Information Technology (IT) Policy
Approved by AFNWA Board
Date: October 7, 2021

Purpose

The AFNWA employee has been issued AFNWA electronics/devices. These electronic devices are for work related activities and thus carry a responsibility. The AFNWA employee agrees to adhere to this policy and related procedures (as amended from time to time).

To better serve our communities and provide our employees with the best tools to do their jobs, AFNWA makes available to our workforce access to one or more forms of electronic media, services and devices, including computers, e-mail, telephones, cell phones, text messaging, voicemail, fax machines, software, Intranet, and Internet services.

AFNWA encourages the use of these media, services and associated devices as they can make communication more efficient and effective and provide access to valuable sources of information. However, all employees and everyone connected with the organization should be hereby advised that electronic media, services and devices provided by the organization are organizational property and their purpose is to facilitate and support the organization's business. All electronic media users have the responsibility to use these resources in a professional, ethical, and lawful manner.

To ensure that all employees recognize their responsibilities under this policy, the following guidelines have been established for using electronic media. No policy can lay down rules to cover every possible situation. Instead, it is designed to express the AFNWA's philosophy and set forth general principles when using electronic media, services and devices.

Issuance

A cellular phone /laptop computer is only issued through the Information Technology (IT) Department once proper authorization has been received from the Manager of Corporate Services. For adherence to this policy and for inventory purposes, Employees are prohibited from purchasing their own cellular phone/ Laptop computer for purposes of AFNWA business.

A request must be made through the Department Manager, who will assess the need and make a recommendation to the Manager of Corporate Services for final approval. A written approval from the Manager of Corporate Services is required.

Written approval must be forwarded to the IT Coordinator; and once received, the equipment (cellular phone and/or laptop computer) will be issued, with all software licenses and network access purchased and maintained by AFNWA. All staff will be provided with a sign out sheet for all hardware that is under their care, to be supported by serial numbers, where available.

The AFNWA will not reimburse Employees that have purchased their own cellular phone/ laptop computer.

Prohibited Communications

Electronic media shall not be used for knowingly transmitting, retrieving, or storing any communication that is:

Discriminatory or harassing,
Derogatory to any individual or group,
Obscene, sexually explicit, or pornographic,
Defamatory or threatening,
In violation of any license governing the use of software; or
Engaged in for any purpose that is illegal or contrary to the AFNWA's policy or business interests.

Employees are responsible for the content of blogs and social media posts, both professional and personal.

AFNWA, in compliance with the respective provincial regulations, prohibits employee use of cellular phones while driving, unless a hands-free device is used. This prohibition of the use of a cell phone or similar device while driving includes, but is not limited to, receiving, or placing calls, text messaging, surfing the Internet, receiving, or responding to email, and checking for phone messages.

Personal Use

The electronic media services, and devices, including computers, laptops, and cell phones, provided by AFNWA are primarily for business use to assist employees in the performance of their jobs. Limited, occasional, or incidental use of electronic media (sending or receiving) for personal, non-business purposes is understandable and acceptable (i.e., personal banking or checking personal email accounts during lunch/break times), and all such use should be done in a manner that does not negatively affect the systems' use for their business purposes. However, employees are expected to demonstrate a sense of responsibility and not abuse this privilege.

Keep in mind that AFNWA owns any communication sent via email or that is stored on AFNWA owned laptop/Cell Phone equipment. Please do not consider electronic communication, storage, or access to be private if it is created or stored or transmitted at work.

Access To Employee Communications

Electronic information created and/or communicated by an employee on an AFNWA device or network using e-mail, word processing, computer programs, spreadsheets, cell phones (text messaging), voicemail, telephones, Internet and Intranet and similar electronic media may be periodically reviewed and monitored by the organization.

The following conditions should be noted: AFNWA does routinely gather logs for most electronic activities or monitor employee communications directly, e.g., cell phone/telephone numbers dialed, sites accessed, call length, and time at which calls are made, for the following purposes:
1. Cost analysis.
2. Resource allocation.

3. Optimum technical management of information resources; and
4. Detecting patterns of use that indicate employees are violating organization's policies or engaging in illegal activity.

AFNWA reserves the right, at its discretion, to review any employee's electronic files and messages to the extent necessary to ensure electronic media, services and devices are being used in compliance with the law, this policy or other organization policies.

Employees should assume that all electronic communications are not private, although best efforts shall be made to respect employee's privacy where electronics communications are clearly personal.

Accordingly, if they have sensitive personal information to transmit, they should use other means.

Software

To prevent computer viruses from being transmitted through the organization's computer system, downloading of any unauthorized software is strictly prohibited. Only software registered through AFNWA may be downloaded. Employees should contact the system administrator if they have any questions. All AFNWA computers must use authorized anti-spy and anti-virus software. Employees need to inform their Director/Manager and the IT Coordinator if this software is not functioning and/or about to expire.

Security/Appropriate Use

Employees must respect the confidentiality of other individuals' electronic communications. Except in cases in which explicit authorization has been granted by AFNWA management, employees are prohibited from engaging in, or attempting to engage in:
1. Monitoring or intercepting the files or electronic communications of other employees or third parties.
2. Hacking or obtaining access to systems or accounts they are not authorized to use.
3. Using other people's logins or passwords; and
4. Breaching, testing, or monitoring computer or network security measures.

No e-mail or other electronic communications can be sent that attempt to hide the identity of the sender or represent the sender as someone else.

Electronic media and services should not be used in a manner that is likely to cause network congestion or significantly hamper the ability of other people to access and use the system.

Anyone obtaining electronic access to other organizations' or individuals' materials must respect all copyrights and cannot copy, retrieve, modify or forward copyrighted materials except as permitted by the copyright owner.

Loss Of Equipment

If an Employee loses their cellular phone/ Laptop computer and other related equipment due to employee negligence, that Employee shall pay AFNWA the fair market value of the equipment lost. No

other cellular phone / laptop computer will be issued to that Employee until notification is received from the AFNWA Finance Division or Department that the replacement cost has been received. The replacement cellular phone /laptop computer is to be considered AFNWA property.

If the original cellular phone /laptop computer is found, it is to be returned to the IT Department. The new cell phone is still to be considered AFNWA property, but reimbursement of the amount paid by the Employee for the lost cellular phone/laptop computer will be returned to the Employee by the AFNWA Finance Division or Department.

Repairs to Equipment

If it is found that a cellular phone /Laptop computer needs repair due to misuse by the Employee, the repair cost will be borne by the Employee. Notification must be made by the Finance Division or Department that they have received restitution before repairs can be authorized. The cost for minor repairs or replacement in ordinary day to day usage will be paid by the AFNWA.

As a cellular phone /laptop computer must be outsourced to be fixed, in the interim, if a replacement is available, it shall be issued to the Employee whose cellular phone/laptop computer is out for repair on the same terms and conditions as set out in this policy.

Expenses

The Director/Manager must ensure that expenses associated with cell phone/Laptop computer usage are to be charged to the appropriate departmental budget.

AFNWA will not be responsible for any charges incurred through personal use; whether it be long distance calls or use that causes the employee to exceed a monthly allocated budget for a data plan. The Employee shall reimburse AFNWA via the next payroll after the cost(s) is incurred.

Encryption

Employees may only use encryption software supplied to them by the systems administrator for purposes of safeguarding sensitive or confidential business information. Employees who use administrator-provided encryption on files stored on an organization computer must provide their supervisor with a sealed hard copy record (to be retained in a secure location) of all the passwords and/or encryption keys necessary to access the files.

Participation in Online Forums

Employees should remember that any messages or information sent on AFNWA-provided electronic media or services to one or more individuals via an electronic network—for example, Internet mailing lists, Facebook, MSN, bulletin boards, and online services—may be identified and attributed to the AFNWA. It is not permissible for any employee to identify themselves as employees of the AFNWA on

Facebook or other internet sites/other forums that do not form part of their professional duties and that they are using for personal reasons, including using their work email or other contact details.

AFNWA recognizes that participation in some forums might be important to the performance of an employee's job. For instance, an employee might find the answer to a technical problem by consulting members of a professional association devoted to the technical area.

Violations

Any employee who abuses the privilege of their access to electronic media, services and devices (such as computers, e-mail, telephones, cell phones, text messaging, voicemail, fax machines, Intranet, and Internet) in violation of this or any other AFNWA policy will be subject to corrective action, including possible termination of employment, legal action, and criminal liability.

Password Protection & General Procedures

The purpose of this procedure is to specify guidelines for use of passwords. Most importantly, this procedure will help users understand why strong passwords are necessary and help them create passwords that are both secure and useable. Lastly, this procedure will educate users on the secure use of passwords. This procedure applies to any person who is provided an account on the organization's network or systems, including: employees, guests, contractors, partners, vendors, etc.

The best security against a password incident is simple: following a sound password construction strategy. The organization mandates that users adhere to the following guidelines on password construction:

1. Passwords should be at least 8 characters
2. Passwords should be comprised of a mix of letters, numbers and special characters (punctuation marks and symbols)
3. Passwords should be comprised of a mix of upper- and lower-case characters
4. Passwords should not be comprised of, or otherwise utilize, words that can be found in a dictionary
5. Passwords should not be comprised of an obvious keyboard sequence (i.e., qwerty)
6. Passwords should not include "guessable" data such as personal information about yourself, your spouse, your pet, your children, birthdays, addresses, phone numbers, locations, etc.

Passwords should be considered confidential data and treated with the same discretion as any of the organization's proprietary information. The following guidelines apply to the confidentiality of organization passwords:

1. Users must not disclose their passwords to anyone
2. Users must not share their passwords with others (co-workers, supervisors, family, etc.)
3. Users must not write down their passwords and leave them unsecured
4. Users must not check the "save password" box when authenticating to applications
5. Users must not use the same password for different systems and/or accounts, except under Single Sign On software, as prescribed by the IT coordinator
6. Users must not send passwords via email
7. Users must take care to change their passwords regularly (minimum every 90 days) and to not re-use old passwords

Since compromise of a single password can have a catastrophic impact on network security, it is the user's responsibility to immediately report any suspicious activity involving his or her passwords to their manager/director and IT Coordinator. Any request for passwords over the phone or email, whether the request came from organization personnel or not, should be expediently reported. When a password is suspected to have been compromised the IT Coordinator will request that the user, or users, change all his or her passwords.

This policy will be enforced by the IT Coordinator and/or Corporate Service Manager. Violations may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment.

Outsourcing External IT Support

Outsourcing is often necessary when specialized expertise is required, which happens frequently in the field of Information Technology (IT). Trust is necessary for a successful outsourcing relationship; however, the AFNWA must be protected by a policy that details and enforces the terms of the outsourcing relationship.

All outsourced IT functions are at the discretion of the Manager of Corporate Services or the CEO. Under no circumstances should you grant access to your system to a third party without the expressed permission of the Manager of Corporate Services and CEO.

Standards and Controls for Network Access and Authentication

Consistent standards for network access and authentication are critical to the AFNWA's information security and are often required by regulations or third-party agreements. Any user accessing the AFNWA's computer systems has the ability to affect the security of all users of the network. An appropriate Network Access and Authentication procedure reduces risk of a security incident by requiring consistent application of authentication and access standards across the network.

Please contact the Manager of Corporate Services or the IT Coordinator if you require Network Access for yourself or for a contractor, or guest of the AFNWA.

Employee Agreement

I have read, understand, and agree to comply with the IT Policy and conditions governing the use of the organization's electronic media, services and devices. I understand that the organization may, from time to time, need to gain access to my work computer and, as such, I am only entitled to a reasonable level of privacy on my work computer. I am aware that violations of this guideline on appropriate use of the e-mail and Internet systems may subject me to disciplinary action, including termination from employment, legal action, and criminal liability. I further understand that my use of the e-mail and Internet may reflect on the image of the Atlantic First Nations Water Authority to our clients, community members, and other stakeholders and that I have responsibility to maintain a professional and positive representation of the organization. Furthermore, I understand that this policy can be amended at any time.

Date: _____

Print name: _____ Employee Signature: _____

Witness: _____ Witness Signature: _____