



Fish & Wildlife Branch Data Sharing Policy



March 2024

Contents

- Guiding Statement..... 2
- Purpose 2
- Related Policies..... 2
- Scope 3
- Definitions..... 3
- Governing Principles 7
- Policy Statements 8
- Procedures 9
 - Data and Information Acceptance and Management..... 10
 - Identifying Sensitive Ecological Data..... 13
 - Data Distribution 19
 - Administration 26
- Appendix A: Confidentiality and Non-disclosure Agreement 28

Guiding Statement

Our data are reliable, secure, and available for use internally and by individuals, organizations or governments. We share information among parties to facilitate effective and informed planning, decision-making and research.

Purpose

The purposes of this policy are to:

1. Identify a set of principles to govern the acceptance, management and distribution of species and ecosystems data and information.
2. Establish a common terminology and associated definitions.
3. Identify categories of species and ecosystems data and information that may be deemed [Sensitive Ecological Data](#) and whose distribution may be restricted ([Restricted Access](#)).
4. Reference a set of procedures that guide policy implementation.

This policy does not supersede the Access to Information and Protection of Privacy (ATIPP) Act and requirements to release information under an ATIPP request.

Related Policies

- Access to Information and Protection of Privacy Act ([ATIPP](#))
- Access to Information and Protection of Privacy Regulation ([ATIPP Regulation](#))
- GAM Directive 2.14 – Records Management
- GAM Policy 2.26 – Information Management Governance Policy
- GAM Directive 2.3 – Information and Communications Technology Program
- Management Board Directive 34/19 – Open Information and Open Data Directive

Scope

This policy applies to:

- All data and information gathered by the Fish and Wildlife Branch as part of wildlife¹, habitat and biodiversity research and population monitoring projects and includes harvest data associated with fishing, hunting, trapping or related activities. This includes digital datasets and spatial files collected by a third party, such as a contractor or partner, and stored and managed by the Fish and Wildlife Branch.

¹ wildlife is defined as all organisms that grow or live wild in an area.

Definitions

Business Case

The demonstration by a **Client** of the existence of a legitimate business or regulatory requirement to warrant provision of **Restricted Access** data and information. The primary considerations for assessing a Business Case are interests in planning or decision-making or a high likelihood the distribution of data and information will ultimately serve conservation and recovery, and the existence of appropriate controls to minimize risk or misuse of the data.

Client

A consumer of data and information. For the purposes of these policies and procedures a client specifically refers to an individual, or representative of an agency or organization, who has requested access to data and information.

Confidentiality and Non-disclosure Agreement

A document that prescribes the terms of **Client** access, constraints to the use of, and redistribution of **Sensitive Ecological Data**.

Data Owner

The Fish and Wildlife Branch's designated authority over the management and security of the relevant data system(s) and the data managed within. The Fish and Wildlife Branch Director is the Data Owner, unless this authority is delegated to another staff.

Data Security

Data security, or information security, includes the practices, policies and principles to protect data and information from unauthorized access, accidental loss, destruction, corruption, or theft. It includes organizational policies and procedures that govern how data access is managed and the operations and management of data systems that adhere to industry standards for protecting database software, hardware, and the data contained within.

Data Security Committee

A Department of Environment committee tasked with evaluating and providing recommendations regarding **Sensitive Ecological Data** to the data authority (**Data Owner**).

Data and Information Whose Release May Adversely Affect Government Programs

Data and information whose unrestricted distribution and sharing are likely to harm government management programs. For detailed descriptions, see the relevant procedure in this document.

Data and Information Whose Release May Adversely Affect Program Relations

Data and information whose unrestricted distribution and sharing are likely to harm program relations of the Fish and Wildlife Branch, Department of Environment, or Government of Yukon. For detailed descriptions, see the relevant procedure in this document.

Data Sharing Agreement

A signed document used to formalize the interests of both the Fish and Wildlife Branch and **Client** in sharing and using data and information, including any restrictions or guidance on use, distribution, or attribution.

Ecological Data and Information

Data and information (metadata or products derived from data) of a biological or geographical nature pertaining to **Elements** as defined in this policy.

Element(s)

An identifiable and recognized unit of natural biological diversity. Elements represent species and infraspecific taxa (taxonomic level below that of species), natural ecosystems, or other non-taxonomic biological entities (e.g., migratory species aggregation areas or mineral licks).

Element(s) Susceptible to Harm

Elements for which unrestricted sharing of data and information of a biological, geographical, or ecological nature places populations, residences, or occurrences at risk of intentional or inadvertent harm or interferes with their conservation or recovery.

Federal or Territorial Statute

A Bill that has passed in the Yukon Legislative Assembly or Parliament of Canada, and is thereby enacted, becoming an Act (statute) or law.

First Nations Settlement Lands Data and Information

Data and information which has been collected from or linked to First Nations settlement lands in Yukon and for which the agency or organization holding and managing the data does not possess appropriate permissions to facilitate unrestricted sharing and distribution. This does not include data collected remotely, where no land access was required (e.g. remote sensing, remote observation).

Non-sensitive Ecological Data

All ecological data and information that is otherwise not designated as **Sensitive Ecological Data**.

Private Land Data and Information

Data and information which has been collected from private lands and for which the Fish and Wildlife Branch does not possess appropriate permissions to facilitate unrestricted sharing and distribution. This does not include data collected remotely, where no land access was required (e.g. remote sensing, remote observation).

Proprietary Data and Information

Data and information for which the Fish and Wildlife Branch does not possess appropriate rights or permissions to facilitate unrestricted sharing and distribution. This includes data and information owned by Yukon First Nations and the Inuvialuit and includes, but is not limited to, Traditional Knowledge.

Restricted Access

Designates the limitations placed on the distribution and sharing of various types of **Sensitive Ecological Data** and other data and information that the Fish and Wildlife Branch may hold and manage.

Sensitive Ecological Data

Data and information that:

- pertain to **Elements Susceptible to Harm** and, if inappropriately released, could significantly increase the risk of harm to such **Elements**, their habitats, or the environment, or interfere with their conservation or recovery; or
- are **Proprietary**, relevant to **Private Lands** or to **First Nations Settlement Lands**, and have associated restrictions on their release; or
- if inappropriately released, would unduly harm **Program Relations**; or
- if inappropriately released, could cause an unacceptable risk to **Government Programs** and activities; or

- if released, would be in violation of the *Access to Information and Protection of Privacy Act*.

Governing Principles

1. Our data and information should be maintained within well-managed, secure data systems that adhere to best practices.
2. Conservation and management of [Elements](#) is best served by providing “decision makers” access to best available data and information (including spatial data and information).
3. In the spirit of openness and accountability, public bodies should make a deliberate effort to make their information easily accessible outside of the formal *Access to Information and Protection of Privacy Act* process.
4. Access to [Sensitive Ecological Data](#) will not be granted where the risk of disclosure outweighs the risk of non-disclosure, which is dependent on the category under which the data are labelled as sensitive ecological data. In other words, data should be widely available unless a strong, rational argument for limiting access is made. Such rationale should be transparent, well documented and align with the *Access to Information and Protection of Privacy Act* requirements.
5. If access to data and information is restricted, the Fish and Wildlife Branch has a responsibility to communicate what data are involved, why access is limited, and spatially, as explicitly as possible without compromising the data, what broad geographic area those data are pertinent to.
6. The authority to limit access to data should be identified publicly.
7. Entities with a [Business Case](#) should be provided access to [Restricted Access](#) data and information, with appropriate data management provisions in place (e.g., [Confidentiality and Non-disclosure Agreements](#), [Data Sharing Agreements](#)).
8. The Fish and Wildlife Branch should use a common approach to [Data Security](#) when sharing data and information.
9. Data and information that are widely available should be so at as fine a resolution or scale as possible. The Fish and Wildlife Branch has a responsibility to transparently communicate that scale to [Clients](#).

10. The Fish and Wildlife Branch should only release data and information where they have appropriate authority to do so.
11. The Fish and Wildlife Branch should only accept and store data where the ability to share is clearly articulated in writing by the party(ies) providing the data, unless that data has been accepted in confidence following ATIPP Regulation procedures.

Policy Statements

1. It is the policy of the Fish and Wildlife Branch to accept and manage data and information only when it has been collected consistent with relevant Federal and/or Territorial statutes and regulations.
2. It is the policy of the Fish and Wildlife Branch to make data and information as freely and openly available as possible, in the spirit of openness and accountability.
3. It is the policy of the Fish and Wildlife Branch to have a Data Security Committee designate data and information as [Restricted Access](#) if and only if they meet one or more of the following criteria to identify them as [Sensitive Ecological Data](#):
 - a. The data and information have been identified to pertain to [Elements Susceptible to Harm](#).
 - b. The data and information are [Proprietary](#) , relevant to [Private Lands](#) or relevant to [First Nations Settlement Lands](#) and have associated limitations on their re-distribution.
 - c. Release of the data and information would unduly harm [Program Relations](#) of the Fish and Wildlife Branch, Environment Yukon or Yukon Government.
 - d. Release of the data and information would unduly harm [Government Programs](#).
 - e. Release of the data and information would be in violation of relevant Legislation or Regulation.
4. It is the policy of the Fish and Wildlife Branch to routinely provide access to [Sensitive Ecological Data](#) where the [Client](#) has demonstrated an appropriate [Business Case](#) and where the Fish and Wildlife Branch has the relevant authorities to distribute those data.
5. It is the policy of the Fish and Wildlife Branch to provide access to [Sensitive Ecological Data](#) subject to relevant guidelines, restrictions, and agreements as necessary to maintain the integrity of those data (e.g., [Confidentiality and Non-Disclosure Agreements](#), [Data Sharing Agreements](#), Training Requirements).

6. Implementation of this policy is guided by relevant procedures for:
 - a. Data and Information Acceptance and Management.
 - b. Identification of [Sensitive Ecological Data](#).
 - c. Data and Information Distribution.
 - d. Administration and Documentation.
7. It is the policy of the Fish and Wildlife Branch to make its Data Sharing Policy and associated procedures publicly available.

Procedures

The following is a list of procedures that provide guidance for policy implementation in four broad categories.

Data and Information Acceptance and Management

[Criteria for Acceptance of Data and Information](#)

[Accepting Data in Confidence](#)

[Marking Restrictions in Data Systems](#)

Identifying Sensitive Ecological Data

[Identifying Elements Susceptible to Harm](#)

[Identifying and Managing Proprietary Data and Information](#)

[Identifying Data and Information Whose Release May Adversely Affect Government Programs](#)

[Identifying Data and Information Whose Release May Adversely Affect Program Relations](#)

[Identifying Data and Information Subject to Restrictions under Relevant Legislation and Regulations](#)

Data Distribution

[Responding to Direct Data Requests \(General\)](#)

[Responding to Direct Requests for Sensitive Ecological Data](#)

[Confidentiality and Non-disclosure Agreements and Data Sharing Agreements](#)

[Displaying Sensitive Ecological Data](#)

Administration

[Administration and Documentation](#)

Data and Information Acceptance and Management

Procedure: Criteria for Acceptance of Data and Information

Purpose:

This procedure outlines steps required to ensure that data and information received by the Fish and Wildlife Branch have been legitimately acquired and to determine whether those data are at all encumbered.

Procedural Steps:

1. At the time of submission, the Fish and Wildlife Branch will assess, through examination of the data and possible follow-up communications with the data submitter, that:
 - a. Any necessary permits were in place to gather the data. It will be assumed that individuals or organizations providing data as part of a licence requirement have obtained the necessary permits to collect such data.
 - b. The data submitter owns the copyright of the data and information (or is acting as an agent for the owner of the copyright) or the data and information are provided under open data license.
 - c. The collection and collation of the data did not violate any relevant statutes or the provisions of Yukon's modern treaties.

- d. The data submitter explicitly acknowledges that landowner permission exists to submit data collected from private lands where access to those lands was required to gather the data. This includes First Nation settlement lands.
2. The Fish and Wildlife Branch may, at its discretion, request a review of the data submitter's relevant permits and permissions.
3. The Fish and Wildlife Branch may request that a data submitter provides written details regarding the Branch's use and authority to disclose such information and data.
4. The Fish and Wildlife Branch may refuse receipt of data where it cannot be determined whether the data were acquired legitimately or where sharing restrictions on data could contravene the ATIPP Act.
5. The Fish and Wildlife Branch will use risk assessment approaches to determine whether any data and information currently in their holdings require review of appropriate permissions.

Procedure: Accepting Data in Confidence

Purpose:

This procedure outlines steps required to accept data in confidence from another government or individual or to accept a trade secret or the commercial, financial, scientific or technical information of a third party in confidence, as outlined in the [ATIPP Regulation](#).

Procedural Steps:

1. The government, third party, or individual providing the information must first identify the information that it wants the Government of Yukon to accept in confidence. In the case of an individual, they must also indicate if they want their identity to remain confidential.
2. The Deputy Minister of Environment (the head of the public body) must determine whether to accept the information in confidence, taking into consideration the reasons why access to the information should be restricted and whether the information would be provided if it were not accepted in confidence.

3. A receipt must be written that confirms that the Government of Yukon accepts the information in confidence and specifies the following:
 - a. The name of the government, third party or individual providing the data or information;
 - b. The types of information that is being provided;
 - c. the program that is accepting the information;
 - d. the name and position of the employee who is responsible for the program that is accepting the information;
 - e. in the case of a third party, if the information was required to be provided under an enactment, set out the provision of the enactment under which it was provided;
 - f. the reasons for agreeing to accept the information in confidence, including whether the information would have been provided if it were not accepted in confidence and the reasons why the Government of Yukon considers that access to the information should be restricted
4. The receipt must be signed by the Deputy Minister of Environment, as the head of the public body, or by the employee responsible for the program that is accepting the information.
5. The signed receipt must be provided to the government, third party or individual that provided the information.
6. A copy of the receipt must be retained for as long as the information is held in confidence and for one year afterwards.
7. The information accepted in confidence must be identified as having been accepted in confidence in whatever data system it is stored.

Procedure: Marking Restrictions in Data Systems

Purpose:

This procedure outlines steps required to ensure that any use restrictions, whether imposed by a data submitter on the subsequent use and/or distribution of submitted data or imposed by the Fish and Wildlife Branch on data in its holdings, are recorded in the relevant data systems.

These restrictions may be permanent (e.g., they are never removed) or temporary (time-limited), limit the spatial precision at which data can be displayed or redistributed, and/or access may be limited to specified personnel.

Procedural Steps:

1. The Fish and Wildlife Branch will ensure that when data submitters request restrictions on the distribution of submitted data and information that the following are recorded in the relevant data system:
 - a. Existence of a restriction on distribution.
 - b. Type of restriction (permanent, temporal, spatial precision, specified personnel).
 - c. Time limit for restriction.
 - d. Rationale for restriction.
 - e. Relevant contact information.

It is up to the individual Program areas of the Fish and Wildlife Branch to decide whether to accept encumbered data.

2. The Fish and Wildlife Branch will ensure that data identified as [Sensitive Ecological Data](#) by the [Data Security Committee](#) (see also procedures related to identifying sensitive ecological data) are marked in the relevant data system with:
 - a. Existence of a restriction on distribution.
 - b. Category under which it has been identified as [Sensitive Ecological Data](#).

Identifying Sensitive Ecological Data

Procedure: Identifying Elements Susceptible to Harm

Purpose:

This procedure outlines steps required to determine whether an [Element](#) warrants the [Element Susceptible to Harm](#) designation due to the risk that unrestricted sharing of data may result in intentional or inadvertent harm to populations, residences, or occurrences, or interfere with their conservation or recovery.

Procedural Steps:

1. The Fish and Wildlife Branch will establish a [Data Security Committee](#) responsible for reviewing proposed inclusions to or removals from the list of [Elements Susceptible to Harm](#).

2. Staff of the Department of Environment can nominate [Elements](#) as [Elements Susceptible to Harm](#) by contacting the [Data Security Committee](#) members.
3. The list of [Elements Susceptible to Harm](#) will be reviewed every 3 years.
4. An emergency evaluation for inclusion to the list prior to a scheduled review date can be requested by contacting the [Data Security Committee](#) members.
5. The [Data Security Committee](#) will review risk to persistence and/or recovery of the [Elements](#) by evaluating the following criteria:
 - A. [Element](#) status (global, national and subnational status ranks (G, N and S ranks), COSEWIC Status, SARA listing, CITES Appendix, IUCN status) and any relevant information that might indicate changes to abundance, trends, and threats since the most recent status evaluation.
 - B. Evidence and nature of threats, potential impacts of the threats, and potential mitigating factors for the following categories of threats **associated with making locational data and information publicly available**:
 - i. Existing legal capture or harvest of individuals.
 - ii. Existing illegal collection, persecution, or harassment.
 - iii. Existence of legal or illegal captive breeding or propagation.
 - iv. Existence of legal or illegal markets for the species.
 - v. Disturbance or displacement (temporary or permanent).
 - C. Risks associated with not disclosing locational data (e.g., inadvertent destruction of [Element](#) or associated habitat, preventing prosecution, restricting ability to develop conservation plans).
 - D. Existing protection associated with:
 - i. Relevant Territorial legislation (e.g. [Wildlife Act](#), [Animal Health Act](#), [Yukon Territory Fishery Regulation](#))
 - ii. Federal legislation (e.g. [Species At Risk Act \(SARA\)](#), [Migratory Bird Convention Act](#), [WAPPRIITA](#) -Wild Animal and Plant Protection and Regulation of International and Interprovincial Trade Act, [Fisheries Act](#))
 - iii. Land use regulatory authorizations currently in effect (e.g. land use permits, mineral exploration/development licenses) containing terms/conditions prescribing protection measures for elements.
 - E. Relevant references.

6. The [Data Security Committee](#) will provide recommendations and rationale for inclusions to and deletions from the list of [Elements Susceptible to Harm](#) to the [Data Owner](#) for approval.
7. The Fish and Wildlife Branch will publish the list of [Elements Susceptible to Harm](#).

Procedure: Identifying and Managing Proprietary Data and Information

Purpose:

This procedure outlines steps required to ensure that any restrictions associated with [Proprietary Data and Information](#) are labelled upon receipt of the data and information in the relevant data system and are managed appropriately. This procedure refers to restrictions imposed by the owner of the data and information (the entity owning the data and/or holding Intellectual Property Rights), the land owner on whose property the data was collected ([Private Land Data and Information](#)), or the First Nation on whose settlement lands the data were collected ([First Nations Settlement Lands Data and Information](#)).

It is up to the individual Program areas of the Fish and Wildlife Branch to decide whether to accept encumbered data. Acceptance of proprietary data with encumbrances is discouraged in most cases, with some exceptions, as this data is limited in value due to the encumbrances and require more resources to manage effectively.

If such data is accepted, the following procedural steps should be followed.

Procedural Steps:

1. The Fish and Wildlife Branch will inform the data owner, at the time of data submission, of the branch's obligations under the ATIPP Act regarding Third Party data. If the data owner does not wish to have their data released under those conditions, a formal procedure for accepting data in confidence, as outlined in the ATIPP Regulation, may be considered (see [Procedure: Accepting Data in Confidence](#)).
2. The Fish and Wildlife Branch will ensure that when data are received that are collected from private lands or First Nations settlement lands that the data have

been collected in adherence with relevant permissions (see [Procedure: Criteria for Acceptance of Data and Information](#)).

3. The Fish and Wildlife Branch will ensure that the restrictions are recorded in the data entry system, following the procedures for [Marking Restrictions in Data Systems](#).
4. If the Fish and Wildlife Branch has ownership and/or Intellectual Property Rights of data collected from private lands, there can be no restrictions placed on its distribution under this category.
5. Where associated restrictions allow some form of distribution, the Fish and Wildlife Branch will strive to enter into a formal [Data Sharing Agreement](#) with the data owner to formalize terms for that distribution (see [Procedure: Confidentiality and Non-disclosure Agreements and Data Sharing Agreements](#)). The data and information will be managed according to the terms set out in the Data Sharing Agreement.
6. Where associated restrictions have a defined time limit, at the end of that timeframe, the Fish and Wildlife Branch will remove the associated restrictions and the data will be managed as per all other relevant policies and procedures.
7. Once data and information have been made public (i.e., distribution restrictions have been removed) then these restrictions cannot be re-instated retroactively.

Procedure: Identifying Data and Information Whose Release May Adversely Affect Government Programs

Purpose:

This procedure outlines steps required to identify data and information whose distribution may cause unacceptable risk to government mandates, programs and activities.

The standards by which data and information are restricted for these purposes will be governed by strict adherence to criteria that demonstrate substantive risk to government programs. In this procedure, the risk to the interests of government programs must be considered to outweigh the risk of not making the data and information available. One such example of sensitive data that could present an unacceptable risk to government programs if it were shared is locations of concentrated animals which are harvestable; if the data was shared, it could result in

harvest related mortality of wildlife beyond sustainable harvest limits, which could undermine the Department's ability to manage a sustainable harvest per our shared management responsibilities with indigenous governments and other stakeholders. Data should be widely available unless a strong, rational argument for limiting access can be made. Such rationale should be transparent and well documented.

Procedural Steps:

1. The Fish and Wildlife Branch will establish a [Data Security Committee](#) responsible for reviewing proposed inclusions to or removals from the list of [Elements](#) associated with this procedure due to the risk posed to government mandates, programs and activities by distributing all or some data and information for those [Elements](#).
2. Relevant staff of the Department of Environment can nominate [Elements](#) or subsets of data for consideration under the [Data and Information Whose Release May Adversely Affect Government Programs](#) Category by contacting the Data Security Committee members.
3. The list of Elements or subsets of such data that fall in this category will be reviewed every 3 years.
4. An emergency evaluation for inclusion to the list prior to a scheduled review date can be requested by contacting the [Data Security Committee](#) members.
5. The [Data Security Committee](#) will review risk to Elements or subsets of data for [Elements](#) for consideration under the [Data and Information Whose Release May Adversely Affect Government Programs](#) Category by evaluating demonstrated or perceived risk to government mandates, programs and activities (e.g., legal investigations, wildlife harvest management programs, delivery of joint conservation/protection programs for elements with shared or agreed to terms with indigenous governments).
6. The [Data Security Committee](#) will consider whether data restrictions need to be permanent or have a defined time limit.
7. The [Data Security Committee](#) will provide recommendations and rationale for inclusions to and removals from the list of [Elements](#) or subsets of data for consideration under the [Data and Information Whose Release May Adversely Affect Government Programs](#) Category to the [Data Owner](#) for approval.
8. The Fish and Wildlife Branch will publish the list of [Elements](#) or subsets of data for which datasets have been deemed [Sensitive Ecological Data](#) under the [Data](#)

[and Information Whose Release May Adversely Affect Government Programs](#)
Category.

Procedure: Identifying Data and Information Whose Release May Adversely Affect Program Relations

Purpose:

This procedure outlines steps required to identify data and information whose distribution may cause unacceptable risk to program relations of the Fish and Wildlife Branch, Department of Environment and Government of Yukon in general.

The standards by which data and information are restricted for these purposes will be governed by strict adherence to criteria that demonstrate substantive risk to program relations. In this procedure, the risk to the interests of program relations must be considered to outweigh the risk of not making the data and information available. Data should be widely available unless a strong, rational argument for limiting access can be made. Such rationale should be transparent and well documented.

Procedural Steps:

1. The Fish and Wildlife Branch will establish a [Data Security Committee](#) responsible for reviewing proposed inclusions to or removals from the list of data to be restricted due to the risk posed to program relations by distributing all or some such data.
2. The Fish and Wildlife Branch will provide avenues for relevant staff to put forth data for consideration under the [Data and Information Whose Release May Adversely Affect Program Relations](#) Category.
3. The list of data to be restricted under this category will be reviewed every 3 years.
4. The [Data Security Committee](#) will review risk by evaluating demonstrated or perceived risk to Fish and Wildlife Branch mandate and relations (e.g., government to government relations and agreements, government to non-government relations).
5. The [Data Security Committee](#) will consider whether data restrictions need to be permanent or have a defined time limit.

6. The [Data Security Committee](#) will provide recommendations and rationale for inclusions to and removals from the list of data for consideration under the [Data and Information Whose Release May Adversely Affect Program Relations](#) Category to the Data Owner for approval.
7. The Fish and Wildlife Branch may, at their discretion, choose to consult with the relevant affected parties in the relationship.
8. The Fish and Wildlife Branch will publish the list of datasets that have been considered [Sensitive Ecological Data](#) under the [Data and Information Whose Release May Adversely Affect Program Relations](#) Category.

Procedure: Identifying Data and Information Subject to Restrictions Under Relevant Legislation and Regulations

Purpose:

This procedure outlines steps required to identify data and information whose distribution may be in contravention of established statutes, legislation and/or regulations.

Procedural Steps:

1. The Fish and Wildlife Branch will be bound by relevant [Federal and Territorial statutes](#) and will label and restrict access to all data whose distribution would violate such statutes (e.g. ATIPP).
2. Data and information considered [Sensitive Ecological Data](#) under this category will only be released by the relevant statutory authority.

Data Distribution

Procedure: Responding to Direct Data Requests (General)

Purpose:

This procedure outlines general procedures for providing effective and timely responses to requests for data and information made directly to the Fish and Wildlife Branch. Note that this procedure does not cover formal ATIPP requests, which have their own procedures established by the ATIPP office.

Procedural steps:

1. The Fish and Wildlife Branch will make available contact information that can be used to request data and information from the various Program Areas within the Branch.
2. The Fish and Wildlife Branch will routinely receive, review and respond to [Client](#) requests for access to data and information.
3. The Fish and Wildlife Branch will assess each data request received to determine if any of the data requested has been labelled as [Restricted Access](#) according to this policy. If there are such encumbrances, the [procedure for responding to data requests for Sensitive Ecological Data](#) will be followed. If there are no encumbrances, the procedure for responding to general Data Requests (this procedure) will be followed.
4. The Fish and Wildlife Branch will inform the [Client](#) of service standards for data request response times and, if necessary, negotiate a reasonable deadline with the [Client](#).
5. The Fish and Wildlife Branch may contact the [Client](#) for clarifications on their request, if necessary.
6. The Fish and Wildlife Branch will prepare the data for release and may prepare a [Data Sharing Agreement](#) where deemed necessary by the Program Area that manages the data, to be signed by the appropriate signing authorities for both the [Client](#) and Fish and Wildlife Branch.
7. Once the [Data Sharing Agreement](#), if applicable, is signed by both parties the data will be released by the Fish and Wildlife Branch.

Procedure: Responding to Direct Data Requests for Sensitive Ecological Data

Purpose:

This procedure outlines steps required to provide effective and timely responses to [Client](#) requests for access to [Sensitive Ecological Data](#) made directly to the Fish and Wildlife Branch. This includes data and information in the following categories:

- Data and Information for [Elements Susceptible to Harm](#)

- [Proprietary Data and Information](#) (including [Private Land](#) and [First Nations Settlement Lands](#) data and information)
- [Data Relevant to Government Programs](#)
- [Data Relevant to Managing Program Relations](#)
- Data whose distribution is prohibited by ATIPP

Note that this procedure does not cover formal ATIPP requests, which have their own procedures established by the ATIPP office.

Procedural steps:

If a data request is for data that falls in one of the above categories and is therefore deemed to have [Restricted Access](#), the following steps will be followed:

1. The Fish and Wildlife Branch will initiate contact with the [Client](#), letting them know that some or all of their request involves restricted access data, identifying which category it falls in, and requesting that they provide rationale for needing the data (if not sufficiently provided in the initial request for data).
2. The Fish and Wildlife Branch will determine the scope of data requirements to assess whether the needs of the [Client](#) can be met by limiting the geographic and/or taxonomic scope of data provided, thereby potentially, but not necessarily, eliminating the need for Sensitive Ecological Data. They will discuss these options with the Client.
3. If the [Client](#) still wishes to pursue their request for [Sensitive Ecological Data](#), the Fish and Wildlife Branch will determine the Client's [Business Case](#) using the following criteria:
 - a. The Client has a **legal, regulatory, or policy requirement** to consider [Sensitive Ecological Data](#) within their business activities and/or,
 - b. The Client is a licensee on a project where their authorization requires them to comply with certain terms/conditions to protect and/or mitigate effects to an element(s) occurring within their project area, and the information is needed to support their own compliance and any compliance/enforcement related inspections by officers,
 - c. The Client has an established **management responsibility** for the [Element](#) included in the request for [Sensitive Ecological Data](#) and/or,
 - d. The Client's activities will **further conservation** of the [Element](#) included in the request for [Sensitive Ecological Data](#) and/or,

- e. The Client's use of the data requested will **improve knowledge** for the [Element](#) included in the request for [Sensitive Ecological Data](#) and/or,
 - f. The Client is a member or representative of an organization, agency or business that has a **vested interest** (ownership, proposed activity, management responsibility) **in a project or property where activities may have effects on** the [Element](#) included in the request for [Sensitive Ecological Data](#) and/or,
 - g. The Client has a **mandate** specific to the [Element](#) included in the request for [Sensitive Ecological Data](#) (e.g., develop status assessments, management plans, recovery strategies) and/or,
 - h. The Client requires the data for the [Element](#) included in the request for [Sensitive Ecological Data](#) **to make recommendations regarding the management of specified lands or waters** and/or,
 - i. The data for the [Element](#) included in the request for [Sensitive Ecological Data](#) are **required by legislation or are required for legal enforcement purposes**.
4. The Fish and Wildlife Branch will weigh the perceived benefits of providing the [Sensitive Ecological Data](#) to the [Client](#) against the potential risks to the security of the data. In the absence of legitimate reasons to the contrary, [Sensitive Ecological Data](#) will be provided to [Clients](#) with legitimate requests.
 5. If the [Client](#) is unable to establish a [Business Case](#), the [Sensitive Ecological Data](#) requested will not be provided. The Fish and Wildlife Branch will communicate that decision, along with a written rationale for the decision, to the Client in a timely manner, ideally within 30 days.
 6. [Clients](#) whose requests are denied will be able to appeal the decision to the [Data Owner](#), the Director of the Fish and Wildlife Branch. The appeal process will be published so that [Clients](#) are aware of it.
 7. Results of decisions regarding requests for [Sensitive Ecological Data](#) will be communicated to relevant staff within the Fish and Wildlife Branch.
 8. The Fish and Wildlife Branch will maintain a log specific to data requests for [Sensitive Ecological Data](#) where details on the decision (to provide or deny) is recorded. This log will include the following:
 - a. Date of request
 - b. Client name and contact information¹
 - c. Entity the Client is representing (if the Client is not a member of that organization)

- d. [Sensitive Ecological Data](#) requested
 - e. Program area(s) involved
 - f. Decision (provide or deny)
 - g. Date of decision
 - h. Reasons for denying the request (if applicable)
9. If the decision is made to provide the [Sensitive Ecological Data](#), the Fish and Wildlife Branch will prepare the data for release, request from the [Client](#) that they sign a [Confidentiality and Non-disclosure Agreement](#) (CNDA), and draft a [Data Sharing Agreement](#) (where necessary) to be signed by the appropriate signing authority. The Data Sharing Agreement may place a time limit or other limited use restrictions on the use of the [Sensitive Ecological Data](#) by a [Client](#) and may require the eventual destruction of the [Client's](#) copy of said [Sensitive Ecological Data](#).
10. When the [Confidentiality and Non-disclosure Agreement](#) (CNDA) and [Data Sharing Agreement](#) (if relevant) are signed by all parties, the Fish and Wildlife Branch will release the data to the [Client](#) ensuring their communication:
- a. informs the [Client](#) that the data is subject to the signed CNDA;
 - b. includes any necessary guidance regarding limitations of use and interpretation of the data;
 - c. includes any restrictions and/or guidance regarding subsequent use and display of [Sensitive Ecological Data](#) in the [Client's](#) documents, reports and maps.

¹Collecting this information will require a Privacy Impact Assessment

Emergency release of Sensitive Ecological Data

11. The Fish and Wildlife Branch may, in an emergency and under the relevant designated authority, release [Sensitive Ecological Data](#) where not releasing the data would further jeopardize the relevant [Elements](#) or other considerations that led to their designation of [Restricted Access](#) data.
12. In the case of emergency release, the Fish and Wildlife Branch will only release [Sensitive Ecological Data](#) to those personnel who have an immediate need-to-know.
13. In the case of emergency release, the Fish and Wildlife Branch will retroactively ensure that personnel with whom [Sensitive Ecological Data](#) were shared enter

into [Confidentiality and Non-disclosure Agreements](#) and [Data Sharing Agreements](#).

Procedure: Confidentiality and Non-disclosure Agreements and Data Sharing Agreements

Purpose:

This procedure outlines the use of [Confidentiality and Non-disclosure Agreements](#) and [Data Sharing Agreements](#) by the Fish and Wildlife Branch.

Our [Confidentiality and Non-disclosure Agreements](#) prescribe the terms of [Client](#) access, constraints to the use of and redistribution of [Sensitive Ecological Data](#).

[Data Sharing Agreements](#) are used to establish formal data sharing arrangements between the Fish and Wildlife Branch and a [Client](#). Our [Data Sharing Agreements](#) formally detail the interests of both the Fish and Wildlife Branch (or a program within) and a [Client](#) in sharing and using data and information, including any restrictions or guidance on use, distribution or attribution.

Procedural steps:

Confidentiality and Non-disclosure Agreements

1. The Fish and Wildlife Branch will publicize the requirement for [Clients](#) to enter into [Confidentiality and Non-disclosure Agreements](#) prior to receiving access to [Sensitive Ecological Data](#).
2. The Confidentiality and Non-disclosure Agreement is available on Yukon.ca.
3. The Fish and Wildlife Branch may institute time limits associated with signed [Confidentiality and Non-disclosure Agreements](#).
4. The Fish and Wildlife Branch will publish any other [Client](#) requirements related to entering into [Confidentiality and Non-disclosure Agreements](#) (e.g., Training Requirements, Data Licenses) on relevant platforms and portals.
5. The Fish and Wildlife Branch will maintain records that document [Confidentiality and Non-disclosure Agreements](#) (including recipient name, contact information and date of signature).

Data Sharing Agreements

1. The Fish and Wildlife Branch may use [Data Sharing Agreements](#) to facilitate access to [Sensitive Ecological Data](#). [Data Sharing Agreements](#) may also be used for the sharing of [Non-sensitive Ecological Data](#), where deemed appropriate by the Program area that manages the data.
2. The Fish and Wildlife Branch may institute time limits associated with signed [Data Sharing Agreements](#).
3. The Fish and Wildlife Branch will publish template [Data Sharing Agreements](#) on relevant platforms and portals.
4. The Fish and Wildlife Branch will publish any other [Client](#) requirements related to entering into [Data Sharing Agreements](#) (e.g., Training Requirements, [Confidentiality and Non-disclosure Agreements](#)) on relevant platforms and portals.
5. The Fish and Wildlife Branch will maintain records that document established [Data Sharing Agreements](#).

Procedure: Displaying Sensitive Ecological Data

Purpose:

This procedure outlines steps to be taken to make known the presence of [Sensitive Ecological Data](#) within the Fish and Wildlife Branch's data holdings and to facilitate steps the Fish and Wildlife Branch may take to provide a generalized product for data that is otherwise classified as [Sensitive Ecological Data](#).

Procedural steps:

1. The Fish and Wildlife Branch will select a means of making known the presence of [Sensitive Ecological Data](#) consistent with their data distribution service (e.g., data portals, on-line map-based services).
2. When receiving direct requests for data, the Fish and Wildlife Branch will develop and utilize a standard response to [Clients](#) to inform them of the presence of [Sensitive Ecological Data](#) within their area of interest.
3. When utilizing web-based portals and/or data services, the Fish and Wildlife Branch will spatially obfuscate location data (e.g., fuzzing) and/or withhold taxonomic identifiers for [Sensitive Ecological Data](#). The Fish and Wildlife Branch

may choose, as necessary, to withhold additional data attributes to maintain the security and integrity of the [Sensitive Ecological Data](#).

4. The Fish and Wildlife Branch will obfuscate [Sensitive Ecological Data](#) at a scale that is as close as possible to the scale used for [Non-Sensitive Ecological Data](#) without compromising the security and integrity of the [Sensitive Ecological Data](#).
5. The Fish and Wildlife Branch will choose to display taxonomic identifiers for spatially obfuscated/generalized [Sensitive Ecological Data](#) unless doing so would irreparably harm the security and integrity of the [Sensitive Ecological Data](#). Where taxonomic identifiers may need to be withheld, the Fish and Wildlife Branch will strive to provide taxonomic identifiers for obfuscated [Sensitive Ecological Data](#) at a level of detail that is as close as possible to the level of detail used for [Non-Sensitive Ecological Data](#).
6. The Fish and Wildlife Branch may develop [Sensitive Ecological Data](#) products that could be displayed and routinely distributed as [Non-Sensitive Ecological Data](#) by spatially obfuscating [Sensitive Ecological Data](#) to a scale whose routine distribution would not interfere with the security and integrity of the [Sensitive Ecological Data](#).
7. The Fish and Wildlife Branch may provide the de-sensitized product as an integral component of their standard suite of data offerings through relevant data portals, platforms, or other data services.
8. The Fish and Wildlife Branch will clearly communicate to [Clients](#) where data has been generalized or otherwise obfuscated on data portals or through relevant data services.

Administration

Procedure: Administration and Documentation

Purpose:

This procedure outlines the administrative steps required under this policy.

Procedural Steps:

1. The Fish and Wildlife Branch will publish the position of their designated Data Authority ([Data Owner](#)) and relevant contact information for the different program areas that can be contacted for requests for data on relevant data

portals, data platforms, web sites, and within relevant meta-data for data systems.

2. The Fish and Wildlife Branch will maintain searchable electronic records that at a minimum document:
 - a. Establishment of [Confidentiality and Non-disclosure Agreements](#) and [Data Sharing Agreements](#) or other such instruments and any relevant expiry dates.
 - b. Provision of [Sensitive Ecological Data](#) to [Clients](#) (See [Procedure: Responding to Requests for Sensitive Ecological Data](#)).
 - c. Denial of provision of [Sensitive Ecological Data](#) to [Clients](#).
 - d. Metadata for (a-c) including names, dates, restrictions, and any other relevant details.
3. The Fish and Wildlife Branch will ensure that their approved operational Data Sharing Policy and enabling Procedures are made publicly available by publishing them on relevant data portals, data platforms and web sites.

Appendix A: Confidentiality and Non- disclosure Agreement

The Access to Information and Protection of Privacy Act (the Act) provides for the disclosure of information about species and ecosystems except where such disclosure could reasonably be expected to result in damage to, or interference with, the conservation of the species or ecosystem as per section 78 of the Act. It also provides for refusal to disclose information that could be harmful to relationships with other governments or to third party business interests or to personal privacy as per sections 76, 77 and 70 of the Act respectively. This form is an appendix to the Fish and Wildlife Branch Data Sharing Policy.

Access the form on Yukon.ca.