Yuułuʔiłʔatḥ Government

Data Governance Policies and Procedures

Approved by Executive on August 8, 2023

Yuutuʔitʔatḥ

Table of Contents

Introduction

These policies serve to address Data Governance and Management within the Yuułuʔiłʔatḥ Government. According to our right of knowledge and information sovereignty, it is imperative that the Yuułuʔiłʔatḥ Government establishes proper policy and procedure to ensure proper data integrity, management, and appropriate use.

The availability and proper management of Yuułuʔiłʔatḥ related data is essential for the Yuułuʔiłʔatḥ Government to properly accommodate and provide support for its Citizenry.

This document includes the six following policies and their related procedures.

1. Information Privacy Policy
2. Privacy Breach Awareness Policy
3. Privacy Breach Notification Policy
4. Privacy Breach Investigation Policy
5. Records and Information Management Policy
6. Information Systems and Technology Policy

In accordance with relevant laws, Yuułuʔiłʔatḥ values, and the general wellbeing of Yuułuʔiłʔatḥ community members, these policies seek to provide the Yuułuʔiłʔatḥ Government with a functioning Data management and Protection process to support our community.

Definitions

“Assets” Anything of value owned by the Yuułuʔiłʔatḥ Government.

“Budget” A plan or outline of expected money and spending over a specified period.

“Classification” Process of categorizing records in an organized way.

“Confidentiality” Data being protected from inappropriate, unauthorized, unlawful, or unintentional access, disclosure, loss, or theft.

“Contract” Legally binding agreement between two parties.

“Data” Information that is collected for reference or analysis, and includes stories, facts, measurements, values, qualities, or observations. Data is a type of structured information and can be qualitative or quantitative.

“Data Steward” The role that has legal and ethical accountability for the collection, retention, use, disclosure, disposition, management, and overall protection of data stored and governed by the Yuułuʔiłʔatḥ Government, including data that our Nation governs and is stored in another Party’s environment. A Data Steward does not “own” the data but instead is a “trusted agent and overseer” of the data. Taking care of this data is more than just protecting it – it requires being accountable for whatever actions are taken with the data. Those actions can include defining, creating, modifying, deleting, and securing data, as well as ensuring its confidentiality, overseeing its use, and other data/information management activities.

“Director of Operations” Person who is responsible for leading the day-to-day administration or management of the Yuułuʔiłʔatḥ Government and who reports directly to the Executive.

“Executive” Elected or appointed official representatives of Yuułuʔiłʔatḥ that includes the President, Executive members and any equivalent terminology used by the Yuułuʔiłʔatḥ Government.

“Executive Data Steward” The role responsible for overseeing all Data Stewards within the Yuułuʔiłʔatḥ Government. The Executive Data Steward is also responsible for the general oversight and management of data security in the Yuułuʔiłʔatḥ Government.

“Information” Knowledge received and any documented material regardless of source or format.

“Need to know basis” Access to otherwise confidential information if that information is needed to complete specific and relevant duties.

“Personal Information” Information about an identifiable individual recorded in any form. Includes:

- age, marital status, race, national or ethnic origin, religion
- medical, education or employment history,
- financial information,
- DNA,
- identifying numbers such as your social insurance number, or driver’s license,
- views or opinions about you as an employee.

“Privacy Breach” A Privacy Breach is the loss of, unauthorized access to, or disclosure of, personal information. Breaches can happen when personal information is stolen, lost or mistakenly shared.

“Privacy Breach Investigation” A Privacy Breach Investigation occurs when a privacy breach or issue is suspected or identified within any Yuułuʔiłʔatḥ Government information systems. The goal of a Privacy Breach Investigation is to identify and notify what and whoever’s information privacy was breached, and to identify what vulnerabilities in the Yuułuʔiłʔatḥ Government’s information privacy system permitted the Breach to occur.

“Privacy Issue” A privacy Issue is an identified problem or vulnerability within the Yuułuʔiłʔatḥ Government’s information security systems. Privacy issues occur when such gaps are identified, however a breach has yet to occur. Once a Privacy Issue is identified, a Privacy Breach Investigation shall occur.

“Record”

Information created, received, and maintained by the Yuułuʔiłʔatḥ Government for operational purposes or legal obligations. A record may be electronic, or hardcopy paper based.

“Recordkeeping”

How an organization creates, obtains, and manages records.

“Staff”

An employee, contractor, or volunteer of the Yuułuʔiłʔatḥ Government, including members of the Executive. This also includes directors, employees, contractors, and volunteers of legal entities owned by the Yuułuʔiłʔatḥ Government.

“Virtual Private Network” (VPN)

VPN is a way to use public telecommunication infrastructure, such as the internet, to provide remote offices or individual users with secure access to the Yuułuʔiłʔatḥ Government’s virtual network

1. Information Privacy Policy

Purpose

The purpose of this policy is to provide guidance on the implementation and maintenance of appropriate information privacy practices within Yuułuʔiłʔatḥ related to the collection, retention, use, disclosure, safeguarding, and disposition of personal information. This policy reflects the Yuułuʔiłʔatḥ government's commitment to implementing and maintaining information privacy best practices across the organization in accordance with our *Freedom of Information and Protection of Privacy Act*.

Scope

This policy applies to all Executive members, Officers and employees of the Yuułuʔiłʔatḥ Government and any contractors or volunteers performing services on behalf of the Yuułuʔiłʔatḥ Government. The direction provided in this policy applies to all personal information created and acquired by Yuułuʔiłʔatḥ regardless of format (i.e., both electronic and hardcopy paper records).

Background

This policy maintains the Yuułuʔiłʔatḥ Government's right to and use of knowledge sovereignty. It ensures the confidentiality, integrity, and availability of Yuułuʔiłʔatḥ Government and Citizen information. In accordance with Yuułuʔiłʔatḥ values, this policy seeks to balance the right of access with the right to personal privacy and pledges to balance those rights in a way that respects both the person requesting the information and the person the information is about.

Policy Statement

It is the Executive's policy to establish a process around ensuring the privacy of personal information provided to the Yuułuʔiłʔatḥ Government in compliance with the procedures outlined in our most current *Freedom of Information and Protection of Privacy Act.* This act controls the Yuułuʔiłʔatḥ Government's use, release, and protection of citizen's personal data and records, as well as the Government's data and records.

Any and all information collected, retained, and used by the Yuułuʔiłʔatḥ Government will be done so following a confirmation of consent by the relevant individuals and/or groups.

Incidents of privacy breaches will be attended to according to the Yuułuʔiłʔatḥ Government's *Privacy Breach Policies and Procedures.*

Roles and Responsibilities

The Executive is responsible for

- approving and complying with the policy for privacy and the management of personal information

The Director of Operations is responsible for

- establishing and implementing documented procedures for privacy and the management of personal information
- responding in writing to the requests for access to, and correction of personal information submitted by employees and community members within 30 days from the date of the receipt. This 30-day period may be extended, upon approval of the Executive and qualification under the terms outlined in section 2.8 of the Yuułuʔiłʔatḥ government's *Freedom of Information and Protection of Privacy Act*
- designating an employee as Privacy Officer to manage and oversee the Yuułuʔiłʔatḥ Government's compliance with privacy requirements and this policy. The Director of Operations must assume the role of Privacy Officer if one has not been designated.
- ensuring compliance with this policy

The Privacy Officer (or Director of Operations if one is not appointed) is responsible for

- developing and maintaining the Yuułuʔiłʔatḥ Government's privacy program and standards
- recommending policies and procedures that support the objectives of the Yuułuʔiłʔatḥ Government's privacy program
- ensuring that all Yuułuʔiłʔatḥ activities are conducted in compliance with the established privacy standards, policies and procedures and in accordance with the generally accepted privacy principles. For this, the employee will:
    - provide training and awareness on privacy protection
    - make sure that Yuułuʔiłʔatḥ Citizens, and any contractors or volunteers performing services on behalf of the Executive, are aware of their rights as they relate to privacy, including their right of access to, and the right to request the correction of, all the personal information which is kept about them by the Yuułuʔiłʔatḥ Government
    - act as an expert resource on privacy matters
    - conduct periodic reviews of Yuułuʔiłʔatḥ activities that involve the collection, retention, use, disclosure, safeguarding, and disposition of personal information
- investigate all complaints regarding the collection/creation, accuracy, use, sharing/disclosure, protection, retention and destruction of personal information and reporting the results to the appropriate supervisor and, where warranted, to the Executive
- recommend changes to policies, procedures and practices in response to the issues raised in the complaints

Employees, contractors and volunteers are responsible for

- complying with the established policy
- immediately reporting to the privacy officer any privacy breaches

Exceptions

The Director of Operations may refuse the disclosure of certain information if that information's disclosure would, or can be expected to, fall within the predetermined causes for information nondisclosure. These causes are outlined in detail in section 2.9 and 2.13 of the Yuułuʔiłʔatḥ government's *Freedom of Information and Protection of Privacy Act.*

Compliance

All Executive members, Officers, and employees of Yuułuʔiłʔatḥ and any contractors or volunteers performing services on behalf of the Executive must comply with this policy. Furthermore, all parties must not willfully commit any offences outlined in section 5.2 of the Yuułuʔiłʔatḥ government's *Freedom of Information and Protection of Privacy Act.* Any person who commits one or more of the listed offences may be subject to, on summary conviction, a fine of up to $10,000.

Information Privacy Administrative Procedures

The following procedures allow for the straightforward and clear implementation of the Information Privacy Policy. They are also in accordance with the Yuułuʔiłʔatḥ government's *Freedom of Information and Protection of Privacy Act.*

Accountability

The Director of Operations will designate an employee as privacy officer to ensure the principles outlined in these procedures are implemented. The Director of Operations must assume the interim position of privacy officer in the event that one has not been designated.

Identifying Purpose

The purposes for the collection, use, retention, disclosure, safeguarding, and disposition of personal information should be communicated to individuals at or before the time of collection. Depending upon the way in which the information is collected, this can be done orally or in writing. An application form, for example, may give notice of the purposes.

Persons collecting personal information must be able to explain to individuals the purposes for which the information is being collected, retained, used, disclosed, safeguarded, and disposed of.

Consent

With limited exceptions, the Yuułuʔiłʔatḥ Government must obtain consent, verbal or written, from an individual before collecting their personal information. Consent requires that the individual is advised of the purposes for which the information is being collected and how it will be used and disclosed.

Consent must be stated in such a manner that the individual can reasonably understand how the information will be used or disclosed. Consent must not be obtained through deception.

Personal information can be collected, used, or disclosed without the knowledge and consent of the individual in only limited circumstances, such as legal or security reasons which may make it impossible or impractical to seek consent.

Individuals can give consent in many ways. For example:

- use of the Authorization of Consent form
- consent may be given orally
- consent may be given through electronic means

An individual may withdraw consent at any time, subject to legal or contractual restrictions and reasonable notice.

Limiting Collection

The Yuułuʔiłʔatḥ Government cannot collect personal information unethically. Both the amount and the type of information collected must be reasonable, appropriate, and limited to that which is necessary to fulfill the purposes identified.

Limiting Use, Disclosure, and Retention

Personal information will only be used or disclosed for the purpose for which it was collected, specifically:

- consistent with the original collection of the personal information
- when consent of the individual is obtained
- for complying with a subpoena or warrant issued or order made by a court, person or body with jurisdiction to compel the production of information or for the purpose of complying with rules of court relating to the production of information

Personal information that has been used to make a decision about an individual must be retained long enough to allow the individual access to the information after the decision has been made. Yuułuʔiłʔatḥ will retain such information for a minimum of one year following receival.

Identifiable personal information must only be used and disclosed if required.

Personal information that is no longer required to fulfill the identified purposes will be destroyed, erased, or made anonymous in accordance with the Yuułuʔiłʔatḥ Government's retention and disposition schedule, as identified within the Yuułuʔiłʔatḥ Records and Information Management Policy and Procedures.

Accuracy

The Yuułuʔiłʔatḥ Government will take all reasonable steps to make sure that personal information that is used to make a decision about an individual is as accurate, up-to-date and complete as possible to minimize the possibility that inappropriate information may be used to make a decision about the individual.

Safeguards

Personal information should be protected with appropriate safeguards to make sure only those with a need to know will have access to the records:

- for electronic records containing personal information, the records should be protected with controls on the document itself (such as password protection) and other administrative controls, such as restricting access to the electronic storage location in which the record is stored
- for hardcopy paper-based records, containing personal information, the records should be always stored in secure filing cabinets unless being used, and transported in a secure manner if required to be taken offsite

Yuułuʔiłʔatḥ must make its employees, contractors, and volunteers aware of the importance of maintaining the confidentiality of personal information.

Care must be used in the disposal or destruction of personal information, to prevent unauthorized parties from gaining access to the information.

Openness

The Yuułuʔiłʔatḥ Government must be open about its policies and practices with respect to the management of personal information. Individuals will be able to easily acquire information about its policies and practices. This information must be made available in a form that is generally understandable.

The information made available should include:

- the name or title, and the address, of the privacy officer, who is accountable for the Yuułuʔiłʔatḥ Government's policies and practices, and to whom complaints or inquiries can be forwarded
- the means of gaining access to personal information held by the Yuułuʔiłʔatḥ Government
- a description of the type of personal information held by the Yuułuʔiłʔatḥ Government

Individual Access

Within reasonable limitations, an individual may request to be informed if the Yuułuʔiłʔatḥ Government holds personal information about the individual an account of the third parties to which it has been disclosed.

The identity of an individual will be authenticated before discussing their personal information with them.

Within reasonable limitations, when requested, the Yuułuʔiłʔatḥ Government must provide an individual with access to their personal information within a reasonable time and at minimal or no cost to the individual. The requested information will be provided or made available in a form that is generally understandable. Yuułuʔiłʔatḥ Citizens and other relevant individuals should have access to personal information about themselves and their communities regardless of where that information is physically held.

In certain situations, the Yuułuʔiłʔatḥ Government may not be able to provide access to all the personal information it holds about an individual. Exceptions to the access requirement will be limited and specific. The reasons for denying access will be provided to the individual upon request. A detailed list of exceptions is located within section 2.9 of the Yuułuʔiłʔatḥ government's *Freedom of Information and Protection of Privacy Act.*

Exceptions may include information that:

- contains references to other individuals
- cannot be disclosed for legal, security, or commercial proprietary reasons
- is subject to solicitor-client or litigation privilege

Individuals who are given access to their personal information may:

- request correction of the personal information where the individual believes there is an error or omission therein
- require that a notation be attached to the information reflecting any correction requested but not made
- require that any person or body to whom that information has been disclosed for use for a decision-making process, within a reasonable time that a correction or notation is requested, be notified of the correction or notation

Challenging Compliance

The Yuułuʔiłʔatḥ Government will make sure that a process exists to receive and respond to complaints or inquiries about its policies and practices relating to the handling of personal information. The complaint procedures will be easily accessible and simple to use.

If a complaint is found to be justified, the Yuułuʔiłʔatḥ Government will take appropriate measures, including, if necessary, amending its policies and practices.

References and Related Authorities

Yuułuʔiłʔatḥ Government's *Freedom of Information and Protection of Privacy Act*

2. Privacy Breach Awareness Policy

Purpose

The purpose of a Privacy Breach Awareness policy is to ensure that the Yuułuʔiłʔatḥ Government has a privacy culture that demonstrates our commitment and knowledge on wise practices for protecting data, auditing these practices, and following up on any reported concerns which may or may not prove to be a privacy breach. This policy focuses on raising awareness and demonstrates our commitment to improving our privacy culture and following up on issues.

Policy Statement

Yuułuʔiłʔatḥ Citizens, Government staff, and other volunteers or contract workers must be informed on how to report a potential privacy breach. This will be done using the following methods:

- A Privacy Breach Notification poster must be posted within the locations where Yuułuʔiłʔatḥ Citizens, Government staff, and other volunteers or contract workers reside or function (e.g., reception areas, lunchrooms, staff offices or hallways, etc.)
- The Privacy Breach Notification Poster should also be posted online on the Government website, and other through other appropriate methods of digital communication such as social media.
- Where an individual receives services outside of our facilities (e.g., nursing care in their hospital, employment fair, etc.) Yuułuʔiłʔatḥ staff must provide a pamphlet that supports the same outcome as the Privacy Breach Notification poster.
- Where an individual receives recurring services outside of our facilities (e.g., nursing care in their home the pamphlet is to be left with the individual/guardian)
- Individuals have the option of reading the poster or pamphlet; and may retain a copy if desired
- When data is collected/used over the phone an equivalent telephone script must be spoken to replace the poster/pamphlet
- The poster, pamphlet, or telephone script may be integrated with other privacy related posters, pamphlets, or telephone scripts
- The poster, pamphlet and telephone script must:
    I. Provide information on how to report a potential privacy breach to the Yuułuʔiłʔatḥ Government or the B.C. Office of the Information and Privacy Commissioner
    II. Inform the individual/guardian that reporting will not cause any harm to themselves
    III. Provide the contact details of the applicable Privacy Officer (i.e., Data Steward) or Executive Data Steward

Roles and Responsibilities

The Director of Operations is responsible for:

- Approving various privacy breach awareness communication methods

Data Stewards

- Draft posters, pamphlets, and telephone scripts, and other methods of communication and obtain Governance approval; post and maintain the quality and content of the various methods of communication.

Department Managers

- Implement the use of the pamphlets and telephone scripts and other methods of communication.

Related Procedures

1. The Data Steward drafts the poster, pamphlet, or telephone script and reviews with the Director of Operations.
2. The Data Steward presents the poster, pamphlet, or telephone script to the Governance Board.
3. The Governance Board reviews and approves. If approval cannot be met the board must provide guidance. The Data Steward then updates accordingly and resubmits until approval is met.
4. Once approved the Data Steward posts the posters and distributes the pamphlet and telephone scripts to the Director of Operations
5. Department Managers are responsible for implementing the use of the pamphlet and telephone scripts.
6. Annually the Data Steward reviews the poster; updates if required and seeks re-approval; and upon approval reposts accordingly. If no updates are required, the Data Steward reprints/reposts if the condition of the poster that is currently posted requires a fresh copy to be posted

3. Privacy Breach Notification Policy

Purpose

The purpose of this policy is to provide a framework for a person/group to submit a privacy issue. An individual (e.g. Yuułuʔiłʔatḥ Citizen, staff, member of the public, member of a Yuułuʔiłʔatḥ Government legal entity, privacy commissioner, etc.) or a group representing or advocating on behalf of an individual may have a privacy issue (e.g. risk, concern, complaint, incident(s) of actual or suspected unauthorized access, misuse of personal information, inappropriate disclosure, etc.) that needs to be reported and followed up. The item may be perceived or actual; it may pertain to himself or herself or another Party; and it may involve our Nation or another organization. It is important that the Yuułuʔiłʔatḥ Government supports the reporting of privacy issues.

Policy Statement

Every privacy issue, hereafter referred to as a 'Privacy Breach Notification' are to be reported to one of the Data Stewards. The Data Steward is responsible for recording the issue on the Privacy Breach Notification report within seven (7) business days. Once logged the Data Steward immediately notifies the Executive Data Steward and the two parties initiate the Privacy Breach Investigation.

All Privacy Breach Notifications must be numbered sequentially, labelled with the date received, and recorded in the Privacy Breach Notification Log.

The Privacy Breach Notification Log must be stored electronically in a secure location that is only accessible to the approved support staff members.

If the Privacy Breach involves one or more of the Data Stewards, the Privacy Breach Notification Log cannot be updated. Instead, the receiver of the notification must retain the notification report in a secure location and report in writing to the Director of Operations. In this circumstance the Director of Operations takes the lead in conducting an investigation.

A Privacy Breach Notification may be an item reported by a person, an organization, or a result of conducting an audit. A privacy breach may also be linked to a privacy breach that is associated with an item reported to another Party. For example, if a person reports privacy breach to one of our associated partners who in turn contact us as part of their investigation. This contact must be recorded as a Privacy Breach Notification.

Staff are informed to report Privacy Breaches vis-à-vis the following:

- Staff Data Governance Awareness Training
- Privacy Breach Poster that is posted in the staff common areas

Yuułuʔiłʔatḥ Citizens and staff are informed to report Privacy Breaches vis-a-vis the Privacy Breach Notification poster, pamphlet, or telephone script, or the Request for Information form and response letter.

Roles and Responsibilities

Data Stewards:

- Receiving and maintaining the Privacy Breach Notification Log

Executive Data Stewards

- Initiating and overseeing the Privacy Breach Investigation

Director of Operations

- Receiving Privacy Breach Notifications where they involve the Data Stewards and initiating the investigation immediately

4. Privacy Breach Investigation Policy

Purpose

The purpose of this policy is to ensure that the Yuułuʔiłʔatḥ Government review and investigate all privacy breach notifications in an objective manner so that we may respond positively and supportively to the person/group who notified us of a potential privacy breach. Furthermore, the Yuułuʔiłʔatḥ Government must show evidence that each privacy breach notification has been investigated fairly and a conclusion has been determined. If the outcome of an investigation results in privacy being compromised, the Yuułuʔiłʔatḥ Government must have a plan to notify the parties affected and have an action plan that remediates the issue.

Policy Statement

Privacy Breach Investigations work to identify what sensitive information was disclosed and what individuals are affected by the information's illicit disclosure; furthermore, Privacy Breach Investigations identify how that privacy was breached and systemic vulnerabilities that may exist as well as who was responsible for the breach.

If a Privacy Breach Notification involves data managed/stored internally the notification document must be forwarded to the applicable Manager(s) unless it is speculated that the Manager(s) is involved in which case, it must be forwarded to the Director of Operations who is not likely involved.

If a Privacy Breach involves data that is managed/stored by another third-party the notification document must be forwarded to the other Party as per agreements that govern the data.

Each Privacy Breach Notification initiated by the Yuułuʔiłʔatḥ Government must have an investigation initiated within 2 business days. All investigation details will be recorded in the Privacy Breach Investigation Report. All evidence will be securely protected using industry wise practices.

Investigations involving data that is managed by our organization will be led by a Data Steward and managed by the Executive Data Steward; or if it is possible the Executive Data Steward is involved it must be led by the Director of Operations who is not likely involved or a hired 3rd party contractor. Additional support resources from the Office of the Information and Privacy Commissioner may be obtained.

Each investigation will remain confidential and deemed highly sensitive information. An investigation is considered a 'potential' breach until such time that the investigation is complete.

At a minimum each investigation must include:

- Immediate containment of the breach/violation
- Breach Awareness Notification(s)
- The process of contacting other departments or individuals within our organization or other organizations to assist in managing the breach

- Investigating and documenting the details, including the cause and extent
- Identifying impacts to other organizations
- Determining if a breach occurred and if so, making reprimanding recommendations; identifying risks and plans to mitigate the breach in the future; and communicating the results and action plans to the applicable leaders of our organization.

Any individuals affected must be notified. This type of notification is referred to as a 'Breach Awareness Notification' and is required as soon as possible after the breach, and no later than three (3) business days after the breach was reported (i.e., the full investigation is not required to be completed). The Breach Awareness Notification may be delayed in order to not impede a criminal investigation if deemed necessary after contract from law enforcement authorities. The Breach Awareness Notification must be documented to ensure the appropriate information is conveyed completely and accurately. It may be made in person, by phone, or in writing.

Investigations involving data that is managed/stored by another Party will be led by the given other Party in accordance with the agreement that governs the data.

The Executive Data Steward or Director of Operations is responsible for approving the final report that reflects Yuułuʔiłʔatḥ's position on the given Privacy Breach Notification and completing any of the necessary Investigation steps identified above.

All Yuułuʔiłʔatḥ Government staff are required to cooperate with anyone involved in the investigation and support the outcomes of an investigation.

During an investigation the Data Steward designated Investigation Lead will be responsible for determining the communication(s) that will occur during the investigation. This person will also be responsible to follow-up on the outcomes of the Breach Investigation.

Failure to comply with the privacy and security policies / procedures may lead to termination of access, termination of employment, termination of contract, withdrawal of privileges, and/or be subject to applicable laws and the applicable Acceptable Use and Confidentiality agreement. A privacy breach may also result in notifying the relevant professional organization a staff/contractor may be associated with which may result in professional sanctions invoked by the given professional organization in accordance with their policies/procedures.

Approval to dispose of any evidence is made on a case-by-case basis and at a minimum requires the approval of the Lead Investigator and Executive Data Steward. If a single person holds these roles the Lead Investigator and Director of Operations must approve instead. In the case where external organizations are also involved in the investigation it would also require approval by the given organizations.

Roles and Responsibilities

Director of Operations:

- Seeking outside investigatory expertise and authority if necessary

Executive Data Steward:

- Managing Privacy Breach Investigations
- Approving final investigation reports

Lead Investigator (Designated Data Steward):

- Leading privacy breach investigations
- engaging other Parties as required
- facilitator-informing individuals as described herein
- approving disposition of investigation notifications and reports according to this policy
- participating in investigations led by other Parties
- Following-up on the outcomes of the investigation

Data Stewards

- Supporting the Lead Investigator

Information Technology Professional

- Conducting risk assessments of implicated systems

Privacy Breach Investigation Related Procedures

When a Privacy Breach Notification is received the breach must be confirmed, contained, responded to and investigated. The following procedures support these activities while also assisting the Lead Investigator in determining if the breach is contained within the Yuułuʔiłʔatḥ Government, when and how to notify individuals and other Parties of the breach and when to collaborate with partner organizations that may be impacted by the breach.

1. **Receive Notification of Possible Breach**

Refer to Privacy and Security Policy ‘Privacy Breach Notification’.

2. **Confirm Breach**

When the Privacy Breach Notification is received the Lead Investigator department managers confirm the breach. This may include some high-level investigative actions to verify the accuracy of the breach details such as:

- Reviewing access logs (both to systems and facilities)
- Talking with staff members, Yuułuʔiłʔatḥ citizens, or other relevant personal
- Reviewing audit logs
- Reviewing documentation/media

This work needs to be done immediately and with precision, however it must also be done quickly.

3. **Contain Breach**

Once the breach has been confirmed, immediate action must be taken to contain the breach e.g.:

- Halting unauthorized practices
- Changing computer/facility access codes or keys
- Recovering records
- Ensuring no copies of data have been made or retained by the individual(s) involved in the privacy breach
- If the data/material has been securely destroyed rather than retrieved, obtaining confirmation in writing from the party responsible for the secure destruction of the data/material

4. **Conduct Preliminary Assessment**

Once the breach has been contained, preliminary assessment activities can occur to determine the extent of the breach, impacted individuals, potential risk factors and internal communication about the breach. Preliminary assessment activities are added to and expanded throughout the breach investigation.

a. **Designate a Breach Response Team:** Investigation Lead selects and designates a Breach Response Team and assigns a Lead:

- Appointing an individual to conduct the initial investigation and make recommendations for follow-up
- Determining if a Breach Response Team should be assembled with representatives from appropriate business areas (if the breach is determined to impact other organizations, the Breach Response Team consists of representatives from some/all Parties/Organizations)
- The Breach Response Team must include a minimum of three (3) people whereby no more than two (2) members are Data Governance Board Members

b. **Internal Notification:** Breach Response Team determines who, internally, should be aware of the incident. Internal notification should not include identifiable personal information about the person(s) under investigation or the individual(s) impacted by the breach.

c. **Report Criminal Activity:** If the breach involves theft or other criminal activity, the police must be contacted and will provide guidance for breach investigation and communication.

d. **Preserve Evidence:** When conducting preliminary analysis of risks and cause of breach, make sure the evidence is preserved appropriately. Do not destroy evidence that may be valuable in determining the cause of the breach or support you in taking corrective action.

e. **Analyze and Document Breach Information:** The Breach Response Team analyzes and investigates breach information.

Notifications and all other activities associated with the breach investigation must be documented.

Follow the guidelines below when conducting the preliminary investigation:

i. Consider what information has been breached, e.g.,

- Consider the sensitivity of the information (e.g., health information, financial account numbers, government issued identification etc.)
- Determine if the information can be used for fraudulent or harmful purposes

ii. Analyze the cause and extent of the breach e.g.,

- Cause of the breach
- Risk of ongoing or further exposure of the information
- Extent of unauthorized collection, use or disclose, including number of likely recipients and risk of further access, use or disclosure, including in mass media or online
- Determine if information was stolen and, if so, if it was the target of theft
- Is the information encrypted or protected
- Has the information been recovered
- Steps taken to minimize harm
- Is this a systemic problem or an isolated incident

iii. Determine individuals affected and potential harm from the breach e.g.,

- Who received the information (an accidental breach/mistake or intended breach)
- Is there a relationship between the unauthorized recipients and the data subject?
- Security risk
- Identify potential harm to the individuals that may result from the breach
- Identity theft/fraud
- Loss of business/employment
- Hurt, humiliation, damage to reputation or relationships

iv. Identify potential harm to the organization as a result of the breach e.g.,

- Loss of trust in public body or organization
- Loss of assets
- Financial exposure
- Loss of contracts/business

v. Identify potential harm to the public as a result of the breach e.g.,

- Risk to public health
- Risk to public safety

5. Breach Contained Within Yuułuʔiłʔatḥ?

It is imperative to determine if the breach is contained internally within the Yuułuʔiłʔatḥ Government or if it impacts other Nations/Parties/customers. The impact on others may result from the person(s) under investigation being employed by/affiliated with another Nation or organization or from the breach occurring through the use of a computer-based system used by us and our Partners.

a. Is the unauthorized recipient(s) of information employed by the Yuułuʔiłʔatḥ Government?

b. Is the unauthorized recipient of information on contract with the Yuułuʔiłʔatḥ Government and/or work for any other organizations? (If yes, breach is not contained within Yuułuʔiłʔatḥ)

c. Are any other organizations impacted by the breach? (If yes, breach is not contained within Yuułuʔiłʔatḥ)

Note that if a breach is not contained within Yuułuʔiłʔatḥ, affected Parties and/or the Office of the Information and Privacy Officer must be contacted for support. All further activities regarding the breach will be done in conjunction with and with support from these other Parties.

6. Conduct Risk Assessment

The Information Technology professional must conduct a new risk assessment for the implicated system.

If a risk assessment has previously been done for the system, the Information Technology professional must conduct a new assessment and update their findings.

Procedure for conducting a risk assessment can be found in the administrative procedures of the Yuułuʔiłʔatḥ Government *Information Technology and Systems Policy*

7. Partner Organization Impacted?

Determine if the breach directly impacts Partner Organizations (e.g., Regional Health Authority (RHA), Ministry of Health, Ministry of Children and Families, etc.), and/or if the breach involves a computer-based system that is shared between our Nation and our Partners.

8. Contact Partner Organization Privacy Officer for Breach Support

If the breach affects a Partner Organization, contact the Partner Organization(s) for Breach Management support to collaborate on and align response activities for the breach and/or follow the arrangements set out in the support or data governance and information sharing agreements.

9. OIPC Reportable?

For internally managed/stored data determine if the breach should be reported to the B.C. Office of Information Privacy Commissioner. Refer to the Checklist for Notifying the Office of the Information and Privacy Commissioner (OIPC) below:

CHECKLIST FOR NOTIFYING THE OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER (OIPC)	
Consider the following factors when determining if the Office of the Information and Privacy Commissioner should be notified of the breach.	
□	The breach involves Personal Information and it is sensitive
□	There is a risk of identity theft or other harm including pain and suffering or loss of reputation
□	A large number of people are affected by the breach
□	The information has not been fully recovered
□	The breach is the result of a systemic problem or a similar breach has occurred before
□	Our Nation requires assistance in responding to the privacy breach
□	Our Nation wants to ensure that the steps taken comply with our Nations obligations under privacy legislation
If any of the boxes in the checklist are checked, you should report this breach to the OIPC	

To report this breach to the OIPC, fax a copy of the following documents to the OIPC (250-387-1696):

i. Checklist for Notifying the Office of the OIPC

ii. FNHSO Breach Reporting Form,

iii. Breach Notification Letter(s) sent to impacted individual(s)

iv. Any additional information you determine the OIPC should be aware of.

If notification to the OIPC is required and the breach involves an eHealth system, you must also provide a copy of the report to eHealth Operations Privacy Services and Health Information Privacy, Security and Legislation (HIPSL). In addition, HIPSL has the responsibility to notify the Office of the Chief Information Officer (OCIO) of all OIPC reportable events.

10. Notify Impacted Individuals/ Communities?

Assess the need to notify individuals/communities impacted by breach. If the breach impacts partner organizations, notification assessments and messaging shall be jointly undertaken by all impacted organizations.

a. Will notification avoid or mitigate harm to an individual whose personal information has been inappropriately collected, used or disclosed?

b. Do legislation or contractual obligations require notification

c. Is there a risk of identity theft, fraud, physical harm, hurt, humiliation, damage to reputation, loss of business or employment?

d. Has law enforcement been contacted and have they requested delayed notification in order not to impede a criminal investigation?

11. Send Notification to Impacted Individuals/Communities

If notification is required, it should occur as soon as possible following the breach.

- Direct notification (via phone, letter or in person) is preferred.
- Indirect notification (via websites, posted notices and media) should only occur where direct notification could cause further harm, if cost prohibitive or contact information is lacking.

Notification should include the following**:**

- Date of breach
- Description of breach
- Description of information inappropriately collected, used or disclosed
- Steps taken so far to reduce or control harm
- Future steps planned to prevent further privacy breaches

- Steps the individual can take (e.g. how to change PHN, DL number etc.)
- Privacy Commissioner contact information (for concerns, complaints)
- Contact information for the Yuułuʔiłʔatḥ Government Privacy Officer (i.e. Executive Data Steward)

Determine if other organizations should be contacted (note that personal information should not be shared with these entities unless required)

- Professional or regulatory bodies
- Technology suppliers (if breach was due to a technical failure or could be mitigated through technical fixes

12. Coordinate Disciplinary Action

Determine if disciplinary action is required regarding the person(s) under investigation for the breach

- Deprovision user(s) from internal and/or eHealth systems (the Data Steward is responsible for initiating de-provisioning of users from all internal and eHealth systems)
- Suspension/Termination of employment/contract
- Removal of facility access

13. Develop and Implement Remediation/Prevention Strategy

Determine actions to remediate impacts from breach and develop strategies to prevent future privacy breaches

- Review investigative findings and develop prevention strategies
- Monitor prevention strategies

5. Records and Information Management Policy

Purpose

The purpose of this policy is to establish the authority and responsibilities necessary to effectively define and implement a Records and Information Management (RIM) program for the Yuułuʔiłʔatḥ Government. Furthermore, this policy provides guidance on effective recordkeeping practices to create, manage and protect the integrity any and all Yuułuʔiłʔatḥ records that support its decision-making, reporting, performance and accountability requirements.

This policy reflects the Yuułuʔiłʔatḥ Government's commitment to implementing and maintaining records management best practices across the organization in conformance with our *Freedom of Information and Protection of Privacy Act*.

Scope

This policy applies to all Executive members, officers and employees of the Yuułuʔiłʔatḥ Government and any contractors or volunteers performing services on behalf of the Executive. The direction provided in this policy applies to all records created and acquired by the Yuułuʔiłʔatḥ Government regardless of format (i.e., both electronic and paper records).

Background

The Yuułuʔiłʔatḥ Government recognizes the importance of good information and the proper organization of that information to assist with decision making, strategic planning, and to be open and accountable to the members of the Yuułuʔiłʔatḥ Government. Properly storing, organizing, and understanding our Government's data is an important tool for remembering our history, charting our path for the future, preserve Yuułuʔiłʔatḥ data sovereignty and serving the Yuułuʔiłʔatḥ people.

Policy Statement

This policy establishes the authority for records management practices and standards within the Yuułuʔiłʔatḥ Government. It is the Yuułuʔiłʔatḥ Government's policy to establish a process around the creation, collection, organization, retention, and safeguarding of records for long-term availability, understandability, and usability. This policy establishes the Director of Operations to assume responsibility for implementing and overseeing the Records and Information policy and program.

Roles and Responsibilities

The Executive is responsible for

- approving the policy for records and information management

The Director of Operations is responsible for

- Designating and employee to implement and oversee the records management program

The designated employee is responsible for

- establishing and implementing documented procedures for records and information management
- implementing appropriate recordkeeping practices
- making sure appropriate safeguards of Yuułuʔiłʔatḥ records
- ensuring compliance with the established records retention and disposition schedule and overseeing the disposition process
- ensuring that employees and any contractors or volunteers performing services on behalf of the Executive are fully knowledgeable of their responsibilities as they relate to recordkeeping practices

Department managers are responsible for

- Following up on any reported compliance breaches, this may include administering disciplinary action if deemed necessary

Employees, contractors and volunteers are responsible for

- complying with the established policy
- immediately reporting to their department manager any potential breach related to with the recordkeeping policy

Records and Information Management Administrative Procedures

Accountability

Each record will have a designated employee that makes sure the recordkeeping framework outlined in this policy is applied to the record. All employees, contractors, or volunteers that are in custody of a record must make sure it is managed in accordance with this policy.

Permanent records such as policies and procedures will be reviewed and updated by the assigned employee on a regular basis, in accordance with these respective required polices and approvals.

Records under the safekeeping of a departing employee, contractor or volunteer must be formally transferred to another employee of a similar designated role through a knowledge transfer process. This process should include information on the types of records to be transferred, how the records are organized, in which location the records are kept, and required safeguards.

Creation and Collection

Key activities and decision-making processes of the Yuułuʔiłʔatḥ Government should be identified, including the records required to support those processes, to ensure accountability, preserve an audit trail, and protect the Yuułuʔiłʔatḥ Government from liability.

All information at the time of creation or collection should be assessed to determine if it supports the Executive’s business purposes and/or legal obligations and enables decision-making. If determined to be a record, the management of the record should comply with the procedures outlined within this policy.

The record will contain information necessary to achieve the objectives for which each record is created and will be limited to only what is necessary to achieve those objectives.

Whenever possible, the record will contain information about one single function or activity to facilitate information classification, organization, retention and retrieval.

Yuułuʔiłʔatḥ records will be legible, written in plain language and adapted to their specific audience.

Only one copy of each record should be created or collected either physically or digitally. When creating or collecting a record, individuals should first check to see if the record is already in existence. In instances of multiple copies of the same record, copies should be securely disposed of in accordance with the requirements of this policy.

Organization and Classification

A classification plan structure will be implemented based on the Yuułuʔiłʔatḥ Government’s functions and activities, with records stored in accordance with the activity and/or function that it supports.

Records should be subject to a consistent naming convention, with the name of the record including at minimum the date, title and version.

The title of the document should be short.

An official storage location will be identified and designated for each record. The number of storage locations should be limited and be consistent to support the format and type of record.

Records should be made accessible, shared and re-used to the greatest extent possible, subject to technological, legal policy and security restrictions.

Maintenance, Protection and Preservation

Records will be protected and stored in the appropriate storage location in a way that preserves their long-term availability, understandability and usability.

Backups will be taken of all electronic records on a regular basis and stored in a physical or digital location separate from the location of the original records.

Any records that are only in hardcopy paper-based format should be assessed to determine if they need to be scanned or if other physical security measures need to be taken (e.g., use of fire/waterproof cabinets) to protect their long-term availability.

Confidential records should be protected with appropriate safeguards to make sure only those with a need to know will have access to the records:

- for electronic records, confidential records should be protected with controls on the document itself (such as password protection) and other administrative controls, such as restricting access to the electronic storage location in which the record is stored.
- for hardcopy paper-based records, confidential records will be always stored in secure filing cabinets, and labelled as CONFIDENTIAL unless being used, and transported in a secure manner if required to be offsite

Retention and Disposition

The records will be retained for the period specified in the records and information retention and disposition schedule, as outlined in the attachments. They will be disposed of in a manner that prevents their reconstruction (for paper-based records) or recovery (for electronic records).

Attachments

1. Document Retention Periods (see below)

1. Document Retention Periods

Record or information	Duration
General Yuułuʔiłʔatḥ governance records	
Yuułuʔiłʔatḥ laws, bylaws, legislative amendments, regulations, codes, directives, constitution, and membership resolutions	Permanent
Appointments and terms of appointments	Permanent
Agreements, funding arrangements, Executive commitments	Permanent
Executive meeting minutes, Executive committee meeting minutes, annual reports, debenture records, membership records, public notices, records of incorporation, corporate seal	Permanent
Legal files and papers	
Customer and supplier contracts and correspondence related to the terms of the contracts	7 years beyond life of contract
Contractual or other agreements (e.g., contribution, impact benefit, trust) between the Yuułuʔiłʔatḥ Government and others and correspondence related to the terms of the contracts	7 years beyond life of the contract
Papers relating to major litigation including those documents relating to internal financial misconduct	5 years after expiration of the legal appeal period or as specified by legal counsel

Papers relating to minor litigation including those documents relating to internal financial misconduct	2 years after the expiration of the legal appeal period
Insurance policies including product or service liability, Executive and Officers liability, general liability, and third-party liability, property and crime coverage	7 years after the policy has been superseded
Documents related to the purchase, sale or lease of property	Permanent
Documents related to equity investments or joint ventures	Permanent
Human Resources	
Personnel manuals and procedures	Permanent
Organization charts	Permanent
Where there is a pension plan (excluding RRSP plans): • original plan documents • records of pensionable employee service and eligibility • associated personal information including name, address, social insurance number, pay history, pension rate	7 years after the death of the employee or employee's spouse in the case of spousal eligibility
Letters of offer and individual contracts of employment	2 years after termination of the employee
Signed Code of Conduct obligations and signed Conflict of Interest declarations	2 years after termination of the employee

Attendance records	2 years after termination of the employee
Financial information such as payroll history including RRSP contributions, commission and bonus history	2 years after termination of the employee
Medical information	2 years after termination of the employee
Job descriptions	2 years beyond the period to which it applies
Performance assessments	2 years beyond the period to which it applies
Applications, resumes, and correspondence related to individuals not hired	2 years beyond the period to which it applies
Financial records	
Operations manuals, procedures, and internal control guidelines	Permanent
Signed annual financial statements and corresponding signed independent auditor reports	Permanent
Internal reports, including but not limited to: • reviews • special purpose reports • internal audit reports	10 years

Accounting documentation, including but not limited to: • general ledgers, general journals, financial records and supporting documentation • monthly and quarterly financial statements • monthly and quarterly management reports • month / quarter / year-end financial closing and reporting working papers • financial institution account statements and reconciliations • canceled cheques and cash register tapes • invoices • annual budgets • multi-year financial plans	8 years
Asset management documentation, including but not limited to: • tangible capital asset register • reserve fund reports • life cycle planning • capital project budgeting • contract and tendering provisions	8 years beyond completion of the project or asset utilization
If applicable, property taxation related documentation, including but not limited to: • property tax working papers • tax roll • tax filings	8 years
Operational records	
Operations manuals, policies and procedures	Permanent
Original patents, trademarks, and copyrights	7 years after the expiration of the right

Customs documents	7 years
Annual physical inventories	Permanent
Safety committee minutes, inspection reports and related action reports	10 years
Backup drives	
Backup drives before being overwritten or deleted.	3 months

6. Information Technology and Systems Policy

Purpose

The purpose of this policy is to make sure that the Yuułuʔiłʔatḥ Government's information is adequately protected, and that the information system has integrity to maintain and support the strategic and operational requirements of the Yuułuʔiłʔatḥ Government. Furthermore, this policy serves to address protocol for the onboarding and offboarding process of incoming and past employees regarding any and all information technology and systems of relevance to their positions.

This policy will also guide the acquisition, maintenance, and disposition of Yuułuʔiłʔatḥ Government hardware and software systems. This will include defining user access controls and acceptable use of Yuułuʔiłʔatḥ Government technology systems aligned with existing Yuułuʔiłʔatḥ Government human resource policy.

Scope

This policy applies to all staff involved in the selection, implementation, and ongoing use and maintenance of Yuułuʔiłʔatḥ Government information systems.

Background

The Information Technology and Systems Policy seeks to address the need for ensured integrity and continual accessibility of Government data. By addressing this need, the Yuułuʔiłʔatḥ Government can ensure and maintain their right to and use of knowledge sovereignty.

Policy Statement

It is the Executive's policy to establish a process around the Yuułuʔiłʔatḥ Government's information systems to support its operational data management requirements and have appropriate safeguards and monitoring processes in place. The Yuułuʔiłʔatḥ Government recognizes the importance of information technology and systems to ensure integrity and continual accessibility of Government data.

This policy asserts that proper preemptive risk assessment actions shall be taken on all Yuułuʔiłʔatḥ Government technology systems.

The Yuułuʔiłʔatḥ Government shall ensure all maintenance, diagnostic, and repair activities, whether performed on site or remotely and whether the equipment is serviced on site or removed to another location, are managed and monitored to preserve the confidentiality, integrity, and availability of the Yuułuʔiłʔatḥ Government information systems and data.

Since inappropriate use of Yuułuʔiłʔatḥ Government systems exposes Yuułuʔiłʔatḥ Government to risk, this policy explains responsibilities for the use of Yuułuʔiłʔatḥ Government information technology resources (including but not limited to computer systems, mobile devices, voice mail, email, the network, and Yuułuʔiłʔatḥ Government Internet connection) and specifies the actions that are prohibited.

While this policy is as complete as possible, no policy can cover every situation, so use common sense when using Yuułuʔiłʔatḥ Government resources. Supervisors should be consulted for any questions regarding what constitutes acceptable use.

All Information Technology users have the responsibility for safeguarding Information Technology resources from unauthorized use, intrusion, destruction or theft. This policy not only includes data, but also the computer systems, software, and hardware resources used to process electronic information, including those provided by third parties.

Roles and Responsibilities

Council is responsible for:

- approving the information technology policy used by the Yuułuʔiłʔatḥ Government
- approving exemption requests made by the Director of Operation

The Director of Operations is responsible for:

- ensuring that controls are in place over information technology and systems, whether performed by an internal staff member or outsourced
- establishing and implementing documented procedures for information technology and systems used by the Yuułuʔiłʔatḥ Government
- monitoring the performance of internal and/or external information technology professionals
- approving appropriate requests for access into Yuułuʔiłʔatḥ Government technology systems
- submitting exemption requests if necessary

The designated information technology professional (internal and/or external) is responsible for:

- maintaining the integrity of information technology and systems within the Yuułuʔiłʔatḥ Government
- receiving risk assessment reports
- following-up on privacy issues to assure resolution of the issue

Exceptions

The Director of Operations may submit an exemption request if they believe that compliance with any information security standards would adversely impact the governing process of the Yuułuʔiłʔatḥ Government.

Requests are to be approved by the Executive and must follow the format outlines in the related procedures.

Information Technology and Systems Administrative Procedures

Risk Assessment

To limit Information Technology vulnerabilities and avoid potential privacy breaches, the designated Information Technology professional must enforce the following Risk Assessment requirements for each Information Technology system classified as sensitive to:

a) Identify potential threats to the confidentiality, integrity, and availability of an Information Technology system and the environment in which it operates;

b) Determine the likelihood that threats will materialize;

c) Identify and evaluate vulnerabilities; and

d) Determine the loss impact if one or more vulnerabilities are exploited by a potential threat.

Risk assessments take into account vulnerabilities, threat sources, and security controls planned or in place to determine the level of residual risk posed to organizational operations and assets, individuals, and other organizations.

Risk assessments also take into account risk posed to Yuułuʔiłʔatḥ operations, Yuułuʔiłʔatḥ assets, or individuals from external parties, including but not limited to:

i. Service providers.

ii. Contractors operating information systems on behalf of the organization.

iii. Individuals accessing Yuułuʔiłʔatḥ information systems.

iv. Outsourcing entities.

v. Entities that may have an interested in information stored by the Yuułuʔiłʔatḥ Government

Risk assessments must be a collaborative effort among representatives of management, operational, technology and information security disciplines. Risk Assessments should be conducted every three years. Once completed, a risk assessment report should be provided to the Director of Operations

The designated Information Technology professional shall require that the Yuułuʔiłʔatḥ Government develop a risk assessment plan. Attached to the plan should be any previously conducted risk assessment reports.

The risk assessment plan must include the following

a) The contact information of individual submitting the plan,

b) The date of submission,

c) The system full name and abbreviation,

d) The planned assessor,

e) The date the last risk assessment was conducted for the system, and

f) Scheduled assessment completion date.

Note: Scheduled assessment completion date is the planned date of the completion of the future risk assessment covering a three-year period from the submission date.

Until completion of all corrective actions in the risk assessment, the Information Technology professional shall receive reports, at least quarterly, from the risk register. The quarterly risk update will report progress toward implementing outstanding risk treatments.

Upon completion of the risk treatments shown in the risk register, the Information Technology professional shall arrange for a follow-up review to verify implementation of the specified corrective actions.

Planning and Evaluation

The Director of Operations, with input from information technology professionals (internal and/or external), will make sure that information systems are developed that support the Yuułuʔiłʔatḥ Government's strategic plan and operations.

When there are no individuals internally with the requisite technical skills to identify information technology requirements or evaluate options, the Director of Operations will seek advice from a qualified external individual or organization.

Outsourcing

Subject to the purchasing section of the finance policy, the Director of Operations is responsible for arranging the selection of contractors providing information technology services, the definition of services in their contracts, establishing service level agreements and the administration of the contracts.

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

- a requirement that the service provider submits regular reports of all work performed on Yuułuʔiłʔatḥ Government information technology and systems
- a requirement that outsourced parties are responsible to comply with legal and regulatory requirements, including the protection of confidential and private information
- access by outsourced parties to Yuułuʔiłʔatḥ Government information is provided on a 'need to know basis' only

Controlled Maintenance

The designated Information Technology Professional must Schedule, perform, document, and review records of maintenance and repairs on information system components in accordance with Yuułuʔiłʔatḥ Government requirements.

These requirements include:

- Controlling all maintenance activities, whether performed on site or remotely and whether the equipment is serviced on site or removed to another location
- Explicitly approving the removal of the information system or system components from organizational facilities for off-site maintenance or repairs
- Sanitize equipment to remove all information from associated media prior to removal from organizational facilities for off-site maintenance or repairs
- Check all potentially impacted security controls to verify that the controls are still functioning properly following maintenance or repair action; and
- Maintain information system maintenance records for the life of the system that include:

    Date and time of maintenance.

    Name(s) of the individual(s) performing the maintenance.

    Name of escort (if necessary).

    Description of maintenance performed.

    List of equipment removed or replaced (including identification numbers if applicable).

Data Management

Subject to the Yuułuʔiłʔatḥ Government's *Records and Information Management Policy*, data retention allows access to appropriate data to specified personnel where required, depending on the type of data retained.

All sensitive, valuable, or critical data stored on Yuułuʔiłʔatḥ Government information technology systems must be regularly backed-up.

Backup drives must be stored in a secure location with access limited to the Director of Operations and limited to other staff as appropriate. Ideally, backup drives will be securely stored at an offsite location that is easily accessible to individuals with authorized access.

Acceptable use of Yuułuʔiłʔatḥ Government Network Systems

Account Use

Network accounts must be implemented in a standard fashion and used consistently across the organization.

Users of Yuułuʔiłʔatḥ Government Information Technology resources are prohibited from knowingly disclosing or modifying any assigned or entrusted access control mechanism (such as: log-in identifiers, passwords, terminal identifiers, user identifiers, digital certificates, IP addresses, etc.) for any purpose other than those required to perform any authorized employment functions.

Internet Use

Acceptable use of the Internet consists of activities necessary to support the purpose, goals, and values of the Yuułuʔiłʔatḥ Government and each user's authorized job functions.

The following are Internet Use guidelines:

a) Do not access online games, including games found on social websites.

b) Do not use streaming media unless its use is work related.

c) To access the Internet, use only software that is part of the Information Technology standard software suite or that has been approved by Information Technology. This software must incorporate all vendor-provided security patches required by Information Technology.

d) If using blogs or websites, do not discuss Yuułuʔiłʔatḥ Government matters or publish material that shows the Yuułuʔiłʔatḥ Government in a negative light. The user assumes all risks associated with blogging and social networking.

e) Make sure all files downloaded from the internet are scanned for viruses using the approved Information Technology -distributed software suite and current virus detection software.

f) Make sure content on all Yuułuʔiłʔatḥ Government websites and social medias has been approved by the department publishing the information.

g) Do not make offensive or harassing material available through Yuułuʔiłʔatḥ Government websites or social media accounts.

h) Do not post personal commercial advertising on the Yuułuʔiłʔatḥ Government websites or social media accounts.

i) Do not use Yuułuʔiłʔatḥ Government Internet access for personal financial gain unrelated to Yuułuʔiłʔatḥ Government job duties.

j) Do not make data available on Yuułuʔiłʔatḥ Government websites or social media without ensuring that the material is accessible to only those groups and individuals who are authorized.

Network Access

Avoid accessing network data, files, and information not directly related to your job. The existence of access capabilities does not imply permission to use this access.

Unacceptable Use

Users cannot use the Yuułuʔiłʔatḥ Government network or systems to:

i. Access data or programs to seek information on, obtain copies of, or modify files, other data or passwords belonging to other users.

ii. Access, download, print, or store sexually explicit material

iii. Gamble,

iv. Perform activities that are illegal under local, provincial, federal, or international law.

v. Knowingly send sensitive data unencrypted through email.

vi. Tamper with or otherwise attempt to circumvent security controls.

   1. Understand that tools to inventory the hardware and software will be installed by Yuułuʔiłʔatḥ Government on each Yuułuʔiłʔatḥ Government device and that removing, tampering or disrupting these tools in any capacity is not allowed.
   2. Understand that image and operating system integrity standards will be kept on all PC's. Non-standard applications or operating systems that are needed for business functions will be installed by the Yuułuʔiłʔatḥ Government.

vii. Use for product advertisement.

viii. Install unauthorized encryption hardware or software on Yuułuʔiłʔatḥ Government systems.

ix. Add hardware to, remove hardware from, or modify hardware on a Yuułuʔiłʔatḥ Government system.

x. Sending large numbers of messages to an individual or a group (Mail bombing).

xi. Attempting to subscribe anyone else to mailing lists.

xii. Perform activities that might cause embarrassment, loss of reputation, or other harm to the Yuułuʔiłʔatḥ Government

xiii. Send out defamatory, discriminatory, vilifying, sexist, racist, abusive, rude, insulting, threatening, obscene, or otherwise inappropriate messages or media.

xiv. Perform activities that cause an invasion of privacy.

xv. Perform activities that cause disruption to users, services, or equipment or create a hostile workplace.

   1. Disruptions include, but are not limited to, distribution of unsolicited advertising, intentional propagation of computer viruses, and using the network to gain unauthorized entry to any other machine accessible through the network.

xvi. Perform port scanning, security scanning, network sniffing, keystroke logging, or other IT information gathering techniques when they are not part of your job.

xvii. Download, install or distribute, without the authorization of the designated Information Technology Professional

   1. Games.
   2. Screen Savers.
   3. Peer-to-peer file-sharing programs

4. Non-Yuułuʔiłʔatḥ Government supported software

xviii. Reveal personal or network passwords to others, including coworkers, family, friends, or other members of the household, when working from home or remote locations.

If there are any questions about allowable programs or materials on the Yuułuʔiłʔatḥ Government network, please contact your supervisor.

Further instructions regarding appropriate network access are located on Page 48 of the Yuułuʔiłʔatḥ Government *Employee Handbook.*

Overuse

Users should not knowingly perform actions that negatively affect the computer network or other corporate resources or that negatively affect job performance.

Copyright Infringement

Users are prohibited from using the Yuułuʔiłʔatḥ Government computer systems and networks to download, upload, or otherwise handle illegal or unauthorized copyrighted content.

All of the following activities constitute violations of this Acceptable Use Policy if done without permission of the copyright owner:

a) Copying and sharing images, music, movies, or other copyrighted material using P2P file sharing or unlicensed CDs or DVDs

b) Posting or plagiarizing copyrighted material

c) Downloading copyrighted files that have not been legally procured

d) This list does not include all violations; copyright law applies to many more activities

Remote Access

Yuułuʔiłʔatḥ Government employees and partners who remotely access agency network resources will use only Yuułuʔiłʔatḥ Government provided equipment, unless otherwise authorized. Access to network resources, including the Internet, will be via broadband or modem dial-in and Virtual Private Networking (VPN). This does not apply to users accessing Microsoft Outlook Web Access from a remote location.

In the case that an employee has been authorized to use non-Yuułuʔiłʔatḥ Government provided technological equipment, such technological equipment must comply with all standard information technology security standards, including but not limited to the installation of antivirus software.

Yuułuʔiłʔatḥ Government employees and business partners must only use approved remote access processes and procedures when connecting remotely.

Email Usage

Using any outbound email sent from a Yuułuʔiłʔatḥ Government agency email account is to be considered as equivalent to a message sent on agency letterhead, therefore:

a) The content and tone of any such message must reflect the official responsibilities of the author;

b) The content of any message should use proper grammar and spelling

c) Any untrue, prejudicial, misleading, obscene, racist, sexist, or other unprofessional remarks may make the organization liable for legal action and will be grounds for further consequential actions

It is prohibited to:

a) Send an email using another's identity, an assumed name or anonymously;

b) Use Yuułuʔiłʔatḥ Government email for personal use

c) Use email for the propagation of viruses, computer worms, Trojan Horses, and other malicious software.

Further instructions regarding email usage are located on Page 49 of the Yuułuʔiłʔatḥ Government *Employee Handbook.*

Protecting Electronic Devices

To protect electronic devices:

a) Password-protect all PCs, laptops, portable computing devices, and workstations, with the automatic activation feature set for a maximum of 30 minutes.

b) Use IT-provided encryption or other security measures to protect information stored on laptops and portable computing devices and to protect such devices from theft.

c) Make sure all PCs, laptops, and workstations contain approved virus-scanning software with a current virus database.

d) If a portable device supports virus-scanning software, make sure the software is active.

e) If it is determined that required security-related software is not installed or that a remote computer has a virus, is party to a cyber-attack, or in some way endangers the security of Yuułuʔiłʔatḥ Government network, disable the account and network connection. Access will be re-established once IT determines the computer or device to be safe.

f) Make sure unattended portable computing devices are secured from unauthorized access. For example, make sure these devices are locked in an office, locked in a desk drawer or filing cabinet, or attached to a desk or cabinet via a cable lock system. Logical security options include screensaver passwords and automatic session timeouts.

Protecting Data

Store all data files and other critical information on a network share, such as the "S:\" drive. These drives should be backed up nightly and backups are sent off-site for disaster recovery purposes. All sensitive data must be stored on network drives.

Store media (diskettes, tapes, CD-ROM, flash drives, portable drives etc.) in a secure location away from extreme temperature and sunlight.

Peer-To-Peer File Sharing

Peer-to-Peer (P2P) networking is not allowed on the Yuułuʔiłʔatḥ Government network under any circumstances.

Bandwidth Usage

Excessive use of Yuułuʔiłʔatḥ Government bandwidth and other computer resources is not permitted. Perform large file downloads and other bandwidth-intensive tasks that can degrade network capacity or performance only during times of low usage.

Incidental Use

Occasional and incidental personal use of Yuułuʔiłʔatḥ Government Information Technology resources is permitted, providing such use does not violate any Yuułuʔiłʔatḥ Government policies and procedures, interfere with the conduct of state business or job performance (based on volume or frequency), involve solicitation or illegal activities, adversely affect the efficient operations of the agency's computer systems, harm Yuułuʔiłʔatḥ, or involve for-profit personal business.

Incidental personal use of electronic mail, Internet access, fax machines, printers, copiers, etc., is restricted to approved users; it does not extend to family members or other acquaintances.

Note: This policy does not attempt to define all acceptable or unacceptable personal use. The above information is provided as a guideline. If the employee is unclear about acceptable personal use, he/she should seek the advice of his/her supervisor or division director.

Use For Illegal Activities

Users must not knowingly use Yuułuʔiłʔatḥ Government owned, or Yuułuʔiłʔatḥ Government provided computer systems for activities that are considered illegal under local, provincial, federal, or international law.

Such actions include, but are not limited to:

k) Unauthorized Port Scanning

l) Unauthorized Network Hacking

m) Unauthorized Packet Sniffing

n) Unauthorized Packet Spoofing

o) Unauthorized Denial of Service

p) Unauthorized Wireless Hacking

q) Any act that might be considered an attempt to gain unauthorized access to or escalate privileges on a computer or other electronic system

r) Acts of Terrorism

s) Identity Theft

t) Spying

u) Downloading, storing, or distributing violent, perverse, obscene, lewd, or offensive material as deemed by applicable statutes

v) Downloading, storing, or distributing copyrighted material

Personal Storage Media

Personal storage devices represent a serious threat to data security and are prohibited on Yuułuʔiłʔatḥ Government network.

Software Installation

Installation of non-Government-supplied programs is prohibited. Numerous security threats can pretend to be safe software; malware, spyware, and Trojans can all be installed without user knowledge through games or other programs. Additionally, software can cause conflicts or have a negative impact on system performance.

Information Technology Equipment and Software Purchase

All Information Technology hardware and software purchases needed to conduct internal Yuułuʔiłʔatḥ Government business must be done by the Yuułuʔiłʔatḥ Government.

Access Management

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

Requests for access to the Yuułuʔiłʔatḥ Government network, accounting system, or other access restricted information system must include a description of an employee's role and rationale for the level of access required. Signed approval must be obtained from the Director of Operations or other assigned staff with proper authorization from the Director of Operations.

User ID and password are required for access to the network and other critical programs/areas such as the accounting system.

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

Upon termination of employment, all security-related organizational information system-related property in position of the former employee must be retrieved (e.g., hardware authentication tokens, system administration technical manuals, keys, identification cards, and building passes).

Upon termination of employment, Access to the former employee's organizational information and information systems formerly controlled by terminated individual must be retained.

i. Prior to archiving or permanent disabling of accounts, transfer all Yuułuʔiłʔatḥ Government information to appropriate personnel or archives.

ii. In the event of an adverse removal or involuntary termination, rotate the employee or contractor to a non-sensitive position or restrict access or rights to information systems before notification, whenever possible, to avoid the potential for malicious actions to information systems.

The following activities must be performed for all personnel, including contractors, leaving, changing jobs, or on extended absences:

a) Change or cancel all passwords, codes, user IDs, and locks.

b) Disable user IDs for extended absences (60 days).

c) Update access control lists, mailing lists, etc.

d) Collect all keys, badges, and similar items.

e) Reconcile any financial accounts over which the employee had control.

f) Ensure electronic records are accessible and properly secured, filed, or appropriately disposed.

Support personnel must notify the user when attempting to take control of a workstation. All instances where specific software is loaded to remotely control a workstation must be removed when the support function is completed. The use of the remote-control software must be in accordance with applicable agreements.

Information System Security

Security tools and techniques are implemented to enable restrictions on access to programs and data.

Security tools and techniques are administered to restrict access to programs and data.

Each computer resource must have an approved antivirus program installed. The following standards must be met:

- the antivirus program must not be disabled and must be configured to scan all programs and files upon execution and must have real time protection enabled
- antivirus files must be updated on the network regularly or whenever a new threat is identified

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

- firewall and proxy servers must be securely installed
- detailed firewall logs must be maintained
- alerts must be raised if important services or processes crash

Change Management

All new data structure and modifications to data structure will be tested before implementation.

All computers, hardware, software and communication systems used for a production environment must employ a documented change control process. The change management process should include the following activities:

- data structure is consistent with the needs of the Yuułuʔiłʔatḥ Government
- description and rationale for the new network, hardware, communication and systems software change and how it is consistent the needs of the Yuułuʔiłʔatḥ Government
- assessment of any risks involved with the change
- roll-back considerations
- implementation considerations
- description of required testing
- approval from the relevant Officer
- communication of changes to Yuułuʔiłʔatḥ staff as appropriate

Monitoring

Only approved and authorized programs will be implemented onto Yuułuʔiłʔatḥ Government information management systems. The Director of Operations, or other assigned staff with proper authorization from the Director of Operations will conduct periodic reviews of the workstations and the system to monitor compliance with this requirement.

A log of staff, their user IDs, and their access levels within Yuułuʔiłʔatḥ Government information systems will be maintained. On a periodic basis, the Director of Operations will review the log to make sure users and the associated access rights are appropriate. Access rights that will be monitored include the following:

- user access management (i.e., the accounting system)
- third party access (i.e., outsourced information technology professionals)
- network access and file sharing
- remote and VPN access

Network system performance is monitored on a regular basis.

The firewalls must be monitored regularly.

Exception requests

If the Director of Operations determines that compliance with any information security standards would adversely impact the governing process of the Yuułuʔiłʔatḥ Government, the Director of Operations may request approval to deviate from a specific requirement by submitting a Yuułuʔiłʔatḥ Government Security Policy & Procedure Exception Request to the Executive.

The Executive must approve the exception request through the standard policy approval process.

a) Each request for an exception must provide:

   i. Technical Justification detailing the reasons for the exception including the Yuułuʔiłʔatḥ Government Security Policy or Procedure for which the exception is being requested;

   ii. Scope including quantification and requested duration (not to exceed one (1) year);

   iii. Analysis of all associated risks;

   iv. Explanation of the controls to mitigate the risks;

   v. Explanation of any residual risks; and

   vi. Approval of the department managers in any area related to the requested exception.