KWANLIN DÜN FIRST NATION

HEALTH AND SOCIAL DEVELOPMENT DEPARTMENT

PANORAMA SECURITY POLICIES

May 10, 2016

Table of Contents

Building Security……3

Confidentiality Policy ……5

Privacy Breach Policy ……8

Clean Desk Policy……11

Password Management……12

Secure Use of Removable Data Storage Devices……14

Appendices

1. Building After Hours Alarm Response Procedure……17
2. Code of Conduct and Ethics ……18
3. Oath of Confidentiality……19
4. Discipline Policy…… 20
5. Return of Property……23

These security policies were developed for using the Panorama Database. However, the policies apply to all staff and program areas of the Health and Social Development Department to ensure that client confidentiality is maintained at all times.

Approved by Council Resolution 2016-16 , May 10, 2016

Building Security

Purpose: The purpose of this policy is to establish and maintain security measures for the Kwanlin Dün Health and Social Development Department

Policy: Accountability for all keys and electronic key fobs issued is paramount to the personal safety and security of the staff and a vital component in the protection of client information maintained within the buildings.

Keys, key fobs and access codes will be issued on a demonstrated needs basis and will require the approval of the Director of Health or delegate. Keys, key fobs and access codes are not provided to visitors accessing the health centre or the Social Development Branch.

All keys and key fobs assigned for access to the health centre or House of Learning remain the property of Kwanlin Dün and shall not be duplicated. Staff assigned keys and key fobs must return them to the Director upon termination of employment, or when the need for access is no longer required.

Keys, key fobs and access codes are not to be shared among staff. A master list of codes, keys and key fobs is maintained by the Director of Health or designate. All lost or stolen keys, key fobs or access codes must be reported immediately to the Director of Health or designate.

Procedures:

- Locks: The health centre is on an automated security system. The front doors will unlock at 8:30 a.m. and 1:00 p.m. and automatically lock at 12 p.m. (noon) and 4:30 p.m. All remaining outside access doors are closed and locked at all times.
- Security alarm: The security alarm is disarmed by the first person in the building in the morning, and set by the last person to leave the building at night. The security alarm automatically sets at 7 pm.
- Windows: Each staff member is responsible for ensuring their office windows are closed and locked.
- Desks/workstations: each staff is responsible for:
- Computers: locked when staff are away from their desk
- Logging out of computers at the end of the day
- Securing all client files, lab reports, or any data considered sensitive in nature in a locked cabinet at the end of each working day
- Locking all filing cabinets and making sure the door to the chart room is locked

- Generally staff should not be accessing the health centre outside of business hours, but if access is necessary, they are required to disarm and reset the alarm system, **ensure doors and windows are closed and locked**
- If the building alarm or motion sensors are activated after business hours, the building after hours alarm response procedure must be followed. (See Appendix 1)
- Staff will report to their manager or delegate, any missing property, vandalism and threats related to building security.

Confidentiality Policy

Purpose: To safeguard client information

Policy: Health and Social Development Department employees have a legal and ethical obligation to maintain confidentiality of all client information, and be aware of the consequence of not adhering to their obligations and practices in accordance with existing policies and legislation. This applies to personal information and other confidential information under the custody and control of the Health and Social Development Department where employees have access to direct care and program delivery. All staff must recognize the importance of privacy and confidentiality and safeguard personal, family and community information obtained in the context of a professional trusting relationship.

Developments in technology have changed the delivery of health care and the system used to record and retrieve client health information. In addition to using paper medical records, health professionals routinely use computers, phones, faxes, and other methods for recording and transferring information. Protection of privacy and confidentiality are essential.

Staff must follow all existing procedures to protect client privacy and safeguard the confidentiality of health records and information. Client confidentiality is a core responsibility central to ethical health care practices and a primary value in the Code of Ethics for all health care professionals.

All staff members are responsible for upholding the Employee Code of Conduct and Ethics and the Oath of Confidentiality. (Personnel Policy Appendices A and B)

Principles of Confidentiality

The following principles for maintaining confidentiality are adapted from the Nursing Code of Ethics but are applicable to all employees of the Health and Social Development Department.

- respect the right of people to have control over the collection, use, access and disclosure of their personal information.
- take reasonable measures to prevent confidential information, in conversation, from being overheard.

- collect, use and disclose health information on a need-to-know basis with the highest degree of anonymity possible in the circumstances and in accordance with Yukon Government's *Health Information Privacy Management Act* (HIPMA) and Kwanlin Dün's *Freedom of Information and Protection of Privacy Act* (FIPPA).
- when required to disclose information for a particular purpose, disclose only the amount of information necessary for that purpose and inform only those necessary. Attempt to do so in ways that minimize any potential harm to the individual, family or community.
    - when engaging in any form of communication, including verbal or electronic, involving a discussion of clinical cases, ensure the discussion of persons receiving care is respectful and does not identify those persons unless appropriate.
    - advocate for persons in care to receive access to their health care records through a timely and affordable process when such access is requested.
    - respect and follow Kwanlin Dün's policies and legislation that protect and preserve people's privacy, including security safeguards in information technology.
    - do not abuse access to information by accessing health care records, including their own, that of a family member or any other person for purposes inconsistent with professional obligations.
    - intervene if colleagues or others are inappropriately accessing or disclosing person or health information of persons receiving care.

Procedures:

- Health and Social Development Department staff are not permitted to access personal or health information for any purpose that is inconsistent with professional responsibilities.
- store client records in a safe and secure place. Take special care when transporting client records to ensure they are not lost, stolen or accessed by unauthorized persons.
- maintain security of personal information as outlined in the clean desk and building security policies and procedures regarding cabinets, desks and work areas.
- nursing staff to ensure the immunization fridge, lab fridge and cupboard are double locked.
- nursing staff ensures medication cupboard is double locked.
- all staff must ensure their computers are locked when leaving their desks.
- all staff are responsible for securing all client files, lab reports, or any data considered sensitive in nature, in a locked cabinet in a locked room at the end of each working day.
- Counselling staff will ensure all client files are secured in locked filing cabinets fitted with an additional locking security bar.
- each staff member is responsible for logging off their computer at the end of the day.
- be aware of other people in the work environment and make sure that confidential conversations cannot be overheard. White noise machines must be turned on and placed outside office doors to protect client confidentiality.
- work emails include a statement of confidentiality as noted below:

> **Confidentiality Notice**: this email communication is directed solely to the individual addressee(s). If you have received this email in error, please notify the author immediately by return email and permanently delete this transmission from your system without making copies in any format. If you are an intended addressee please be aware that the contents of this email communications may be disclosed under the *Freedom of Information and Protection of Privacy Act*.

- client identifiers (such as names, Yukon Health Information and Serostatus (YHIS) and Date of Birth (DOB) should **not** be used in emails
- if faxes are being used to transmit information, check the fax number to ensure it is correct and use a Kwanlin Dün Health and Social Development fax cover sheet
- the department cover page must clearly state sender's name and phone number and include the following confidentiality statement:

> **Confidentiality Notice**: this fax communication is directed solely to the addressee. If you have received this fax in error, please notify the sender immediately and shred this transmission. Do not make copies. If you are an intended addressee please be aware that the contents of this fax communications may be disclosed under the *Freedom of Information and Protection of Privacy Act*.

- all employees are required to immediately intervene if others inappropriately access or disclose personal or health information of persons receiving care and report any concerns or occurrence to the Director of Health or designate.

Privacy Breach Policy

Purpose: Kwanlin Dün takes its responsibility to protect personal information very seriously. The purpose of this policy is to provide rationale and procedures to identify, contain and notify (in certain circumstances) the affected individuals of a privacy breach. This policy also allows Kwanlin Dün to respond quickly to a privacy breach and take steps to prevent the breach from occurring again.

Definitions: **personal information**

- the individual's name, address and telephone number
- race, national or ethnic origin, colour, religious or political beliefs or associations
- age, sex, sexual orientation, marital status, family status
- identifying number, symbol or other particular assigned to the individual
- fingerprints, blood type, inheritable characteristics
- health care history, including a physical or mental disability
- educational, financial, criminal or employment history
- personal views or opinions

privacy breach

- occurs when there is access, collection, use, disclosure and or disposal of personal information that is not authorized by law. A breach may occur as a result or inadvertent errors or malicious actions by employees, third parties, partners in information sharing agreements or intruders.

lead investigator

- the person chosen to identify and analyze a breach. In most cases will be assigned to the Information and Communications Technology (ICT) department, Records Management, the Director of the department or a combination of all three.

Background The Yukon Government's *Health Information Privacy Management Act (HIPMA) and* Kwanlin Dün's *Freedom of Information and Protection of Privacy Act* (FIPPA) establish the rules for both governments regarding the collection, use, disclosure, disposal and protection of personal information. The governments are obligated to protect personal information by establishing reasonable security arrangements against such risks as accidental loss or alteration, and unauthorized access, collection, use, disclosure or disposal. Disclosure of personal information may only occur if authorized by the respective government's Act. Any other disclosure of personal information is a privacy breach.

There are a variety of ways a privacy breach may occur, such as:

- theft, loss or disappearance of equipment or devices containing personal information
- inappropriate record destruction
- the sale, transfer or disposal of equipment or devices containing personal information without a total purging of the item
- the transfer of equipment or devices without adequate security measures
- inappropriate use of electronic devices to transmit personal information including telecommunication devices
- intrusions that result in unauthorized access to personal information held in buildings, storage containers, computer applications, systems, Local Area Networks (LANs) or other equipment or devices
- low level of privacy awareness among staff, contractors or other third parties who handle personal information
- inadequate security and access controls for information in hard copy or electronic format on or off site
- the absence of or inadequate provisions to protect privacy in contracts or in information sharing agreements involving personal information
- insufficient measures to control access and editing rights to personal information that may result in wrongful access to and the possible tampering with records containing personal information
- there are also more fraudulent ways to obtain personal information such as:
    - the use of deceptive tactics to trick individuals into providing their personal information either directly or by going to a fake website. This is also referred to as "phishing". An example would be if an individual pretending to perform system maintenance calls an employee of an organization to obtain his or her security password.
    - The use of a fake copy of an official website to redirect users to a malicious website in order to steal information without the user's knowledge.

(Excerpt from the Treasury Board of Canada Secretariat's, *Guidelines for Privacy Breaches*)

Privacy Principles:

- Kwanlin Dün Health and Social Development Department must manage personal information in a privacy protective manner in compliance with the law

- an individual's right to protection of personal information when collected by the department
- transparency in how the Kwanlin Dün Health and Social Development Department protects personal information consistent with the government's policies
-

- Obligation to provide notification of any and all privacy breaches
- Continuous improvement of security standards

Roles and Responsibilities

Director, Manager and Supervisor

- ensures employees are aware of this policy
- monitors employee compliance
- ensures employees participate in training in information privacy management and breach prevention
- notifies Yukon Government of privacy breaches for Panorama
- notifies ICT of all information or privacy breaches
- notifies Records Management of all information or privacy breaches
- notifies the Executive Director of a privacy breach
- reviews and signs off on Privacy Breach Reports

All Health and Social Development Department employees

- have a legal responsibility for protecting all personal information they collect or have access to
- are accountable for adhering to this policy
- are responsible for notifying their supervisor immediately of any real or suspected breaches
- may only collect, use and or disclose personal information when necessary to carry out their specific job function

Clean Desk Policy

Purpose: the purpose of this policy is to establish requirements for maintaining a clean desk where sensitive and confidential information on Health and Social Development Department clients is kept secure in locked cabinets with limited access and out of sight

Policy: this policy is established to ensure Health and Social Development Department employees working with sensitive and confidential information, such as client records, in hard copy or electronic form are secure when leaving the work station for any length of time, and at the end of the work day.

Procedures:

- hard copies of client records and other sensitive or confidential information must be removed from the desk and locked in a drawer when the desk is unoccupied and the office door must be closed and locked.
- similarly, electronic client records and other materials containing confidential or sensitive information, must be closed and the computer locked when the desk is unoccupied and the office door must be closed and locked.
- at the end of the day, all sensitive or confidential documents must be returned to the locked filing cabinets.
- sensitive or confidential information must be removed from the printer immediately.
- disposal of confidential or sensitive materials must be in compliance with Kwanlin Dün's records management policies and carried out in coordination with Records Management staff. Transitory records must be either shredded or deposited in a securely locked confidential shredding bin.
- storage devices such as USB drives should only be used for short term storage of records and must be stored in a locked drawer.
- filing cabinets containing sensitive or confidential documents must be kept closed and locked when not in use or unattended. Filing rooms must be locked and keys for this area should not be left on an unattended desk.
- laptops should only be used for short term storage of records and must be password protected and stored in a secure place when not in use.

Password Management

Purpose: the purpose of this policy is to assist Kwanlin Dün Heath and Social Development Department network users to understand the password policy and how to effectively create and manage passwords

Principles:

1. The Kwanlin Dün Health and Social Development Department, as the steward and custodian of a large amount of data, including citizens' personal information, and technology infrastructure, requires a robust and effective system for protecting these assets.

2. User IDs and passwords are the primary authentication and access control tools used across the government. Adoption of a minimum password standard for the government network is a critical component to keep information secure and protect information privacy.

3. Successful implementation of password policy and protection of data and technology infrastructure is a collaborative process and is the shared responsibility of everyone.

Roles and Responsibilities:

Information and Communications Technology (ICT)

- Regularly review this policy and standards included within to ensure that the password protection policy remains robust, responsive to technological and other developments and appropriate to the risk to information security. ICT will amend the policy and standards as appropriate.
- Assist users to understand and comply with this policy and standards.
- Respond to security breaches or weaknesses that are identified or brought to ICT's attention.
- Ensure that new and existing software, systems and networks are protected with an appropriate level of password security.
- Be a central resource to work with government personnel on solutions that incorporate compliance with Kwanlin Dün's information security standards and policy requirements.

System Users

- Comply with the password standards established by this policy
- In the event of a password compromise or suspected compromise, immediately change the password and report it to ICT.
- Keep passwords secure and confidential and agree not to
    - Use the login password or other internal password for access to non Kwanlin Dün network, system or application.
    - Email the password
    - Share the password
    - Store passwords where others may gain access.

Application and system standards

- Kwanlin Dün's network will prompt users to comply with the password standards established in this document.

Strong Passwords

- Password will be at least **8** characters long
- Passwords will use a random mix of characters, including at least three from the following four categories to produce a strong password;
    - Lower case letters – a to z
    - Upper case letters - A to Z
    - Numbers – 0 to 9
    - Special Characters - ! @ # $ % ^ & * ( ) < > : " { } , . / ' ; [ ] \ | - _ + = ~ `

Password Reuse Rules

- Passwords will expire no later than 180 days from the date of their first use
- The system will store the last 24 pass words used

Non-compliance with this policy will result in disciplinary action. (See Human Resources Policy 7.2 Discipline or Appendix 4 of this policy)

Secure use of Removable Data Storage Devices Policy

USB drives will not be used to store confidential information.

Purpose: to provide guidance to all Health and Social Development Department staff on the secure use of removable data storage devices in order to prevent the loss of confidential data and prevent privacy breaches that may impact clients. **If a USB drive is used to temporarily transport information, it must be password protected or encrypted.**

Definitions:

Memory sticks – devices commonly referred to a "USB sticks" that contain memory space for the purpose of storing and transferring data

Encryption – method of protecting data by scrambling the data in a manner that renders it useless without a descrambling key or passphrase. The type of encryption is to be approved and maintained by Information and Communications Technology staff.

Malware – unauthorized software that can cause change of operation or security standards

USB, FIREWIRE, ESATA– common computer interface types for communicating with external devices, and all variations and updated versions. This is not to be considered an exhaustive list.

Policy: Removable storage devices or USB drives have become increasingly popular for storing data and are often used to download information from computers and to transport information to other computers.

Removable data storage devices shall remain the property of Kwanlin Dün and shall be returned to the relevant supervisor as part of the staff exit strategy (see personnel policy 10.3 Return of Kwanlin Dün Property, Appendix 5 of this policy)

Should a removable data storage device be lost or stolen, the process outlined in the Privacy Breach Policy will take effect and the employee will immediately notify his or her supervisor.

There are a number of risks associated with the use of removable storage devices, including:

- potential breach of privacy or loss of sensitive information if the device is lost or stolen
- corruption of data if not handled and stored properly rendering data or information inaccessible or altered
- transmission of viruses and or malware onto a computer network

- data or information being maintained on various devices creating the potential for lost devices going unnoticed for a period of time
- updated versions of data that is not available on the network

The following methods used to prevent and mitigate risks

- avoid physically carrying the information device unless needed
- use devices only when password protected or encrypted to protect data
- physically secure the device when it is not in use
- do not use personal USB drives on work computers
- do not plug unknown USB drives into a work computer as it may contain malware that will infect or steal information from the computer
- ensure that information contained on a USB drive is backed up on the network
- avoid transporting USB devices in checked baggage when travelling

USB drives cannot be used for data housed on the Panorama Database and should be used only when necessary to store information from other Health department databases.

Roles and Responsibilities

Staff

- Work with ICT to encrypt all USB drives that contain records.
- Ensure that any new personal and or confidential information or data stored on a USB drive is transferred promptly to an appropriate government information system and deleted from the USB drive
- Take a focused and deliberate approach to prevent the loss or theft of data in their possession
- Immediately contact ICT and their supervisor of lost or misplaced USB drives

HIPMA and FIPPA Coordinators (Privacy Officers)

- Comply with all HIPMA reporting requirements
- Assist with investigations into breaches of privacy
- Develop a database to monitor and track privacy breaches and provide regular reports to the senior management team
- Develop training and tools for managing privacy and breaches of privacy
- Develop a communications strategy to raise awareness of privacy/breach mitigation and management

The Yukon Government HIPMA coordinator will assist in investigations relating to privacy breaches on the Panorama or eHealth data bases. The Kwanlin Dün FIPPA Coordinator will assist in investigations relating to privacy breaches on all other Kwanlin Dün data bases.

APPENDICES

Appendix 1 Building After Hours Alarm Response Procedure

If the alarm (door/motion sensors/windows) is set off:

1. The KDFN security company shall be the first contact and responder for all after hours burglar alarms (5pm to 8am);
2. Initial response to alarm shall include inspection of the building exterior by the security firm;
3. Once inside, the alarm shall be reset, and an inspection of the interior shall proceed the security firm;
4. If an intruder is suspected, the RCMP are contacted to respond, as well as the primary contact from the department, in case the intruder is an employee working off-hours;
5. If no intruder is found, the primary is contacted to inform them of the false alarm;
6. If a burglary has occurred, the building director or manager will be required to attend the scene for an inventory of missing items.

IF Technical Malfunction:

A. Primary is initial contact for all after hours technical issues;
B. If it is determined by the call centre to be a technical issue, the primary can contact the security firm for further assistance.

Building Contacts:

Primary: _____ Phone: _____
Secondary: _____ Phone: _____
Tertiary: _____ Phone: _____

NOTE: All contacts, as well as all employees in the building, must be aware of the security code word for that building in the event they need to call Advance Security Response Centre.

Provided by Occupational Health and Safety

Appendix 2 Code of Conduct and Ethics (KDFN Personnel Policy)

A foundation of our Kwanlin Dün First Nation is respect: respect for our self, respect for others, respect for Elders and respect for the environment. It is important that we conduct ourselves in the workplace in a manner that reflects our values and way of life as a unique self-governing First Nation.
Further,

We agree to practice active listening and embrace healthy debate that respects all opinions, cultures and beliefs.

We agree that gossiping, spreading unfounded allegations and speaking about others in a negative way is hurtful and unprofessional, and will not be tolerated.

We agree to act with fairness, honesty, integrity and openness in our dealings with others.

We believe in a safe workplace that is free of harassment, abusive language and violence.

We believe that discrimination and racism has no place in our workplace.

We agree to treat everyone - members of the public and each other - with courtesy, professionalism, patience and fairness.

We agree that we are at our best as a self-governing First Nation when we all work together and support each other as a team.

We are committed to the ongoing improvement of the Kwanlin Dün First Nation through the positive interchange of skills, knowledge and experience.

As KDFN employees, we agree not to discuss or participate in Chief and Council politics while at work.

We agree to lead by example, do our best for the Kwanlin Dün community and take pride in our work.

We believe in respecting our Elders at all times.

We agree to not knowingly take advantage of or personally benefit from information that is obtained in the course of our employment at Kwanlin Dün.

We agree to maintain the confidentiality of information entrusted to us except in circumstances where disclosure is authorized or legally mandated.

In performing our work at Kwanlin Dün, we agree to be knowledgeable and respectful of Kwanlin Dün culture, traditions and way of life.

_____ _____

Employee Date

Appendix 3 **KDFN Employee Oath of Confidentiality** (KDFN Personnel Policy)

In the performance of my duties, I may have access to confidential information about this Government's business affairs and operations, and personal information about the Citizens and general public that it serves. I understand that:

- Respecting the privacy of individuals, safeguarding the confidentiality of information and maintaining the security of information systems is extremely important for the credibility and well-functioning of this Government. It is the collective responsibility of all KDFN employees to adhere to the provisions of the *Freedom of Information, Protection of Privacy Act* when dealing with the personal information of other employees, our clients and Citizens, and to safeguard this information against unauthorized disclosure, loss, tampering, unwarranted access or use by unauthorized persons.

- Our ability to maintain confidentiality and security of information promotes integrity in our relationships with Citizens, the general public, fellow staff, contractors, and other governments and agencies.

- Personal information about clients and Citizens acquired through my employment with KDFN is considered confidential and not to be shared with members of the public, unless it has been released to the public in published form or approved for release by Chief and Council.

- I will not make public statements to the media, expressly or implied, on behalf of KDFN.

- Breaches in confidentiality and unauthorized use of private information must be reported immediately to my supervisor or Human Resources. Further, I am aware that I may be subject to disciplinary action, including termination of my employment for cause, or possible legal action should I violate this oath.

I understand that this oath continues with me even when I have left the employ of KDFN.

Signed this _____ day of _____, 20___

_____ _____

Employee's signature Employer's signature

Appendix 4 Discipline (KDFN Personnel Policy 7.2)

Purpose: Correct unsatisfactory performance or behaviour, promote a healthy positive climate of self-discipline and consistent and effective group standards, and ensure that employees are treated fairly and consistently.

Policy: Employee misconduct or incompetence will be subject to progressive disciplinary action aimed at improving employee performance.

Procedure: **1. Disciplinary Action**

There are three general grounds for disciplinary action:

a) Incompetence

Incompetence occurs when an employee does not have the abilities or skills to perform the assigned duties and responsibilities associated with the position.

b) Negligence

Negligent employees may have the required skills but fail to perform at an acceptable or satisfactory level.

c) Misconduct

Misconduct means that policies have been ignored, such as irregular attendance, tardiness, poor attitude towards work or other employees, safety violations and insubordination, all of which may cause a direct or immediate impact on the service delivery, safety or negatively affect the attitudes of other employees, citizens or reputation of KDFN.

Employees are expected to be aware of and, where required as part of their work, understand the legal and regulatory measures enacted and approved by KDFN.

The attributes of discipline involve the provision of an initial warning and responding to concerns in an immediate and consistent manner. Concerns addressed must relate directly to the requirements of the workplace and should not be deemed as a personal attack. The ultimate goal is to correct the problem and retain the employee.

The objectives of disciplinary action will be positive in that they will be corrective and educational rather than negative and punishing.

Disciplinary action will be consistent and fair and apply to everyone. In similar conditions and circumstances, consistent disciplinary action should be taken.

Generally, discipline will be progressive in nature, moving in steps from a minor reprimand for the first offence to discharge as the final action.

Some offenses are considered so serious that they are not dealt with by way of progressive discipline, (e.g. fighting, verbal or physical threats, theft, fraud, forgery, breach of confidentiality, breach of the public trust, serious safety violations that could lead to injury/death or significant financial loss). An employee who commits these offences or similar offences may be dismissed immediately. Employees who commit serious offences may also be suspended without pay, by the Executive Director, for a period of time commensurate with the nature of the offence.

Disciplinary documentation will be placed on an employee's personnel file in a sealed envelope. After two years without further disciplinary action, employees may request that disciplinary documentation be removed from their personnel file. This will allow the employee to have a clean employment record.

Supervisors, managers or departmental directors dealing with disciplinary issues must involve and work in cooperation with Human Resources prior to taking any action. Any and all documentation related to staff relations and/or disciplinary action will be maintained in Human Resources only where access is restricted and essential confidentiality can be assured.

Employees are entitled to dispute any disciplinary action through the process set out in policy section 7.3 Dispute and Complaint Resolution.

2. Steps – Progressive Disciplinary Process

Verbal Reprimand

A verbal reprimand is given to the employee followed by written confirmation to be placed on the employee's personnel file that documents a full accounting of the reprimand.

Written Reprimand

The written reprimand will be specific and:

a) include the date(s), time(s) and location(s) of incident(s);

b) describe the nature of the undesirable performance or behaviour and how it relates to job and organizational performance;

c) identify the section in the Personnel Policy and Procedures and/or Occupational Health & Safety Manual that relate to the incident(s);

d) document any and all discussion and information related to the incident(s), including employee and supervisor responses, and where possible including specific words and actions; and

e) identify, if any, witnesses to the incident

Suspension

In the event that an employee fails to respond to previous measures taken to improve job performance or conduct, the next step in the disciplinary process should be a suspension without pay. The length of suspension will be commensurate with the seriousness of the infraction. Suspensions can range from one day to a maximum of 10 working days. As with every step in the progressive disciplinary process, clear documentation is to be provided to support the action taken as a final attempt to correct incompetence, negligence or misconduct.

Dismissal (Discharge) for Cause

Dismissal should be considered only where an employee fails to respond to all previous measures taken to improve their job performance or conduct.

Personnel files will contain well-documented records of disciplinary history and performance evaluations of employees, including comments of supervisors, a record of disciplinary action taken, the remedial efforts made by an employee and correspondence between supervisor and the employee with regard to work performance and misconduct.

The Executive Director will review all disciplinary action taken up to this step before initiating a dismissal.

In the case of a discharge, a termination letter will be given to the employee signed by the Executive Director. A termination letter for the Executive Director will be signed by the Chief.

All documentation will be recorded promptly, objectively, and based on observations and not impressions. This notification will be sent to the employee and a copy placed in their personnel file.

Appendix 5 Return of KDFN Property (Personnel Policy 10.3)

Scope: All employees

Purpose: Ensure that all KDFN property, including safety equipment and intellectual property, is properly cared for and returned upon termination of an employee.

Policy: Upon termination of employment, all KDFN property will be returned to KDFN.

Procedure: Employees will be responsible for all KDFN property issued to them, created for KDFN by them, or in their possession or control.

Property of KDFN includes work materials, supplies, equipment, information, computers, keys and intellectual property. Intellectual property is defined as documentation, research, policy, reports, email and text message communication and similar information specific to employment with and for KDFN.

Where permitted by applicable laws, KDFN may withhold and recover from the employee's pay cheque the cost of any items that are not returned when required.

KDFN may take all action deemed appropriate to recover or protect its property.