various ways including email, downloading from the internet and removable media (cd, dvd, floppy).

Computer systems owned by **(First Nation or Organization)** will run up to date anti-virus software that must remain active at all times. The primary user of a computer system is responsible for keeping the computer system up to date.

6. Identity Misrepresentation

As an employee of the **(First Nation or Organization)** you may not assume another person's identity or position without prior permission.

7. Enforcement

Failure to comply with this policy may result in disciplinary action, up to and including termination of employment.