NATURESERVE CANADA
A Network Connecting Science with Conservation
Un Réseau pour la science et la conservation

Data and Information Security Policy Template
NatureServe Canada Data Security Working Group
February 22, 2022

Background

This policy template was developed so that it can be adopted by any government body (*Agency*) or non-government organization (*Organization*) that accepts, manages, or distributes data and information on species and ecosystems within Canada. Its purpose is to facilitate the development of consistency in data management and security amongst federal, provincial, territorial agencies, and NGO partners, to establish a common terminology, and to improve data sharing between agencies, organizations, and their *Client*s. The template policy and associated procedures have been developed to encompass, as best possible, the range of circumstances within which Canadian agencies/organizations currently manage and distribute species and ecosystems data and information. The vision is that those agencies/organizations could meet their intent and objectives of the policy by adopting and adapting the template policies and procedures in a manner consistent with their organizational situation. All agencies/organizations responsible for collecting, generating, and managing data and information should freely share data and information using a common approach to data security. This Security Policy template aims to facilitate this.

Purpose

The purpose of this policy is to:

1. Identify a set of principles by which the acceptance, management and distribution of species and ecosystems data and information should be governed.
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 enabling procedures that guide policy implementation.

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 element 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. A client who has requested access to Restricted Access data and information will be required to demonstrate a Business Case and abide by specified obligations associated with that access.

Confidentiality Agreement – a signed agreement which prescribes the terms of *Client* access, constraints to the use of, and redistribution of *Sensitive Ecological Data*. Confidentiality agreements are a means by which the Agency/Organization implements controls on the *Client's* use of *Sensitive Ecological Data*. Confidentiality agreements are considered instruments of the Agency/Organization.

Data Agreement - may be used to establish formal data sharing arrangements between Agencies/Organizations and clients. They are means by which both parties may formally detail their interests in the use of, and identify any restrictions on the distribution of, *Sensitive Ecological Data*. Data agreements are considered an instrument of both parties in this transaction. They may or may not be time limited.

Data Custodian – the Agency/Organization's designated authority over the management and security of the relevant database/data system

Data and Information Relevant to Government Programs – criteria used to designate data and information whose unrestricted distribution and sharing is likely to unduly harm government management programs.

Data and Information Relevant to Program Relations – criteria used to designate data and information whose unrestricted distribution and sharing is likely to unduly harm program relations of the agency or organization holding the data.

Data and Information Relevant to Indigenous Cultural Interests – for the purposes of these policies and procedures, designates a subset of data and information whose unrestricted distribution and sharing without appropriate permissions is likely to infringe upon or harm Indigenous cultural interests.

Data License - are means by which the Agency/Organization will formally detail its interests in the use of, and identify any restrictions on the distribution of, *Sensitive Ecological Data*. Data Licenses are typically used to provide one-time or ongoing *Client* access to *Sensitive Ecological Data* and as such are typically considered instruments of the Agency/Organization.

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 and information contained within.

Data Security Committee – an Agency/Organization committee tasked with evaluating and providing recommendations regarding Sensitive Ecological Data to the relevant data authority (Data Custodian).

Ecological Data and Information– data and information 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, natural communities, or other nontaxonomic biological entities (e.g., migratory species aggregation areas).

Elements of Conservation Concern – ecologically definable entities for which there are legitimate concerns for conservation, survival and/or persistence due to inherent and external threats. These may be identified by an agency or organization in a variety of means including conservation status rank (e.g., S1, S2, S3) or similar status labels (e.g., Endangered, Threatened, Vulnerable) or by other appropriate means.

Elements Susceptible to Harm – Elements of Conservation Concern for which unrestricted provision (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, Provincial, or Territorial Statute - a Bill that has passed in a Legislative Assembly (Provincial or Territorial) or Parliament of Canada (Federal), and is thereby enacted, becoming an Act (statute) or law.

Indigenous Land Data and Information – data and information which has been collected from or linked to indigenous lands and for which the agency or organization holding and managing the data may or may not possess appropriate permissions to facilitate unrestricted sharing and distribution.

Legislation or Regulation – for the purposes of these policies and procedures, designates a subset of data and information whose distribution and sharing may be restricted due the to requirements imposed by Federal, Provincial or Territorial Statutes.

Non-Sensitive Ecological Data and Information – 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 or linked to private lands and for which the agency or organization holding and managing the data does not possess appropriate permissions to facilitate unrestricted sharing and distribution.

Proprietary Data and Information – data and information for which the agency or organization holding and managing the data does not possess appropriate rights or permissions to facilitate unrestricted sharing and distribution.

Public Safety – for the purposes of these policies and procedures, designates a subset of data and information whose distribution and sharing may be restricted to protect the safety of the public (e.g., bear dens).

Restricted Access – designates the limitations placed on the distribution and sharing of various types of Sensitive Ecological Data and other data and information that an agency or organization may hold and manage.

Sensitive Ecological Data – data and information that, if inappropriately released, could significantly increase the risk of harm to Elements of Conservation Concern, their habitats, or the environment, or interfere with their conservation or recovery; Sensitive Ecological Data also includes ecological data and information that could harm the interests of persons, institutions, or jurisdictions or data and information that are linked to private or Indigenous lands; provincial, territorial, proprietary interests; or data and information that were obtained in confidence, release of which could jeopardize trust and relationships, infringe relevant Privacy legislation, or violate confidentiality agreements.

Data Security Principles

1. *Element* data and information should be maintained within well managed, secure data systems that adhere to best practices.
2. Conservation and management of *Elements* is better served by providing "decision makers" access to best available data and information (including spatial data and information).
3. Access to spatial or locality data and information for *Elements* under the criteria for *Elements Susceptible to Harm* should only be restricted in circumstances where the risk to the *Element* is increased to an unacceptable level. In principle the risk of disclosing must outweigh the risk of non-disclosure to limit access. In other words, *Element* data should be widely available unless a strong, rational argument for limiting access can be made. Such rationale should be transparent and well documented.
4. Access to spatial or locality data and information for Elements under other criteria (*Proprietary Data and Information*, *Private Land Data and Information*, *Indigenous Land Data and Information*, *Government Programs*, *Managing Program Relations*, *Indigenous Cultural Interests*, *Public Safety*, and *Legislation or Regulation)* should only be restricted where the risk to the interests specific to those areas or risks to the *Element* are considered to outweigh the risk of not making the *Element* data and information available. *Element* data should be widely available unless a strong, rational argument for limiting access can be made. Such rationale should be transparent and well documented.
5. Any Agency/Organization that restricts access to *Element* data and information 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 *Element* data should be identified by the Agency/Organization and made publicly available.

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., Training, Confidentiality Agreements, Non-Disclosure Agreements, Data Sharing Agreements).
8. The Agencies/Organizations responsible for collecting, generating, and managing *Element* data and information and responsible for using those data and information for conservation and management purposes should freely share data and information using a common approach to data security.
9. Data and information that is widely available should be so at as fine a resolution (scale) as possible. The Agency/Organization has a responsibility to transparently communicate that scale to *Client*s.
10. The Agency/Organization should only release data and information where they have appropriate authority to do so.

Policy Statements

1. It is the policy of the Agency/Organization to accept and manage data and information only when it has been collected consistent with relevant Federal, Provincial and/or Territorial statutes and regulations.
2. It is the policy of the Agency/Organization to make *Element* data and information as freely and openly available as possible, consistent with the philosophies and context of Open Data frameworks and where applicable, relevant Open Data and Information Policies.
3. Element data and information can be considered Restricted Access if and only if they meet one or more of the following criteria to designate them as *Sensitive Ecological Data*:
    a. The data and information have been identified to pertain to *Element(s) Susceptible to Harm*.
    b. The data and information are *Proprietary* and have associated limitations on their re-distribution.
    c. The data and information are relevant to *Private Lands* and have associated limitations on their re-distribution.
    d. The data and information are relevant to *Indigenous Lands* and have associated limitations on their re-distribution.
    e. Release of the data and information would unduly harm *Program Relations* of the *Agency/Organization*.
    f. Release of the data and information would unduly harm *Government Programs*,
    g. Release of the data and information is likely to infringe upon or harm *Indigenous Cultural Interests*.
    h. Release of the data and information may negatively affect *Public Safety*,
    i. Release of the data and information would be in violation of relevant *Legislation or Regulation*.
4. It is the policy of the Agency/Organization to routinely provide access to *Sensitive Ecological Data* where the *Client* has demonstrated an appropriate *Business Case* and where the Agency/Organization has the relevant authorities to distribute those data.

5. It is the policy of the Agency/Organization to provide access to *Sensitive Ecological Data* subject to relevant guidelines, restrictions, and agreements as necessary to maintain the integrity of that data (e.g., Confidentiality and Non-Distribution Agreements, Data Sharing Agreements, Training Requirements).
6. Implementation of this policy is enabled and 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. The *Agency/Organization* will make its Data and Information Security Policy and associated Procedures publicly available.