

Wahnapiṭae First Nation

SECURITY-1: INFORMATION SECURITY POLICY

ADOPTED BY BAND COUNCIL MOTION	BCM #WFN 18/19-014
DATE OF ADOPTION AT CHIEF AND COUNCIL MEETING	MAY 8, 2018
APPROVAL REVIEW AND REVISION DATES:	Every 3 years

1.0 POLICY

The health organization will ensure that an effective information security program is implemented to safeguard sensitive information involved with the delivery of health care services and programs. This includes access and activity on all computer devices, networks and software related to electronic health data and information including password management. Every employee, contractor, student and volunteer (staff) who has access to and deals with sensitive information on paper or in health management systems will be made aware of the program to protect themselves, the health organization's reputation to establish community trust.

Staff who fail to follow this policy will result in temporary or permanent suspension of access to the information and systems, and include disciplinary action up to and including termination, cancellation of contractual arrangement, as well as civil and criminal action. If a user is unsure about how to comply with any aspects of the established security program, they should contact their immediate supervisor or the organization's security contact or their designate.

1.1 Health Organization Operations – involved persons

The health organization is dependent in many ways on information and health information management systems, so information security should be a team effort. If sensitive information is unavailable, unreliable, or disclosed improperly, the organization and the clients could suffer serious harm or loss.

Operational responsibilities of all users to help prevent and respond to different types of threats to information and information systems include unauthorized access, disclosure, duplication, modification, appropriation, destruction, loss, misuse, and denial of use. All employees, contractors, students and volunteers must treat these security measures as confidential.

1.2 Involved Systems

This policy applies to all computer devices and network systems owned by and/or administered by the health organization, as well as any personal devices if authorized to be used for work. It applies to all platforms (operating systems), all computer sizes (from personal digital assistants through to servers), and all software (whether developed by the organization or purchased from third parties). The policy covers only information handled by computers and/or networks. Although this document mentions other forms of information such as voice and paper, it does not directly address the security of information in these forms.

1.3 Security Program Management and Operations

Responsibility for the security program management is assigned to the organization's security contact and management team. The security program management process follows the requirement for

appropriate separation of duties. For example, the person requesting access to information cannot be the person approving the request.

1.4 Authorized Support Personnel Responsibilities

The organization's security contact and authorized support personnel are responsible for the following functions that support the security program:

- Act with "Administrator" privileges on all computers. Ensure that end users do not have Administrator privileges unless authorized by the health organization's management team;
- Manage the security of the computer network and infrastructure;
- Ensure that a record is kept of users that have keys, fobs, passcodes or alarm codes for secure areas;
- Ensure that a record is kept of all information and information technology assets;
- Ensure that user roles and access privileges are reviewed at least once a year to ensure that they are still appropriate for each user's job function;
- Ensure that background reference checks are performed on individuals prior to granting user access to secure areas or systems;
- Ensure that all users have signed the 'Confidentiality and Acceptable Use Acknowledgement' prior to receiving access to information and information systems and annually thereafter;
- Enable and disable user accounts on direction from the organization's management team. In particular, accounts must be disabled within 24 hours of the end of the user's relationship with the organization;
- Ensure that firewalls are used on portable devices and dedicated internet links (ADSL, Cable);
- Manage all computer equipment installations, disconnections, modifications, repairs, servicing and relocations;
- Ensure that users back up data on personal computers and laptops, including documents, contact lists, and email messages. All backups containing critical or confidential information must be stored at an approved off-site location with physical access controls or encryption;
- Ensure that all software used to carry out the business of the organization is appropriately licensed;
- As applicable, ensure that Virtual Private Network (VPN) Split tunnelling is disabled;
- Ensure that current virus detection software is installed on all technology assets including mobile devices, operating correctly, and configured to automatically update daily;
- Identify the encryption tools to be used when PHI is stored on laptop computers and for secure transmission by email. Assist users with the use of encryption;
- Ensure that software is updated on a regular or automatic basis. In particular, recommended security patches are installed for the operating system and other applications in use;
- Monitor the computer network for unauthorized access, viruses, spyware and other security breaches;
- Ensure that all user access to systems is automatically logged with the user's login name, date and time of access, the system / application accessed, and the action taken.
- Ensure that computer access logs are saved securely for a period in accordance with the organization's policy for retention (e.g. for a minimum of two years);
- Ensure that clinical files are saved securely for a period in accordance with the organization's

policy for record retention;

- Investigate any alleged misconduct in consultation with the organization's management team. All investigations will be performed on a case-by-case basis.
- Document procedures for key business processes such as system backup and restore, software upgrades, patch management, etc.

1.5 Physical and Access Location Security

Access to every office and room in the health organization that contains confidential (non-public) information is physically restricted to only people who have a need to know. The organization's security contact or their designate should establish physical key/fob management protocols for all employees, contractors, students and volunteers accessing the physical areas in the organization that contain sensitive information.

- Authorized users will be given keys or door pass codes to allow access to secure areas of the health organization. Key computer system components have battery backup to protect equipment and information if there is a power failure.

1.6 User IDs and Passwords

Each staff member, contractor, student or volunteer accessing the health organization's computer systems has a unique user identification (user ID) and a private password. User IDs are used to limit access to the system based on the job duties and role of each user. Each worker is personally responsible for his or her user ID's and passwords and no master password list should be maintained by any staff member or IT service provider. The following protocols should be followed:

- User ID's & Passwords

Passwords are personal to each authorized user. There are no shared accounts. Users may not access computers or networks anonymously, such as by using "guest" user IDs.

- Easy to remember but difficult to guess passwords

To minimize the risk of unauthorized access and maintain password confidentiality, user passwords should be easy to remember but hard for others to guess. Passwords must not be related to the user's job or their personal life. For example, the following should not be used as passwords:

- User's address, spouse's name or licence number; or
- Single words including names, places, slang words or technical terms.

Password controls should be in place to support the principle of passwords being difficult to guess. As much as possible, these controls are managed automatically. For example, passwords are set to expire every 3-6 months so that users have to change their passwords frequently to ensure security.

1.7 Release of Information

Unless it has been specifically designated as public information, all information maintained by the health organization must be protected from disclosure. This includes client demographic data (such as name and address), contractual and employment information, and data in summary form (such as immunization coverage reports). All release of information (except public information) must be approved. Such information releases may include questionnaires, surveys and interviews, but does not include client requests for access to their own information or a person for whom they are a substitute decision maker.

1.8 Network Infrastructure Security

Only authorized devices will be permitted to access the organization's network. Wireless access points,



peer-to-peer wireless connections and Wi-Fi personal devices of any kind must not be connected to the network without management approval. Network devices connected to the computer network must not be modified, disconnected or relocated without management approval.

- Health organization management reserves the right to suspend access at any time, without notice, for technical reasons, possible policy violations, security or other concerns to the organization's network.
- Health organization management, at its sole discretion, will determine what materials, files, information, software, communications, and other content and/or activity will be allowed or banned.
- Users may have access via the network to PHI, employee records, financial information and other confidential information. All access to such information must be authorized and used only for conducting the business of the health organization.

1.9 Internet Access

Employees, contractors, students and volunteers are provided with internet access if needed to perform their job functions. Such access may be terminated at any time at the discretion of the worker's supervisor. Internet use is monitored to ensure that workers do not visit internet sites unrelated to their work and for potential security issues.

Specific authorization is required in advance for workers to do the following:

- Represent the health organization in internet discussion groups or other forums; or
- Post any information (including public information) managed by the organization to the internet.

All information received from the internet should be treated cautiously unless the source has been confirmed to be reliable.

1.10 Electronic Mail

Employees, contractors, students and volunteers who use computers for their work are given an email address. It is recommended that email communication on behalf of the health organization use the email address issued by the organization. The use of personal email addresses is not recommended.

- A standard email "signature" (authorized by the organization's management team) that includes the user's full name, job title, address, and phone number, along with a privacy statement should be used.
- Sending sensitive information in the body of an email should not be done. If email is used the recommended approach is to use general language without any client identifiable information in the body of the email and attach a word or excel document that is password protected – once sent following up with phone call to the recipient providing the password.
- When sending emails to groups of recipients, the blind carbon copy (Bcc) feature or a distribution list should be used to avoid revealing the email addresses of other recipients. Sound judgment must be used when distributing messages. Client-related messages should be carefully guarded and distributed to only the essential people. Staff must also abide by copyright laws, ethics rules, and other applicable laws.

1.11 Computers, Laptops, Peripherals, Media/mobile Devices Device Security

The following security program measures apply to the use of all computer equipment provided by the health organization, and should be made known to staff, contractors and volunteers by the health organization's security contact or their designate:

- All computer equipment and mobile devices including peripheral portable storage should be kept away from obvious hazards such as direct cold, heat, smoke and liquids;
- Only authorized organization support personnel are permitted to service electronic equipment and devices;
- All computer equipment must have proper physical security mechanisms in place (i.e. be protected by key locks and cables and/or alarms or stored in a security locked and hazard-free location) when not in use or left unattended or in open areas to avoid risk of theft.
- The security contact or their designate must ensure that data on computers and laptops is backed-up. All backups containing critical or confidential information must be stored at an approved off-site location with physical access controls or encryption.
- All computers and portable devices (e.g., laptops and cell phones) that access the network and/or data must be password protected.
- Automatic password protected screen savers must be used with timeout periods appropriate to the sensitivity of the data being accessed (For example, the more sensitive the information, the faster a screen saver should activate during periods of inactivity).
- Computers must not be left logged on when unattended or at the minimum should be locked or shut down completely when not in use. The automatic log off must be set to run after a short period of inactivity;
- Any computer device displaying confidential information must be positioned out of public view.
- Users must ensure that confidential information is not left unattended on desks or on computer screens unless the doors and windows into the room where the computers are located are locked.
- Users are not provided with administrator privileges on any computer system, with the exception of authorized support personnel and any individuals authorized by the organization's management team.

1.12 Remote and Mobile Usage of Computers, Laptops, Peripherals, Media and Mobile Devices

Staff, contractors, and volunteers should follow all protocols in the previous section 1.11 when using equipment remotely. Additionally, with remote usage, requirements also include the following:

- Personal mobile devices must not be connected to the network without management approval;
- Users must not take portable devices or media off the premises without the informed consent of their immediate supervisor. Informed consent means that the supervisor knows what equipment is leaving, what data is on it and the purpose for its use;
- Remote access to the network, applications, and data is for business purposes only. The organization's management team must approve all remote access to sensitive information;
- Log in passwords must be used on all remote-computing devices;
- Users should not use the "Remember Password" feature of any software application (e.g. Internet Explorer);
- Computers and mobile devices supplied by the organization must not have their hardware or



software configuration changed in any way, without management approval. Only authorized support personnel are permitted to make configuration changes;

- All portable laptops, notebook computers and mobile devices, including storage media, must use standard encryption technology when used to carry personal identifiable information or other confidential electronic data;
- Refrain from using remote access while travelling, particularly at airports or working outside the province/territory including while outside Canada.

1.13 Network Threats and Malicious Code from External Sources

All users are responsible for following security protocols while accessing the computer network and services to protect the organization against viruses, worms, Trojan horses and other malicious code. The following security measures are required of all employees, contractors, students and volunteers to minimize these threats:

- All software installation must be coordinated through authorized support personnel;
- Users must not knowingly allow malicious code such as spyware, worms, viruses or other software that may cause a threat to the network to be installed on computers managed by the organization;
- Before use, users must scan for viruses on all portable storage media (including CDs, DVDs, and media sticks) that are new or are of unknown origin;
- The downloading or installing of any files is not permitted unless authorized by the organization's management team. This includes (but is not limited to) software programs, screen savers, music and video files from the internet;
- Only software with a license agreement and management approval is to be installed on computers;
- Any user who suspects that his/her workstation has been infected must immediately power off the workstation and call their authorized support personnel. Users must not attempt to destroy or remove malware, viruses, spyware and/or other internet-born security threat, or any evidence of them, without direction from authorized support personnel;
- Users must immediately report to their direct supervisor and authorized support personnel any signs or suspicions of computer or network tampering, intrusions, or security breaches; and
- If any computer device is damaged, lost or stolen, the user must immediately notify their direct supervisor and follow the Incident Management process.

1.14 Right to Search and Monitor

The organization's management team or their authorized agents have the right to monitor, inspect, or audit all information systems used by the organization staff, contractors, students and volunteers. Such an examination may take place with or without consent, or the knowledge of the involved people. The information systems subject to examination may include among others:

- Email files;
- Hard drive files;
- Voice mail files;
- Printer files;
- Fax machine printouts; and
- Desk drawers and filing cabinets

Employees, contractors, students and volunteers should have no expectation of privacy regarding information stored in or sent using the organization's information systems.

Audits may be performed:

- in response to a complaint or concern;
- in response to a trigger from system monitoring software;
- on a proactive, scheduled or random basis.

2.0 ADDITIONAL REFERENCES

All policies are interrelated and have some similar content - it is highly recommended that you review and become familiar with these other policies which will provide a richer context to Security-1 Information Security Policy:

Privacy-1 Statement on Privacy Guidelines

Privacy-4 Security Contact Responsibilities

Privacy-13 Client Access and Release of Information

Privacy-15 Sending and Receiving Information

Security-7 Incident Management

3.0 POLICY - ACTION ITEMS

Action Items referencing the set of tools (forms, templates, checklists) available in the excel document 'Privacy & Security Implementation Workbook' ('Workbook') that are used to implement the policy if the health organization decides to implement the policy as written. These tools can also be leveraged if the health organization already has protocols and tools in place that may need augmentation.

The action items/tools listed may also be referenced in other policy/s action item lists as all privacy and security policies have interrelated content.



These action items will be recorded in the health organization's 'Action Plan' also housed in the 'Workbook'.

Privacy & Security Implementation Workbook		
Action Item TAB-Tool	Purpose	Policy content section it supports
<i>User Access Audit Templates</i>	Provides the health organization with 3 audit Checklists to leverage for conducting required user audits associated with personal health information 'PHI' or clinical systems.	1.4
<i>C&A Use Acknowledgement template</i>	Provides a template to leverage - for contractors, students and volunteers (i.e. deemed as 'staff') working with the health organization - to read, acknowledge and sign to ensure all sensitive information held is protected.	1.4
<i>Password</i>	To provide the health organization staff with tips for password management for devices and systems - which	1.6

Management Tips	is a key consideration to maintain privacy and security for personal health information.	
------------------------	--	--

X 
Ted Roque
Chief




Page 8 of 8


Wahnapiatae First Nation

SECURITY-2:MOBILE DEVICES POLICY

ADOPTED BY BAND COUNCIL MOTION	BCM #WFN 18/19-014
DATE OF ADOPTION AT CHIEF AND COUNCIL MEETING	MAY 8, 2018
APPROVAL REVIEW AND REVISION DATES:	Every 3 years

1.0 POLICY

The health organization will ensure that employees, contractors, students and volunteers ('staff') who have access to and control of personal health information 'PHI' know they have a responsibility to protect the privacy of information stored on their mobile devices to mitigate risks associated with their use which includes devices issued by the organization and personal devices if authorized for use by the organization.

Mobile devices such as smart phones, laptops, tablets and USB keys offer convenience; however, they raise risks for privacy and the protection of PHI. They are also at risk of threats such as viruses and spyware. All staff will read, understand and sign the health organization's 'Confidentiality & Acceptable Use' that includes a section acknowledging their responsibility to protect PHI when using mobile devices.

1.1 The following policy protocols should also be followed by all staff to help reduce the risks associated with the use of their mobile devices:

- Turn off calendar reminders, text/message popups, email popups etc. to prevent exposing sensitive client information that may be in them;
- Learn how to enable privacy and security settings on the mobile device;
- Only store PHI on the mobile device if it is absolutely necessary;
- Ensure that mobile devices are protected with hard-to-guess passwords;
- Use an automatic lock feature so a password is required to access information;
- Use encryption technology to provide added protection for PHI. If using a USB mobile stick – encryption must be in place or it must not be used to store sensitive information.;
- Install and run anti-virus, anti-spyware, and firewall programs on mobile devices – and keep those programs up-to-date;
- Don't send PHI over public wireless networks (e.g. coffee shop hot-spots). Public wireless networks may not be secure and there is a risk that others may be able to capture the information;
- Keep mobile devices in sight. Never leave a mobile device unattended in a public place or a vehicle;
- Keep laptops locked up when not in use – a security cable attached to an immovable piece of furniture will deter theft;

- Ensure that information stored on a mobile device is purged before the device is discarded.

2.0 ADDITIONAL REFERENCES

All policies are interrelated and have some similar content - it is highly recommended that you review and become familiar with these other policies which will provide a richer context to the Security-2 Mobile Device Policy:

Security-1 Information Security Policy

3.0 POLICY - ACTION ITEMS

Action Items referencing the set of tools (forms, templates, checklists) available in the excel document 'Privacy & Security Implementation Workbook' ('Workbook') that are used to implement the policy if the health organization decides to implement the policy as written. These tools can also be leveraged if the health organization already has protocols and tools in place that may need augmentation.

The action items/tools listed may also be referenced in other policy/s action item lists as all privacy and security policies have interrelated content.

These action items will be recorded in the health organization's 'Action Plan' also housed in the 'Workbook'.

Privacy & Security Implementation Workbook		
Action Item TAB-Tool	Purpose	Policy content section it supports
<i>C&A Use Acknowledgement template</i>	<i>Provides a template to leverage - for contractors, students and volunteers (i.e. deemed as 'staff') working with the health organization - to read, acknowledge and sign to ensure all sensitive information held is protected.</i>	1.0

X

Ted Roque
Chief

Wahnapitae First Nation

SECURITY-3: INFORMATION TECHNOLOGY ASSET MANAGEMENT POLICY

ADOPTED BY BAND COUNCIL MOTION	BCM #WFN 18/19-014
DATE OF ADOPTION AT CHIEF AND COUNCIL MEETING	MAY 8, 2018
APPROVAL REVIEW AND REVISION DATES:	Every 3 years

1.0 POLICY

The health organization will maintain an inventory for all information and information technology assets accessed and/or used by employees, contractors, volunteers and students within the health organization.

- 1.1 **Information Assets:** Includes personal health information 'PHI' in both electronic and paper form and other types of information that are not considered 'PHI' but are still important to the organization, such as financial reports and operating plans.
- 1.2 **Information Technology (IT) Assets:** includes all hardware and software used to deliver the health organization's programs and services.
- 1.3 When assets are purchased, assigned to a health organization employee, contractor, student or volunteer ('staff'), or retired from use, the Asset Management Inventory form should be updated and kept current. At the minimum information captured for each asset should include the following:
 - Asset Name
 - Description
 - Type
 - Used to store PHI?
 - Critical to Operations?
 - Linked to BCP (Business Continuity Plan)?
 - Backup Profile
 - Arrived on (Date)
 - Retired on (Date)
 - Serial Number
 - Make
 - Model
 - Location

2.0 ADDITIONAL REFERENCES

All policies are interrelated and have some similar content - it is highly recommended that you review and become familiar with these other policies which will provide a richer context to the Security-3



Information Asset Policy:

Security-1 Information Security Policy

3.0 POLICY - ACTION ITEMS

Action Items referencing the set of tools (forms, templates, checklists) available in the excel document 'Privacy & Security Implementation Workbook' ('Workbook') that are used to implement the policy if the health organization decides to implement the policy as written. These tools can also be leveraged if the health organization already has protocols and tools in place that may need augmentation.

The action items/tools listed may also be referenced in other policy/s action item lists as all privacy and security policies have interrelated content.

These action items will be recorded in the health organization's 'Action Plan' also housed in the 'Workbook'.

Privacy & Security Implementation Workbook		
Action Item TAB-Tool	Purpose	Policy content section it supports
User Asset & Access Template	Eight (8) forms to manage the health organization users' access to systems and physical environments in your organization.	1.3
P&S Asset Management Inventory	Provides a template to help manage all assets used to work with personal health information 'PHI' (information, hardware and software assets) when onboarding/off boarding staff (including volunteers, contractors, etc.) by anyone working with the health organization.	1.3

X

Ted Roque
Chief

Wahnapitae First Nation

SECURITY-4: BUSINESS CONTINUITY MANAGEMENT PLAN POLICY

ADOPTED BY BAND COUNCIL MOTION	BCM #WFN 18/19-014
DATE OF ADOPTION AT CHIEF AND COUNCIL MEETING	MAY 8, 2018
APPROVAL REVIEW AND REVISION DATES:	Every 3 years

1.0 POLICY

The health organization will have a Business Continuity Management 'BCM' plan in place to help the organization to continue its operations following a disaster or disruptive event. Examples of such events include fire, floods, power disruption, information system failure, illness that affects large numbers of people, etc. The BCM plan involves establishing business continuity and disaster recovery plans for all services, clients, employees, contractors and volunteers.

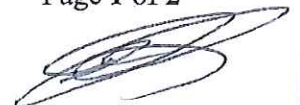
1.1 Key Individuals involved

The health organization's Business Continuity Management Plan 'BCMP' will require a Coordinator, active and committed support from a team of senior staff, and input from key individuals from across the organization:

- i. The **BCM Coordinator** is a person working for the health organization that organizes the BCMP, takes direction from the BCM Senior Team, and works with key individuals in the organization to ensure that departments across the organization participate and contribute to the plan. Identify an Alternate BCM Coordinator and identify the reasons when delegation to the Alternate will occur (e.g. primary BCM Coordinator is not available due to illness or vacation).
- ii. The **BCM Senior Team** provides strategic direction and guidance for the BCM process, approving BCM-related policies.
- iii. Key Individuals represent the different business areas of the organization, acting as contacts for planning purposes and as leaders when a disruptive event happens.
- iv. In the event of a disruption, the delegated individuals will be responsible for assessing the damage and directing recovery activities.
- v. All key and authorized individuals will have a copy of the BCMP and any supporting documentation housed in a secure location with restricted access - that can be reached in the event of a disruption (e.g. a copy at an authorized person's home, a copy located within the health organization facilities, and all relevant documentation required to recover critical information assets (refer to the Information Asset Management Log) and essential services that are affected by a disruption.

2.0 ADDITIONAL REFERENCES

All policies are interrelated and have some similar content - it is highly recommended that you review and become familiar with these other policies which will provide a richer context to the Security-4 Information Asset Policy:




3.0 POLICY - ACTION ITEMS

Action Items referencing the set of tools (forms, templates, checklists) available in the excel document 'Privacy & Security Implementation Workbook' ('Workbook') that are used to implement the policy if the health organization decides to implement the policy as written. These tools can also be leveraged if the health organization already has protocols and tools in place that may need augmentation.

The action items/tools listed may also be referenced in other policy/s action item lists as all privacy and security policies have interrelated content.

These action items will be recorded in the health organization's 'Action Plan' also housed in the 'Workbook'.

Privacy & Security Implementation Workbook		
Action Item TAB-Tool	Purpose	Policy content section it supports
<i>Business Continuity Plan 'BCP'</i>	Provides a Business Continuity Plan 'BCP' template to support the continuity of health care service delivery in the event of a disruption resulting in the unavailability of facilities, systems and/or associated hardware. Provides five TABLES that can be filled out so that you are prepared in the event of a disruption to the operations of the health organization.	1.0
<i>BCP - TABLE - Health Organization BCM CONTACTS</i>	Provides a tool for documenting the key people involved with the BCM plan.	1.1 'F'
<i>BCP – TABLE- BCM Documents Referenced During Disruptions</i>	Provides a tool to document health organization records of where key documents are located.	1.0


 Ted Roque
 Chief

Wahnapiatae First Nation

SECURITY-5: USER ACCESS AND ACTIVITY AUDIT POLICY

ADOPTED BY BAND COUNCIL MOTION	BCM #WFN 18/19-014
DATE OF ADOPTED AT CHIEF AND COUNCIL MEETING	MAY 8, 2018
APPROVAL REVIEW AND REVISION DATES:	Every 3 years

1.0 POLICY

The health organization will ensure that regular privacy and security user access and account activity audits are conducted for each employee, contractor, student, or volunteer (staff) to validate that the scope of their access continues to be relevant to the individual's job duties as well as to identify breaches that require incident management. This includes audits for access and activity relevant to electronic information as well as physical access and activity (e.g. buildings, keys).

Where there is a potential to view sensitive clinical information in the data being reviewed during the audit at least one clinical staff member must be involved. Other staff members including the organization's privacy/security contact or designate could be present for the part of the audit that does not include sensitive clinical client data.

1.1 What should trigger an audit?

The frequency and type of auditing should be a risk-based decision taking into account risk-related factors such as:

- Size of the health organization;
- Number and variety of users;
- Scope of user access;
- Frequency of access to PHI;
- Sensitivity of the information;
- Access by third parties;
- History of previous privacy breaches or incidents.

Reactive access audits are conducted based on a specific complaint, request, incident or other activity that suggests a user may have inappropriately accessed physical locations, sensitive information or abused special privileges.

Proactive access audits must be conducted at least annually and when triggered by staff changes. They may be conducted more frequently (periodically or semi-annually) based on highly sensitive situations such as access to highly sensitive clinical information or where staff may have family or personal relationships with clients.

1.2 Proactive Access Auditing threat examples

The following list of threat use cases are used to guide the frequency and scope of the access audit. Other threat use cases will be included as they are identified.

- A user accesses their own record or records of a family member.
- A user accesses PHI outside of normal working hours.
- A user accesses PHI from an unusual location (e.g. user is based in one location and is accessing client health files in another location).
- A user accesses a large number of health files over a short period of time for his/her job function.
- A user conducts a large number of client searches for his/her job function.
- A user generates a lot of system errors such as frequent login errors, or client not found errors.
- A user accesses a high-profile client and they are not in that person's circle of care.

1.3 Responsibility to Inform Staff about Audit

During Privacy and Security Awareness Training, that should be conducted for all staff annually at a minimum, the privacy contact will ensure that staff:

- Commit to the confidentiality and acceptable use requirements e.g. by signing/resigning the appropriate form;
- Are reminded that their access and activity is regularly audited and that there are consequences if inappropriate access/activity is determined up to and including dismissal;
- Are reminded that if a user suspects inappropriate access they should report it without concern of retaliation.

1.4 Managing Privacy/Security Audit Outcomes

If the outcome of any audit identifies a potential privacy and/or security breach, it must be documented and reported using an 'Incident Reporting Form' and investigated in accordance with the health organizations policies.

1.5 Types of Privacy Access Audits

The health organization's privacy contact or designate will ensure the following types of audits are regularly conducted:

- User access requirements** – applications - user access (including employee, contracted resources, student, volunteer) to system application menus and functionality to ensure the access continues to be relevant to the individual's job duties. This review must also confirm that the scope of access is appropriate. For example, the role(s) assigned in clinical systems (applications) is appropriate for the staff member at the time of the audit. If necessary changes are identified, immediate action must be taken to decommission access or provision a different role to the user;
- User account activity** – applications - user account activity to identify inactive accounts (e.g. no recent activity). If inactive user accounts are identified, the audit must verify whether these accounts are still required by the individuals to perform their job duties. If a user account is no longer required, it must be immediately decommissioned;
- User access** – information - user access to sensitive and important information assets to identify possible inappropriate access;
- Consent-related updates** - user access to a client health file when consent directives have been added, removed, modified or overridden to ensure that user access is appropriate, and the client was notified of consent overrides.

1.6 Types of Security Access Audits (physical & electronic)

The health organization's security contact or designate will ensure the following types of audits are regularly conducted:

- i. **User Physical access** – user access to buildings/offices/clinical rooms, wiring closets, communications cables and areas storing sensitive information to identify potential security weaknesses or breaches, or any unusual patterns and anomalies of access to or unsuccessful attempts to access the sensitive and important information. This includes access to keys, access badges, FOBs, and alarm codes (e.g. buildings, offices, file cabinets, desks, etc.);
- ii. **User Computer-based tool access** – user access to email, internet, network drives, network logs, system logs, ability to install software, personal computers, printers, scanners, fax machines, cell phones, cameras, intranet, other special equipment, etc.;
- iii. **Documentation systems** – user access to systems such as electronic medical records or other clinical systems, financial systems, etc. to ensure that the access is appropriate.
- iv. **Special privileges** - such as afterhours access to buildings, remote access to computer-based networks and tools, ability to take sensitive data offsite, access to sensitive file storage areas such as personal information storage areas, privacy and security records, system and user access logs, archived records, etc.

1.7 Incident/ Breach from an Audit

An audit may reveal a possible incident or breach when PHI may have been stolen, lost, subject to unauthorized use/access or disclosure such as unauthorized copying, modification or disposal, or as a result of a privacy or security failure. Possible incidents or breaches must be investigated following applicable health organization policies.

2.0 ADDITIONAL REFERENCES

All policies are interrelated and have some similar content - it is highly recommended that you review and become familiar with these other policies which will provide a richer context to the Security-5 User Access and Activity Audit Policy:

Privacy-18 Whistle Blower Protection Policy

Security-6 Privacy and Security Breach Incident Response Policy

3.0 POLICY - ACTION ITEMS

Action Items referencing the set of tools (forms, templates, checklists) available in the excel document 'Privacy & Security Implementation Workbook' ('Workbook') that are used to implement the policy if the health organization decides to implement the policy as written. These tools can also be leveraged if the health organization already has protocols and tools in place that may need augmentation.

The action items/tools listed may also be referenced in other policy/s action item lists as all privacy and security policies have interrelated content.

These action items will be recorded in the health organization's 'Action Plan' also housed in the 'Workbook'.

Privacy & Security Implementation Workbook		
Action Item TAB-Tool	Purpose	Policy content section it supports
<i>C&A Use Template</i>	Provides a template to leverage - for contractors, students and volunteers (i.e. deemed as 'staff') working with the health organization - to read, acknowledge and sign to ensure all sensitive information held is protected.	1.3
<i>Access Audit Process</i>	Provides the health organization with more details around the process on how to conduct User Access Audits - from both a privacy AND security perspective.	1
<i>User Access Audit Templates</i>	Provides the health organization with 3 audit Checklists to leverage for conducting required user audits associated with personal health information 'PHI' or clinical systems.	1.5
<i>How to Respond to A Breach</i>	To provide the health organization staff involved with protocols and a checklist to respond to breaches.	1.7

X

Ted Roque
Chief

Wahnapiatae First Nation

SECURITY-6: PRIVACY & SECURITY INCIDENT RESPONSE POLICY

ADOPTED BY BAND COUNCIL MOTION	BCM #WFN 18/19-014
DATE OF ADOPTED AT CHIEF AND COUNCIL MEETING	MAY 8, 2018
APPROVAL REVIEW AND REVISION DATES:	Every 3 years

1.0 POLICY

The health organization will ensure that privacy and security incident protocols are in place including an effective investigation process in order to respond quickly to any privacy and security incidents or breaches that are identified and subsequent communication protocols. Authorized key individuals such as the privacy and security contact/s, IT personnel and senior health organization management will be assigned clearly defined roles and responsibilities for the management of incidents and breaches.

1.1 Privacy and Security Incident Response protocols

Having a strong set of protocols and procedures in place for how to respond to incidents and breaches will demonstrate that the health organization has a robust privacy and security culture in place that:

- i. Limits potential damages resulting from a breach or incident;
- ii. Makes it easier to address any breach or incident and;
- iii. Prepares health organization management to work with the Information and Privacy Commissioner if required.

1.2 Responding to incidents/breaches

This policy covers addressing both an **incident** involving either a privacy and/or security event that has the potential to become a breach or is an actual breach. Examples include:

- An **Information Privacy Incident** is an illegal collection, use, disclosure, storage, or disposal of an individual's personal health information.
- An **Information Security Incident** is an unwanted or unplanned event that threatens the confidentiality, integrity, and/or availability of sensitive information like personal health information 'PHI'.

1.3 Defining a Breach

This policy covers when an actual breach occurs where PHI is stolen, lost, subject to unauthorized use or disclosure such as unauthorized copying, modification or disposal, or as a result of a privacy or security failure. Examples include.:

- i. Theft, loss, damage, unapproved destruction or changes to PHI;
- ii. Accidental or improper disclosure of confidential PHI in paper and/or electronic format;
- iii. Improper disclosure of summary information that identifies a particular community and/or a

- particular subset of the community;
- iv. Improper use of information assets or unauthorized access to information assets by an employee, contractor, student or volunteer;
 - v. Loss or theft of any information technology device such as desktops, laptops, BlackBerry, cell phones, CD/DVD, or any other electronic media that hold (or are capable of holding) PHI or other confidential/sensitive information;
 - vi. Criminal activity, such as piracy, copyright abuse, system or application hacking, virus attacks; and
 - vii. Failing to follow your health organization's security and privacy policies, procedures and standards, such as disclosing PHI on social network sites.

1.4 Reporting and Communicating a Breach

After confirmation of a privacy breach, the health organization will fully document the details of the breach and communicate with the required individuals:

- Reporting Person's Information
- Background/Details
- Healing Actions Planned / Taken to Prevent / Minimize Future Occurrences

1.5 Privacy Commissioner Reporting Guidelines

After confirmation of a privacy breach, consider the following factors in order to determine if the Privacy Commissioner should be notified:

- i. The person committing the breach knew or ought to have known that their actions are not permitted (e.g. looking at an ex-spouse's medical history for no work-related purpose, looking to see why a local celebrity or co-worker was receiving treatment);
- ii. The personal information recorded on paper, laptop, or other electronic device was stolen, including information that was subject to a ransomware or other malware attack or information seized through use of a portable storage device;
- iii. Following an initial privacy breach, the information was or will be further used or disclosed without authority (e.g. a person receives an incorrect fax, and although they return the fax, they keep a copy and threaten to make the information public or wrongly accessed patient information is subsequently used to mark products or services or to commit fraud such as health care or insurance fraud);
- iv. The personal information involved is sensitive;
- v. There is a risk of identity theft or other harm including pain and suffering or loss of reputation;
- vi. A large number of people or a significant volume of information are affected by the privacy breach;
- vii. More than one person was responsible for committing the breach;
- viii. The information has not been fully recovered;
- ix. The privacy breach is the result of a systemic problem or a similar privacy breach has occurred before;
- x. When disciplinary action is taken against a college member (e.g. when an employee who is a member of a college has been terminated, suspended or discipline as a result of a breach, or the individual resigns, and this action is related to a breach);

- xi. When disciplinary action is taken against a non-college member (e.g. a clerk is suspended because they posted patient information on social media after an unpleasant encounter with a patient);
- xii. Your organization or public body requires assistance in responding to the privacy breach; or
- xiii. You want to ensure that the steps taken comply with the organization's or public body's obligations under privacy laws.

1.6 Privacy Breach Risk Factors

To determine what other steps are immediately necessary, the health organization will assess the risks associated with the privacy breach. The risk factors that would need to be part of the risk assessment include:

- Personal Information Involved
- Cause and Extent of the Privacy Breach
- Individuals Affected by the Privacy Breach
- Foreseeable Harm from the Privacy Breach
- Recovery of Personal Information

2.0 ADDITIONAL REFERENCES

All policies are interrelated and have some similar content - it is highly recommended that you review and become familiar with these other policies which will provide a richer context to the Security-6 Privacy & Security Incident Response Policy:

Security-5 User Access and Activity Audit Policy

3.0 POLICY - ACTION ITEMS

Action Items referencing the set of tools (forms, templates, checklists) available in the excel document 'Privacy & Security Implementation Workbook' ('Workbook') that are used to implement the policy if the health organization decides to implement the policy as written. These tools can also be leveraged if the health organization already has protocols and tools in place that may need augmentation.

The action items/tools listed may also be referenced in other policy/s action item lists as all privacy and security policies have interrelated content.

These action items will be recorded in the health organization's 'Action Plan' also housed in the 'Workbook'.

Privacy & Security Implementation Workbook		
Action Item TAB-Tool	Purpose	Policy content section it supports
<i>How to Respond to A Breach</i>	To provide the health organization staff involved with protocols and a checklist to respond to breaches.	1.1

Privacy & Security Implementation Workbook		
Action Item TAB-Tool	Purpose	Policy content section it supports
<i>Assessing Breach Risk Factors</i>	To provide the health organization staff with a checklist to assess any risks that need to be mitigated following an incident or breach.	1.5
<i>Incident Reporting Template</i>	To provide health organization with a template to record any privacy incidents either revealed by the proactive Privacy Access Audit process and or any privacy and security incident identified that needs to be documented.	1.4
<i>Incident LETTER Template</i>	To provide the health organization with a framework communication letter to send to the person whose privacy & security has been compromised.	1.4

X

Ted Roque
Chief

Wahnapiatae First Nation

SECURITY-7: ORGANIZED OFFICE

ADOPTED BY BAND COUNCIL MOTION	BCM #WFN 18/19-014
DATE OF ADOPTION AT CHIEF AND COUNCIL MEETING	MAY 8, 2018
APPROVAL REVIEW AND REVISION DATES:	Every 3 years

1.0 POLICY

The health organization requires that employees, contractors, students and volunteers working on behalf of the health organization ensure that all sensitive and confidential information including personal health information 'PHI', whether it be on paper, on a storage device or a hardware device is safeguarded by practicing organized office protocols. Paper and electronic devices containing PHI must be properly locked away or disposed of when not in use to reduce the risk of unauthorized access, loss of, and damage to sensitive information during and outside of normal business hours or when workstations are left unattended. This includes computers/laptops, cameras, USBs, mobile phones) etc.

- 1.1 Office configuration should be considered by the privacy and security contact or designate to make it easier for staff to protect themselves and the health organization's clients. For example, where people are sitting and where they need to go to perform their job duties; how their equipment is setup to avoid unauthorized people from viewing paper and screens that may contain sensitive information.
- 1.2 Staff, especially those individuals who do not have a private space, need to be reminded that sounds may carry, and that if any conversations involve personal health information about a client, they should move to an area that is more sound proof and keep the volume of conversation low.
- 1.3 When leaving their office workstation for a period of time and/or at the end of the business day, staff must ensure the area is cleared of all client information, and personal or sensitive information of any kind. Paper records containing personal sensitive information must be stored in a locked cabinet or location and not left lying around. Keys for accessing drawers or filing cabinets should not be left unattended at a desk. If staff have their own office, the door should be locked when the staff member leaves; even if it's only for a coffee or lunch break.
- 1.4 All mobile devices (i.e. cell phones, cameras, laptops, USB devices, CDs and DVDs) must be locked up when the work station or office is unoccupied for a length of time, and completely shut down and/or locked up at the end of the work day. For example, if staff are using laptops they should be locked up in a drawer at the end of the day and not left out in the open.
- 1.5 All waste paper which contains sensitive or confidential information must be placed in the designated confidential waste bins. Under no circumstances should this information be placed in regular waste paper bins. Ideally a cross-cut shredder should be made available to staff so that there is no possibility that the resulting waste could be put back together.
- 1.6 Printers/scanners, and fax machines should be treated with the same care under this policy. Any print jobs containing sensitive and confidential paperwork should be retrieved immediately. When possible,



the "Locked Print" functionality should be used so when a document is sent to the printer, the individual needs to physically go to the printer and enter a code to release the document for print. This ensures no unauthorized staff inadvertently or purposefully read sensitive information before retrieval by the authorized individual.

2.0 ADDITIONAL REFERENCES

All policies are interrelated and have some similar content - it is highly recommended that you review and become familiar with these other policies which will provide a richer context to the Security-7 Organized Office Policy:

Privacy-20 Confidential & Acceptable User Policy

Security-1 Information Security Policy

Security-2 Mobile Devices Policy

Security-3 Information Technology Asset Management Policy

3.0 POLICY - ACTION ITEMS

Action Items referencing the set of tools (forms, templates, checklists) available in the excel document 'Privacy & Security Implementation Workbook' ('Workbook') that are used to implement the policy if the health organization decides to implement the policy as written. These tools can also be leveraged if the health organization already has protocols and tools in place that may need augmentation.

The action items/tools listed may also be referenced in other policy/s action item lists as all privacy and security policies have interrelated content.

These action items will be recorded in the health organization's 'Action Plan' also housed in the 'Workbook'.

Privacy & Security Implementation Workbook		
Action Item TAB-Tool	Purpose	Policy content section it supports
<i>How to Respond to A Breach</i>	To provide the health organization staff involved with protocols and a checklist to respond to breaches.	1.1

X

Fred Roque
Chief

Wahnapiitae First Nation

SECURITY-8: AUDIO/VIDEO SURVEILLANCE

ADOTPED BY BAND COUNCIL MOTION	BCM #WFN 18/19-014
DATE OF ADOPTION AT CHIEF AND COUNCIL MEETING	MAY 8, 2018
APPROVAL REVIEW AND REVISION DATES:	Every 3 years

1.0 POLICY

The health organization will ensure that before any audio and/or video surveillance equipment is installed, the rationale and purpose for the surveillance is fully considered, documented and approved by the health organization's privacy/security contact and senior management. This includes carefully weighing the loss of privacy when considering the potential use of video surveillance and the liabilities for the organization around protection, use, disclosure, retention and access. All relevant Canadian/provincial and territorial laws will apply.

- 1.1 Video surveillance will be considered as a last resort after exhausting other less privacy-invasive alternatives to meet the documented need because it puts the health organization at risk for violating privacy and security laws. Safeguards and procedures will be put in place if the health organization chooses to use surveillance equipment for a defined and documented need.
- 1.2 The organization will put periphery applications and management tools in place for both the equipment itself and the footage captured as well as how it is maintained, stored and retrieved including the following considerations:
 - i. Surveillance is susceptible to misuse by those who can access the system and use the video in unauthorized ways so only authorized staff will be given access.
 - ii. Extracts of the recorded footage will be provided to individuals who request a copy of their personal information (with their image), and software must be used to blur faces of third party individuals whose image appears in the footage to protect them from exposure if the footage is released.
 - iii. Audio and/or video surveillance equipment must be placed and calibrated so that it only collects the personal information that is necessary to achieve the intended purpose that has been documented and approved.
 - iv. Use of the equipment must be approved by senior management before it is installed.
 - v. The audio/video equipment must be positioned so that the general public cannot see any display of what is being captured and wherever possible, viewing by staff is kept to a minimum to those that are authorized by the privacy contact or their designate.
 - vi. Once audio and/or video equipment is installed, a clear and understandable warning poster must be visible for individuals to read prior to entering into the space being monitored by the equipment.
- 1.3 Storage, Retention and Destruction - The data and information stored on the audio and /or video surveillance equipment must be encrypted. Access to this information must be restricted to those individuals that maintain security of the building, room or item that is under surveillance. Retention,



archival and destruction of the data and information must follow health organization policies.

- 1.4 Training – authorized staff that setup and maintain the audio and/or video surveillance equipment must receive appropriate training to ensure they understand how to configure it properly to avoid any privacy and security risks.

2.0 ADDITIONAL REFERENCES

All policies are interrelated and have some similar content - it is highly recommended that you review and become familiar with these other policies which will provide a richer context to the Security-8 Audio/Video Surveillance Policy:

Privacy-7 Retention of Personal Health Information 'PHI' Records Policy

Privacy-8 Archiving & Accessing Personal Health Information 'PHI' Records Policy

Privacy-9 Destruction of Personal Health Information 'PHI' Records Policy

Security-1 Information Security Policy

Refer to the following online guides for further information:

- [Guide to using overt video surveillance](#) published by the Office of the Privacy Commissioner for BC.
- [Guidelines for Overt Video Surveillance in the Private Sector](#) published by the Office of the Privacy Commissioner of Canada.
- [Video Surveillance and Privacy Compliance in a Medical Clinic](#) published by the Information and Privacy Commissioner for B.C.

3.0 POLICY - ACTION ITEMS

Action Items referencing the set of tools (forms, templates, checklists) available in the excel document 'Privacy & Security Implementation Workbook' ('Workbook') that are used to implement the policy if the health organization decides to implement the policy as written. These tools can also be leveraged if the health organization already has protocols and tools in place that may need augmentation.

The action items/tools listed may also be referenced in other policy/s action item lists as all privacy and security policies have interrelated content.

These action items will be recorded in the health organization's 'Action Plan' also housed in the 'Workbook'.

Privacy & Security Implementation Workbook		
Action Item TAB-Tool	Purpose	Policy content section it supports
'Poster Templates' for an 'Audio & Video User' sample poster	Provides the health organization with poster templates designs	1.2 vi.



X

Ted Roque
Chief

Wahnapitae First Nation

SECURITY-9: CLOUD-BASED DELIVERY OF SERVICES POLICY

ADOPTED BY BAND COUNCIL MOTION	BCM #WFN 18/19-014
DATE OF ADOPTION AT CHIEF AND COUNCIL MEETING	MAY 8, 2018
APPROVAL REVIEW AND REVISION DATES:	Every 3 years

1.0 POLICY

The health organization will ensure that safeguards are in place to support any cloud-based delivery of services that is being used as part of the organization's operations. Specifically, sensitive information including personal health information/data that is stored and accessed on a third-party server in any cloud-based application/service will be protected under the relevant Canadian/provincial and territorial laws.

- 1.1 If the health organization is using any cloud-based services for any aspects of health care delivery the privacy/security contact will need to determine the risks to privacy/security and implement safeguards.
- 1.2 The organization will need to mitigate any privacy and security risks if a network of remote servers hosted on the internet is being used to store, manage, and process data, rather than using a local server or personal computer for that purpose.

Cloud services used by organizations typically fall into the categories of a private cloud (example: Mustimuhw Client Health Portal), or a public cloud (Dropbox, Survey Monkey).

- 1.3 If sensitive information is involved and the cloud environment is managed by a third-party organization, then the security contact and privacy contact, or their delegates, are responsible for ensuring that the third-party organization has all required safeguards in place before sensitive data is collected and stored on the cloud-based service. For example:
 - The cloud-based service is provided through a private cloud and meets all relevant Canadian/provincial and territorial laws and meets all of the health organization's privacy and security policies.
 - The third-party servers are located on Canadian soil so that all privacy and security laws are relevant.
- 1.4 The privacy contact will confirm that the third-party sign organization has appropriate Confidentiality Agreements in place to ensure that responsibility to protect sensitive information is clearly understood and if not, ensure that appropriate agreements are in place.

2.0 ADDITIONAL REFERENCES

All policies are interrelated and have some similar content - it is highly recommended that you review and become familiar with these other policies which will provide a richer context to the Security-9 Cloud Based Delivery of Services Policy:



Based Delivery of Services Policy:

Security-1 Information Security

Privacy-1 Statement on Privacy Guidelines and Principles

Privacy-3 Privacy Contact Responsibilities

Privacy-4 Security Contact Responsibilities

Privacy-5 Privacy Policy for PHI


3.0 POLICY - ACTION ITEMS

Action Items referencing the set of tools (forms, templates, checklists) available in the excel document 'Privacy & Security Implementation Workbook' ('Workbook') that are used to implement the policy if the health organization decides to implement the policy as written. These tools can also be leveraged if the health organization already has protocols and tools in place that may need augmentation.

The action items/tools listed may also be referenced in other policy/s action item lists as all privacy and security policies have interrelated content.

These action items will be recorded in the health organization's 'Action Plan' also housed in the 'Workbook'.

Privacy & Security Implementation Workbook		
Action Item TAB-Tool	Purpose	Policy content section it supports
C&A Use Acknowledgement	Provides a template for Confidentiality & Acceptable Use Acknowledgement document.	1.4
ISA Guiding Principle	Provides guidelines and a minimum set of items that should be included in an Information Sharing Agreement 'ISA' in place with another organization.	1.4



Ted Roque
Chief