Community. Leadership. Pride.

WESTBANK FIRST NATION

Procedure 2017-39

Privacy Incident Management

ISSUED BY	xatús xʷstcutn/Council Secretariat
DEPARTMENT	Council Secretariat
EFFECTIVE DATE	2024-04-29
RELATED DOCUMENTS	WFN Freedom of Information and Protection of Privacy Law Policy 2015-82 Personal Information and Privacy Protection Standard 2015-02 Security of Information Standard 2017-17 Personal Information Inventory Standard 2018-05 Securing Information When Traveling or Working Offsite Procedure 2017-36 Making and Processing Information Requests
IMPLEMENTATION	Applies to individuals requesting an investigation into an alleged breach of privacy and to stqáʔtkʷɬniẇt sqilxʷ/Westbank First Nation (WFN) səxʷkʷuĺm/Workers responsible for processing those requests. This Procedure is a review, update, and revision to, and supersedes Procedure 2017-39 Privacy incident Management approved and signed by the Council Secretariat/Legal Counsel on spáqtan/January 7, 2019 and Procedure 2017-38 Processing Privacy Incident Investigation Requests approved and signed by the Acting Legal Counsel/Council Secretariat on sk'əlwístən/September 23, 2020.

Purpose This Procedure outlines the steps required to request an investigation into an alleged breach of privacy and to manage that alleged privacy incident.

1. Guiding Principles

a) Individuals may complain of a privacy issue (e.g. risk, concern, complaint, incident of actual or suspected unauthorized access, misuse of personal information, inappropriate disclosure, etc.) that requires investigation and reporting (Privacy Incident). The Privacy Incident may be perceived or actual, and it may pertain to that person or another party. It must also be considered a potential privacy incident until the investigation is complete.

b) Investigations of Privacy Incidents must be conducted in a confidential manner, with all relevant and related information deemed sensitive. At a minimum, investigations must include the following:

- **i.** An immediate containment of any potential breach of privacy.
- **ii.** An investigation and documentation of the details of the Privacy Incident, including cause and extent.
- **iii.** A determination on whether an actual breach of privacy occurred, and if so;
  - **1)** Recommendations for appropriate disciplinary action,
  - **2)** Identification of the risks and plans to mitigate the breach of privacy in the future;

Privacy Incident Management

1. Guiding Principles (Continued)

and

3) Communication of the results of the investigation and resulting action plans to the relevant WFN leaders.

c) To ensure accountability, the Privacy Officer must maintain a secured Privacy Incident Register (Appendix A) for each fiscal year which tracks the status of Privacy Incidents, and submit it to the səxʷkʷulm̓ kl̓ yʕayʕat/Director of Operations at the end of each fiscal year.

2. Procedure

Responsibility	Step	Description of Task
Individual requesting an investigation into an alleged Privacy incident (Requestor)	**a)**	**i.** Requestors who are səxʷkʷulm: Immediately report the Privacy incident to your supervisor and the WFN Privacy Officer. **ii.** Requestors who are not səxʷkʷulm: Submit a completed Privacy Incident Investigation Request (Appendix B) to the WFN Privacy Officer.
Supervisor and Privacy Officer	**b)**	Ensure immediate steps are taken to contain the Privacy incident, through measures such as, but not limited to; **i.** Stopping the unauthorized practice, **ii.** Changing locks, **iii.** Changing or revoking computer access codes, **iv.** Recovering devices or Records, **v.** Shutting down the system which is subject to the breach; and **vi.** Correcting weaknesses in physical security.
Privacy Officer	**c)**	**i.** Create a Privacy incident investigation file. **ii.** Depending on the severity and nature of the Privacy incident; **1)** Immediately report the Privacy incident to the Director of Operations, and the Information Technology Manager if applicable, **2)** Designate a lead investigator and Privacy incident response team to investigate the Privacy incident; and **3)** Contact police if theft or other crime is suspected. **iii.** Respond to the Requestor of the Privacy Incident Investigation Request (Appendix B) within ċiɬkst sx̌ɬx̌ʕaɬt/five (5) business days of receipt of the request.

2. Procedure (Continued)		
Responsibility	**Step**	**Description of Task**
Privacy Officer	**c)**	**iii.** Liaise with the Requestor under Section 2., Step a)i. or ii. of this Procedure, as appropriate, to seek any relevant information to investigate the alleged privacy incident and to identify their desired outcome.
Privacy Officer or Designate	**c)**	**i.** Within ʔasíl sx̌ɬx̌ʕaɬt/two (2) days after discovery of the Privacy incident and in consultation with relevant Directors; **1)** Conduct a preliminary investigation into and analysis of cause and risks of the Privacy incident; and **2)** Take further containment steps, if required, based on the preliminary assessment. **ii.** Within naqs skʕacíẇs/one (1) week after discovery of the Privacy incident; **1)** Complete Sections A to D of the Privacy Incident Investigation Report (Appendix C), **2)** Ensure that any individuals who need to be notified about the Privacy incident are notified; and **3)** Complete Section E of the Privacy Incident Investigation Report (Appendix C.) **iii.** Within kaʔɬís skʕacíẇs/three (3) weeks after discovery of the Privacy incident, determine if further in-depth investigation is required and if so, launch the investigation. **iv.** Within twenty (20) business days of receipt of the complaint of the alleged Privacy incident under Section 2., Step a) of this Procedure, respond to the Requestor advising them; **1)** Of the results of the investigation conducted, in accordance with Section 2, Step d)i. of this Procedure; or **2)** That the circumstances of the preliminary investigation warrant an extension of time to provide them with a response. **v.** Within ʔasíl x̌iyaɬnxʷ/two (2) months after discovery of the Privacy incident, review the investigative findings and develop and being implementing prevention strategies. **vi.** When the investigation of the Privacy incident is complete,

2. Procedure (Continued)		
Responsibility	**Step**	**Description of Task**
Privacy Officer or Designate	**e)**	complete Sections F and G of the Privacy Incident Investigation Report (Appendix C) and submit the report to the Privacy Officer.
Privacy Officer	**f)**	When the investigation of the Privacy incident is complete; **i.** Advise the Requestor, in writing, of the outcome of the investigation and the proposed action, if any, WFN intends to take, summarizing the reasons for the decision and advising them that they may request an adjudicator review if they are dissatisfied with the outcome of the investigation, **ii.** If the investigation revealed that WFN or one of its contracted service providers appeared to have mishandled information held by WFN, direct the relevant Director regarding appropriate steps to take to ensure a similar incident does not recur, **iii.** Enter the details of the Privacy Incident into the Privacy Incident Register (Appendix A); and **iv.** Send the contents of the Privacy incident investigation file under Section 2, Step c)i. of this Procedure to Records and Information Management for archiving.
Privacy Officer	**g)**	At the end of each fiscal year, provide the Privacy Incident Register (Appendix A) to the Director of Operations.

3. Definitions

"Personal Information" means information about an identifiable individual not including information that cannot be associated with a specific individual. In addition to the common basic elements used to identify and interact with an individual such as the individual's name, gender, physical characteristics, address, contact information, identification, and file numbers, also included are criminal, medical, financial, family, and educational history as well as other details specific to the individual's life.

"Privacy Incident" means unauthorized access to or unauthorized collection, use, disclosure, or disposal of Personal Information. Privacy Incidents include, but are not limited to;

a) Misdirected communications such as, but not limited to, mail, email and facsimile,

b) Lost or stolen records,

c) Lost or stolen devices, whether encrypted or unencrypted,

3. Definitions (Continued)

d) Records or devices stolen or otherwise removed from a vehicle,

e) Unsecured storage, transportation, or transmission of Personal Information,

f) Records located in a public place,

g) Inadequate safeguards,

h) Inappropriate access, whether accidental or deliberate,

i) Sharing Personal Information for unauthorized purposes,

j) Inappropriate disclosure to unauthorized individuals,

k) Inappropriate disclosure via social media, texting, or email,

l) Inappropriate use of photography or recordings,

m) Inappropriate collection or over-collection of personal information; and

n) Network attacks, hacking, phishing, and malware.

"Record" means information created, received, and maintained by WFN as evidence of its legal obligations or in the transaction of WFN business, which enables and documents decision-making, and supports WFN reporting, performance, and accountability requirements. Records include books, documents, maps, drawings, photographs, letters, and any other thing on which Information is recorded or stored by graphic, electronic, mechanical, or hardcopy means.

"Worker" (səxʷkʷuɬm) means any employee, volunteer, contractor, client, or other visitor who performs tasks on behalf of WFN at any WFN workplace through a formal arrangement including, but not limited to, an employment agreement, contract, remote work agreement, or approved volunteer application.

4. Cultural Context of Definitions

səxʷkʷuɬm (Worker) The person or profession (səxʷ) "to work, fix, or create" (kʷuɬ). The root of səxʷkʷuɬm comes from kʷɬncutn, the word for "Creator". WFN's səxʷkʷuɬm are, in a sense, creators, working to provide important and valuable programs, services, and tools, and to solve issues as they arise, to ensure a productive, excellent, and fruitful government and community. The word also denotes value. Originating from the Creator, səxʷkʷuɬm have inherent value and are to be treated as such by their supervisors, colleagues, and clients.

səxʷkʷuɬm̓ kɬ̓ yʕayʕat (Director of Operations) The səxʷkʷuɬm who is over (kɬ̓) everyone (yʕayʕat). Through their team of Directors, they oversee all WFN's səxʷkʷuɬm.

sk'əlwístən (September) Moon of the spawning fish (sk'əlwíst means spawning fish).

spáqtan (January) Moon of whiteout when everything is white (piq means white).

spɬiƛ̓mtən (April) Moon of bitterroot (spɬiƛ̓m̓).

stqáʔtkʷɬniẇt sqilxʷ/Westbank First Nation (WFN) The people (sqilxʷ) living where wind blows

4. Cultural Context of Definitions (Continued)

(niẇt) and forms swamps or puddles alongside a large lake (stqáʔtkʷɬ). Being a windy area, the winds would cause the water to wash upon the shore leaving puddles and pools to cleanse the land and which would either seep into the land, creating wet, marshy areas or wash back into the lake. This area has been identified as the portion of syilx territory from Antler's Beach/Hardy Falls area to around the Gellatly/Green Bay area (essentially from the bend in the lake along the whole shoreline) but it includes a few other areas, including xʷaɬ mnik, the area closer to Tsinstikeptum Indian Reserve #10 and many other areas that have specific place names.

xatús xʷstcutn (Council Secretariat) Traditionally, xatus were the heads of extended family clans, and could be either male or female. xatus took care of keeping good relations between their family members and other family clans. If a family member did wrong to a person from another family and the household head could not straighten it out, then it went to all the family heads.

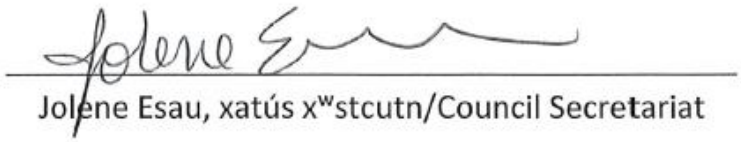
5. Appendices

Appendix A – Privacy Incident Register

Appendix B – Privacy Incident Investigation Request

Appendix C – Privacy Incident Investigative Report

Council Secretariat approved this Procedure on the 29th day of sp̓iƛ̓mtən/April 2024.



Jolene Esau, xatús xʷstcutn/Council Secretariat

Privacy Incident Management

Appendix A – Privacy Incident Register

WESTBANK FIRST NATION

Privacy Incident Register _____
[INSERT YEAR]

Community. Leadership. Pride.

Item #	Date yyyy-mm-dd	Type of Privacy Incident	Description	If a Complaint: Allowed in Full/Allowed in Part/Disallowed?	Actions Taken on Completion of Investigation	Recommendations made by Privacy Officer

Appendix B – Privacy Incident Investigation Request (page 1)

Privacy Incident Investigation Request

To be completed by individuals requesting an investigation into the handling of information held by Westbank First Nation, in accordance with Policy 2015-82 Personal Information and Privacy Protection and related governance instruments. Submit to the WFN Privacy Officer when complete.

Protected when Submitted

Community. Leadership. Pride.

Privacy Statement and Resolution

Westbank First Nation (WFN) has physical, electronic, and procedural safeguards in place to protect personal information. WFN commits to investigating your concern and informing you of any steps taken, or any steps that will be taken, in the resolution of your concern.

The information collected in this form is collected under the authority of the WFN Freedom of Information and Protection of Privacy (FOIPP) Law for the purposes of assessing, investigating and reporting on your privacy concern. The Privacy Officer may collect information about you and the incident you are requesting an investigation into from other individuals or organizations involved for the above purposes.

As part of the FOIPP complaint review process, the Privacy Officer may disclose the information you provide to the individuals or organizations named in the Privacy Incident Investigation Request and, if necessary, to others who have information relevant to your complaint.

You are not required to provide your contact details and may make your privacy complaint anonymously. However, if you do not provide your contact details, the Privacy Officer may not be able to properly investigate your complaint or inform you of the action, if any, taken in response to your complaint.

Individual Requesting a Privacy Incident Investigation

Last Name	First Name	WFN Member ☐ Yes ☐ No

Cell Phone Number	Home Phone Number	Work Phone Number

Current Address *(Include street address, city, province, and postal code)*

Email Address

Privacy Incident Investigation Request (Last Updated July 2023) Page 1 of 2

Appendix B – Privacy Incident Investigation Request (page 2)

Nature of the Privacy Incident I have reason to believe that one or more of the following has occurred: ❑ WFN has inappropriately collected, disclosed, used, or disposed of my personal information. ❑ WFN has inappropriately collected, disclosed, used, or disposed of the personal information of someone I am representing. ❑ Other – Please explain:
If you are submitting this request on behalf of another person, please provide the following information and attach proof of your authorization to represent that individual.
Name of Person You are Representing:
Relationship to the Person You are Representing:
Details of the Privacy Incident Investigation
Please describe the events or circumstances that led to your concern. *(e.g. names or positions of people involved in the incident, the location where the incident occurred, and any other factors you consider relevant).*
Signature

	Date

Appendix C – Privacy Incident Investigative Report (page 1)

Privacy Incident Investigation Report

To be completed by the lead investigator into privacy breach incidents, in accordance with Procedure 2017-39 Privacy Breach Management.

Protected when Completed

Community. Leadership. Pride.

Details of Privacy Incident	
Date	
Name of Person Completing this Report	
Date of Incident	
Location of Incident	
Date Incident was Discovered	
Name and Contact Information of Complainant *(Attach Privacy Incident Investigation Request received, if applicable)*	
Risk Evaluation	
Nature and Cause of the Privacy Incident	
Type of Information Subject to the Privacy Incident	❑ Individual's Name ❑ Address ❑ Social Insurance Number (SIN) ❑ Financial ❑ Indian Registry Number ❑ Medical ❑ Other *(Describe below)*
Estimated Number of Individuals Affected	
Type of Individuals Affected	❑ WFN Member ❑ WFN Employee ❑ Client or Customer ❑ Student ❑ Other *(Describe below)*

Appendix C – Privacy Incident Investigative Report (page 2)

Safeguards	
Describe the Physical Security Measures *(i.e. locks, alarm systems, etc.)*	
Describe the Technical Security Measures *(i.e. encryption, password, etc.)*	
Describe Organizational Security Measures *(i.e. security clearances, policies, role-based access, training programs, contractual provisions, etc.)*	

Real or Potential Harm from the Breach

- ❑ **Identity Theft**
  (Most likely when the breach includes loss of SIN, credit card numbers, driver's license numbers, personal health numbers, debit card numbers with password information and any other information that can be used to commit financial fraud.)
- ❑ **Risk of Physical Harm**
  (When the loss of information places any individual at risk of physical harm, stalking or harassment.)
- ❑ **Hurt, Humiliation, Damage to Reputation**
  (Associated with the loss of information such as mental health records, medical records, disciplinary records.)
- ❑ **Loss of Business or Employment Opportunities**
  (Usually because of damage to reputation to an individual.)
- ❑ **Breach of Contractual Obligations**
  (Contractual provisions may require notification of third parties in the case of a data loss or privacy breach.)
- ❑ **Future Breaches Due to Similar Technical Failures**
  (Notification to the service provider may be necessary if a recall is warranted and/or to prevent a future breach by other users.)
- ❑ **Failure to Meet Professional Standards or Certification Standards**
  (Notification may be required to professional regulatory body or certification authority.)
- ❑ ***Other** (Please specify):*

Privacy Incident Investigation Request Page 2 of 4

Appendix C – Privacy Incident Investigative Report (page 3)

Notification		
Has the Privacy Officer been notified?	❑ Yes *(Please specify who and when)*	❑ No *(Please specify when notification will take place)*
Have the police or other authorities been notified? *(i.e. professional bodies or persons required under contract)*	❑ Yes *(Please specify who and when)*	❑ No *(Please specify when notification will take place)*
Have affected individuals been notified?	❑ Yes Number of individuals notified: _____ Date of notification: _____ Manner of notification:	
	❑ No *(Please explain why not)*	
What information was included in the notification?	❑ Date of the breach ❑ Description of the breach ❑ Description of the information inappropriately accessed, collected, used or disclosed ❑ Risk(s) to the individual caused by the breach ❑ Steps taken so far to control or reduce the harm ❑ Future steps planned to prevent further privacy breaches ❑ Steps the individual can take to reduce the harm ❑ Organization contact information for further assistance ❑ Other *(Please specify):*	

Privacy Incident Investigation Request Page 3 of 4

Appendix C – Privacy Incident Investigative Report (page 4)

Prevention	
Describe the immediate steps taken to contain and reduce the harm of the breach *(i.e. locks changed, computer access codes changed or revoked, computer systems shut down)*	
Describe the long-term strategies you will take to correct the situation *(i.e. staff training, policy development, privacy and security audit, contractor supervision strategies, improved technical security architecture, improved physical security)*	
Name and Signature	
Name *(Please print):*	
Position	
Signature	