NatureServe Canada Data Security Template Policy and Procedures Implementation Guidance

The intent of this document is to provide guidance to agencies and organizations who are considering, or are in the process of, adopting and adapting the NatureServe Canada Data Security Policy and Procedures templates. It will be updated and added to as deemed useful and necessary. It consists of some general guidance and a series of responses to questions that have arisen during the adoption of these templates by various agencies and organizations.

Guidance for Adoption and Implementation

1. Understand your agency's/organization's existing legal, regulatory and policy framework, including those relevant to Open Data/Open Information and Freedom of Information/Protection of Privacy. Familiarity with these will help prevent any issues that might arise as you work to adopt these templates.

2. Familiarize yourself and your team with the Introductory document and the policy and procedure templates (see https://www.natureserve.org/canada/biodiversity-data/data-security-policy-and-procedures). In particular, be familiar and comfortable with the principles upon which the policy is based. These principles, endorsed by the Canadian Wildlife Directors Committee in 2022, are key to establishing a policy and associated procedures that are consistent with other agencies/organizations managing biodiversity data across Canada.

3. Determine the application scope of your new policy and procedures – is it for your local group, a broader sector within your agency/organization or for your entire agency/organization. This will inform the breadth of data and information pertinent to your policy and thus the scope of outreach and consultation necessary to facilitate successful adoption and implementation.

4. Map out the approval process for new/revised policy and procedures for your agency/organization and brief those individuals key to that process.

5. Communicate your project and intentions to colleagues, superiors, and others within your agency/organization whose work may be affected. Early and regular communication and outreach are key to acquiring approval and acceptance by approving authorities and colleagues.

6. It may be helpful in some cases to build a cross-reference table between existing data security terminology in your agency/organization and that of the templates. This will

be particularly useful if the terminology current in use in your agency/organization differs greatly from that in the template.

7. While developing your new policy and procedures, continually evaluate it against real data security situations your agency/organization has experienced. This "real world" testing can be a useful approach for refining the policy and procedures and training staff in how it is to be implemented.

Learnings from agencies/organizations who have worked to adopt these templates (or Frequently Asked Questions).

The following are responses to frequently asked questions from agencies/organizations who have adopted or are in the process of adopting the NatureServe Canada Data Security templates.

1. Does my agency/organization need to incorporate all components of these templates?

    When adopting these templates for your governing environment there are some components that are considered requisite for a comprehensive and effective data security policy and others that are considered optional. The policy is based upon a set of principles, approved by the Canadian Wildlife Directors Committee in 2022. All policy statements should be considered mandatory as part of an agency's/organization's comprehensive data security policy with one exception. Under policy statement 3, only the *Sensitive Ecological Data* categories of 3(a) *Species Susceptible to Harm* and 3(i) *Legislation and Regulation* are considered mandatory. The other categories within policy statement 3 are advisable should they have any relevance to the policy environment of your agency/organization. They reflect existing criteria in policy within various agencies and organizations across Canada that manage and distribute biodiversity data and information.

2. My agency/organization may be challenged in adopting the term "*Elements*". We are considering using "species and ecosystems" instead as they can understand those concepts.

    The NatureServe Data Security Working Group had as one of its primary tasks the development of a common terminology that could be used by agencies/organizations that manage and distribute biodiversity data across the country. The lack of a common terminology was identified as one of the key obstacles to improving data flow and reducing the restrictions on data and information. The term "Element", though perhaps novel to some, is common to all the Conservation Data Centres and Natural Heritage Information Centres that manage the bulk of data and information on species at risk across Canada. It is valuable in that it encompasses not only species, but refers to any element of biodiversity (species, subspecies, populations, ecosystems, and even special features). As such it is a much broader umbrella term and agencies/organizations adopting these templates are strongly advised to use it and the other terminology provided within.

3. My agency/organization feels that it needs to add some terms to the list of terms and definitions within the template policy. Is this acceptable?

    If there are key terms used within your agency/organization's policy and procedure framework that this policy needs to cross-reference, then the addition of those to the list of terms and definitions within the policy template is acceptable. However, it is not advisable to substitute these for existing terms in the template as this will further prolong the issues the template has been developed to resolve. Rather, they should be utilized as additions that assist with connections to your agency/organization's current policy environment.

4. Throughout the policy document the expression “data and information” is common. Is there a reason for using both words? Can we simplify this to data?

   The use of the expression “data and information” is intentional. It recognizes that agencies/organizations that manage biodiversity information may have and distribute a variety of products. One of these might be raw data (e.g., observations) while others may be more synthetic in nature (e.g., results of analyses, source features, element occurrences, range maps). Intellectual property provisions may differ for these. This expression is intended to capture that diversity.

5. How should an agency/organization receiving data and information assess whether “the collection and collation of the data did not violate any relevant statutes”?

   It is advised that agencies/organizations that receive biodiversity data and information demonstrate their due diligence in this matter in two fashions:

   a) In the case of direct data submissions to the agency/organizations by individuals, companies, other agencies, or institutions the receiving agency/organization should require that the data submitter acknowledge that the data and information were gathered legally and that no relevant statutes (e.g., trespass on private property) were violated. If permits were required (e.g., permits to capture wildlife) to gather data the donor body should confirm that such permits were in place. Thus, the onus is placed on the data provider.
   b) In the case of the agency/organizations mining data from other recognized bodies (e.g., GBIF, iNaturalist), the agency/organization should do its due diligence to ascertain those data have similar mechanisms in place to evaluate this factor, or it should explicitly state within its policy that is “*assumes*” that reputable bodies that amass such data and information have extant policy that adequately address this factor. It will be up to the agency/organization to decide on the level they want to risk manage this.

   This policy statement and associated procedure is not intended to be a burden to the agency/organization. Rather, it is intended to communicate to its partners that it has a responsibility to do its due diligence in this matter and that it is achieved by putting the responsibility on the body submitting the data and/or information.

6. What is meant by point 4 in the procedure for Identifying and Managing Private Land Data and Information: *If the Agency/Organization 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.*

   If the agency/organization already has the IP required for data collected from private lands and the data were collected with appropriate permissions, then there is no rational to restrict access to these data under this category. This clause is intended to protect the agency/organization from subsequent landowners requesting to have data designated restricted access retroactively.

7. What is meant by Indigenous land data and information? How are indigenous lands defined?

   The answer to the first question is data and information that is obtained from indigenous lands. The answer to the second is more nuanced and will depend on the existing policies of the agency/organization regarding how indigenous lands are defined and recognized (e.g., Indian Reserves, Treaty Settlement Lands, Traditional Territories). Those agencies/organizations who embrace this criterion for identifying and labelling restricted data will need to clearly articulate a definition, either within their policy, or refer to existing agency/organization policy that already serves that purpose.

8. What is an example of a situation where release of data could cause an unacceptable risk to a government program or activities?

   An example might be release of data that could affect wildlife management programs (e.g., location data for hunted species that could greatly affect hunter success), and thus require further restrictions in hunter opportunities. Governments often have stated objectives of maintaining or increasing hunting opportunities. This is one instance where release of data might negatively affect those objectives. There may also be a valid argument that this could apply to non-government entities that need to be able to restrict access to data and information that might negatively affect any of their relevant programs. Another might be release of data and information that might be detrimental to ongoing investigations by environmental enforcement staff.

9. What is the difference between "data and information relevant to government programs" and "data and information relevant to maintaining program relations"?

   The language in these two clauses is intended to distinguish between internal programs of government (or other agencies/organizations managing biodiversity data) and external relations of the agency/organization managing biodiversity data and their partners and stakeholders.

10. Can the agency/organization releasing *Sensitive Ecological Data* limit the uses that their client intends for that data?

    Agencies/organizations will make decisions as to whether a client has a valid rationale to warrant access to *Sensitive Ecological Data* using the procedure: *Determining a Client's Business Case for Access to Sensitive Ecological Data.* Although the agency/organization may choose to communicate limitations to the intended uses of that data (e.g., relevant to the rationale for the business case), the agency/organization does not likely have the authority to limit the use.

11. The distinction between a guiding principle and a policy statement seems a bit vague. Some of the guiding principles could easily be considered policy statements. Can you explain?

    The guiding principles were developed by the NatureServe Canada Data Security Working Group to set the overall tone and expectations for Data Security Policy and were approved by the Canadian Wildlife Directors Committee in 2021. As such they often read like policy statements. The specific policy statements enable the guiding principles in a formal policy framework. An agency/organization may or may not choose to include guiding principles within their policy document. Operational policy statements based on those principles are mandatory and key to a comprehensive and effective policy.

12. I don't understand the procedure "Identifying Relevant Legislation and Regulations". Is this where I would spell out what ATIPP tells us we cannot share?

    Agencies/organizations have a duty to be knowledgeable about any limitations relevant legislation might place on their data sharing practices. This is typically where relevant FOIPPA or ATIPP legislation would be used to identify any data and information that could not be shared. There may be other legislation or regulations in some jurisdictions that are relevant to this.

13. Who should be able to provide suggestions to the Data Security Committee for elements to include in the list of *Elements Susceptible to Harm*?

    Nominations for elements to consider under this category of Sensitive Ecological Data should come from knowledgeable staff within the organization. The procedure was developed with this intent. It does not restrict an agency/organization from choosing to accept nominations from individuals outside of their organization. An external process will likely, however, require more time and resources to manage.

14. If data and information are received that have been collected from private lands, and the landowner has requested restrictions on their distribution, then can that data ever be distributed under this policy?

    The sharing or distribution of data and information considered Restricted Access due to the Private Lands criteria will be governed by any data agreements between the landowner and the agency/organization managing that data and information. There may be cases where these are never shared or only shared in specifically defined circumstances.

15. There is a statement in the procedure for release of Sensitive Ecological Data that states: The Agency/Organization may place a time limit or other limited use restrictions on the use of *Sensitive Ecological Data* by a *Client* and may require the eventual destruction of the *Client's* copy of said *Sensitive Ecological Data*. We have been told by ATIPP staff that we cannot request that a client destroy our data at a certain time?

    This is typically done to ensure that clients are returning to the agency/organization for the most recent data and information, rather than relying on dated versions. Any requirements imposed by the agency/organization on the client's use and eventual destruction of Sensitive Ecological Data will be subject to limitations imposed by relevant legislation (e.g., ATIPP). The ability of the agency/organization to do this will likely be jurisdiction specific.

16. In the procedure for release of Sensitive Ecological Data are several statements regarding Emergency release of data. What is this for?

This procedure is intended for cases where a client/agency/organization needs the information immediately and there is not sufficient time to conduct the normal steps (e.g., establishing a business case, drafting data release agreements and confidentiality agreements). An example might be an environmental emergency such as a wildfire where action is required immediately and site-specific knowledge of the location of important elements of biodiversity may be a necessary or useful asset to the agency responding to that emergency.

17. The procedure: *Criteria for Acceptance of Data and Information* uses the verb ensure in many places. What if my agency/organization is not able to ensure the various components in this procedure are adhered to.

    Remember that these are policy and associated procedures, not legislation. They outline the intent of the agency/organization and how they will achieve that. In this case there are steps that the agency can take to do their due diligence to ensure ….. Watering this statement down with phrases as "work to ensure" or "attempt to ensure" is not advised.