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

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

Procedures

The following procedures were developed by the NatureServe Canada Data Security Working Group to operationalize the **Data and Information Security Policy**. Procedures provide guidance for policy implementation in four broad areas:

1. Data and Information Acceptance and Management.
    a. Criteria for Acceptance of Data and Information[1].
    b. Marking Restrictions in Data Systems on Entry[1].
2. Identifying *Sensitive Ecological Data*.
    a. Identifying *Elements Susceptible to Harm*[1].
    b. Identifying and Managing *Proprietary Data and Information.*
    c. Identifying and Managing *Private Land Data and Information.*
    d. Identifying and Managing *Indigenous Land Data and Information.*
    e. Identifying and Managing Data and Information Relevant to *Government Programs.*
    f. Identifying and Managing Data and Information Relevant to *Managing Program Relations.*
    g. Identifying and Managing Data and Information Relevant to *Indigenous Cultural Interests.*
    h. Identifying and Managing Data and Information Subject to *Public Safety Restrictions.*
    i. Identifying Relevant Legislation and Regulations[1].
3. Data Distribution.
    a. Responding to Requests for *Sensitive Ecological Data*[1].
    b. Determining a *Client's Business Case* for Access to *Sensitive Ecological Data* [1].
    c. Data Agreements, Data Licenses and Confidentiality Agreements[1]
    d. Training.
    e. Displaying *Sensitive Ecological Data*[1].
    f. Release of *Sensitive Ecological Data*[1].
4. Administration.
    a. Administration[1].

1 - The procedures designated by this footnote are considered mandatory as part of a comprehensive approach to managing *Element* data and information. Others (those not marked) are optional and should be useful to those Agencies/Organizations that choose to use them.

Procedure: Criteria for Acceptance of Data and Information

Preamble:

This is a **required procedure** of a comprehensive **Data and Information Security Policy**.

This procedure outlines steps required to ensure that *Element* data and information received by an Agency/Organization have been legitimately acquired and to determine whether those data are at all encumbered.

Procedural Steps:

1. The Agency/Organization will ensure that all species and ecosystems data submitted to and managed within their data systems have been collected and submitted with appropriate permissions by ensuring that data submitters have verified this at the time of submission.
2. The data submission procedures of the Agency/Organization will recognize appropriate permissions through the evaluation of the data submitter confirmation of the following (as relevant to the jurisdiction):
    a. Any necessary permits were in place to gather the data.
    b. The data submitter owns the data or is acting as an agent for the owner of the data.
    c. The collection and collation of the data did not violate any relevant statutes.
    d. The data submitter explicitly acknowledges that landowner permission exists to submit data collected from private lands where access to those lands were required to gather the data.
3. The Agency/Organization may, at its discretion, request a review of the data submitters relevant permits and permissions.
4. The Agency/Organization will use risk assessment approaches to determine whether any data and information currently in their holdings require review of appropriate permissions.

Procedure: Marking Restrictions in Data Systems on Entry

Preamble:

This is a **required procedure** of a comprehensive **Data and Information Security Policy**.

This procedure outlines steps required to ensure that any use restrictions, whether imposed by the data submitter on the subsequent use and/or distribution of submitted data or imposed by the Agency/Organization on data in its holdings are recorded in the relevant data systems. The suite of acceptable restrictions will be outlined by the Agency/Organization. These restrictions may be permanent (e.g., they are never removed), temporary (time-limited), limit the spatial precision at which data can be displayed or redistributed at, and/or access may be limited to specified personnel. This procedure is only relevant to those agencies/organizations that accept data with such encumbrances. It will be up to the Agency/Organization to decide whether or not to accept encumbered data.

Procedural Steps:

1. The Agency/Organization 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.
2. Where associated restrictions allow some form of distribution, the Agency/Organization will enter into a formal Data Sharing Agreement with the submitter to formalize terms for that distribution (see Procedure for Data Agreements, Data Licenses and Confidentiality Agreements).
3. Where associated restrictions have a defined time limit, at the end of that time frame the Agency/Organization will remove the associated restrictions and the data will be managed as per all other relevant policies and procedures.

Procedure: Identifying Elements Susceptible to Harm

Preamble:

This is a **required procedure** of a comprehensive **Data and Information Security Policy**.

This procedure outlines steps required to determine whether an *Element of Conservation Concern* warrants the *Elements 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.

Consistent with the intent of the **Data and Information Security Policy**, the standards by which *Elements of Conservation Concern* are designated as *Elements Susceptible to Harm* will be governed by strict adherence to criteria that demonstrate substantive conservation risk.

Procedural Steps:

1. The Agency/Organization will establish a *Data Security Committee* responsible for reviewing proposed inclusions to or removals from the list of *Elements Susceptible to Harm*
2. The Agency/Organization will provide avenues for relevant *Agency/Organization* staff to nominate *Elements of Conservation Concern* as *Elements Susceptible to Harm*
3. The Agency/Organization will establish a regular review period (recommend 2-3 years)
4. The Agency/Organization will facilitate emergency evaluations for inclusions to the list of *Elements Susceptible to Harm*
5. The *Data Security Committee* will review risk to *Elements of Conservation Concern* by evaluating demonstrated or perceived risk to illegal trade (to *Elements of Conservation Concern* or their parts), economic value, risks to illegal destruction, persecution, collection, or harassment; or risk of unintended harm resulting from provision of locational data. The *Data Security Committee* will consider evaluation criteria as outlined in **Step A** (below).
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 relevant Data Custodian for approval.
7. The Agency/Organization will publish the list of *Elements Susceptible to Harm*

A. Evaluation Criteria for Elements Susceptible to Harm

1. *Element* status (G rank, S Rank, 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.
2. Existing protection associated with:
    a. Relevant Provincial/Territorial legislation (e.g., Endangered Species Legislation, other relevant legislation associated with natural resource management)
    b. Federal legislation (SARA, Migratory Bird Convention Act, WAPPRIITA)

3. Evidence of threats, the nature of the threat, and potential mitigating factors for the following categories of possible harm associated with making *Element* locational data and information publicly available:
    a. Existing legal capture or harvest of individuals.
    b. Existing evidence of illegal collection, persecution, or harassment.
    c. Existence of legal or illegal captive breeding or propagation.
    d. Existence and nature of any legal or illegal markets for the species.
    e. Potential for negative consequences from disturbance.
4. Risks associated with not disclosing locational data (e.g., inadvertent destruction of *Elements* or associated habitat, preventing prosecution, restricting ability to develop conservation plans).
5. Relevant references.

Procedure: Identifying and Managing Proprietary Data and Information

Preamble:

This is an **optional procedure** of a comprehensive **Data and Information Security Policy**.

This procedure outlines steps required to ensure that any restrictions imposed by the owner of the data and information (the entity owning the data and/or holding Intellectual Property Rights) are labelled upon receipt of the data and information in the relevant data system. In this procedure, the risk to the interests of the data owner must be 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. This procedure is only relevant to those Agencies/Organizations that accept data with such encumbrances. Agencies/Organizations should strongly discourage the acceptance of proprietary data with such encumbrances as they are by nature more limited in value due to the encumbrances and require more resources to manage effectively.

Procedural Steps:

1. The Agency/Organization will ensure that when owners of data request restrictions on the distribution of submitted data 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 the restriction.
    e. Contact information for the data provider.
2. Where associated restrictions allow some form of distribution the Agency/Organization will strive to enter into a formal Data Agreement with the data owner to formalize terms for that distribution (see Procedure for Data Agreements, Data Licenses and Confidentiality Agreements).
3. Where associated restrictions have a defined time limit, at the end of that time frame the Agency/Organization will remove the associated restrictions and the data will be managed as per all other relevant policies and procedures.
4. 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 and Managing Private Land Data and Information

Preamble:

This is an **optional procedure** of a comprehensive **Data and Information Security Policy**.

This procedure outlines steps required to ensure that any restrictions associated with data and information collected from private lands are labelled where necessary upon receipt of the data in the relevant data system. In this procedure, the risk to the interests of the landowner must be 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.

Procedural Steps:

1. The Agency/Organization will ensure that when data are received that are collected from private lands that the data have been collected in adherence with relevant permissions (see Data Acceptance Procedure).
2. The Agency/Organization will ensure that when data and information are received that have been collected from private lands, and the landowner has requested restrictions on their distribution, 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 (if any).
    d. Rationale for restriction.
    e. Relevant landowner contact information.
3. Where data have been collected from private lands remotely (i.e., no land access was required, e.g., remote sensing, remote observation) there can be no restrictions placed on its distribution under this category.
4. 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.
5. Where associated restrictions allow some form of distribution the Agency/Organization will strive to enter into a formal Data Sharing Agreement with the data owner to formalize terms for that distribution (see Procedure for Data Agreements, Data Licenses and Confidentiality Agreements).
6. Where associated restrictions have a defined time limit, at the end of that time frame the Agency/Organization will remove the associated restrictions and the data will be managed as per all other relevant policies and procedures.
7. Once data have been made public (i.e., distribution restrictions have been removed) then these restrictions cannot be re-instated retroactively.

Procedure: Identifying and Managing Indigenous Land Data and Information

Preamble:

This is an **optional procedure** of a comprehensive **Data and Information Security Policy**.

This procedure outlines steps required to ensure that any restrictions associated with data and information collected from Indigenous Lands are labelled where necessary upon receipt of the data in the relevant data system. In this procedure, the risk to the interests of the Indigenous Nation must be 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.

Procedural Steps:

1. The Agency/Organization will ensure that when data and information are received that have been collected from Indigenous Lands that the data and information have been collected in adherence with relevant permissions (see Data Acceptance Procedure).
2. The Agency/Organization will ensure that when data and information are received that have been collected from Indigenous Lands and the pertinent Indigenous Nation has requested restrictions on their distribution 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 (if any).
    d. Rationale for restriction.
    e. Relevant contact information.
3. Where data and information have been collected from Indigenous Lands remotely (i.e., no land access was required) there can be no restrictions placed on its distribution under this category.
4. Where associated restrictions allow some form of distribution the Agency/Organization will strive to enter into a formal Data Sharing Agreement with the pertinent Indigenous Authority to formalize terms for that distribution (see Procedure for Data Agreements, Data Licenses and Confidentiality Agreements).
5. Where associated restrictions have a defined time limit, at the end of that time frame the Agency/Organization will remove the associated restrictions and the data will be managed as per all other relevant policies and procedures.

Procedure: Identifying and Managing Data and Information Relevant to Government Programs

Preamble:

This is an **optional procedure** of a comprehensive **Data and Information Security Policy**.

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

Consistent with the intent of the **Data and Information Security Policy**, 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 *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.

Procedural Steps:

1. The Agency/Organization 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 programs and activities by distributing all or some data and information for those *Elements*.
2. The Agency/Organization will provide avenues for relevant staff to nominate *Elements* or subsets of data for *Elements* for consideration under the *Data Relevant to Government Programs* Category
3. The Agency/Organization will establish a regular review period (recommend 2-3 years)
4. The Agency/Organization will facilitate emergency evaluations for inclusions to the list of *Elements* or subsets of data for *Elements* for consideration under the *Data Relevant to Government Programs* Category.
5. The *Data Security Committee* will review risk to *Elements* or subsets of data for *Elements* for consideration under the *Data Relevant to Government Programs* Category by evaluating demonstrated or perceived risk to government programs and activities (e.g., legal investigations, wildlife harvest management programs).
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 *Elements* for consideration under the *Data Relevant to Government Programs* Category to the relevant *Data Custodian*(s) for approval.
8. The Agency/Organization will publish the list of *Elements* or subsets of data for *Elements* for which datasets have been deemed *Sensitive Ecological Data* under the *Data Relevant to Government Programs* Category.

Procedure: Identifying Data and Information Relevant to Managing Program Relations

Preamble:

This is an **optional procedure** of a comprehensive **Data and Information Security Policy**.

This procedure outlines steps required to identify data and information for *Elements* whose distribution may cause unacceptable risk to program relations of the relevant Agency/Organization.

Consistent with the intent of the **Data and Information Security Policy**, 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 *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.

Procedural Steps:

1. The Agency/Organization will establish a *Data Security Committee* responsible for reviewing proposed inclusions to or removals from the list of *Elements* due to the risk posed to program relations by distributing all or some data for those *Elements*.
2. The Agency/Organization will provide avenues for relevant staff to put forth *Elements* or subsets of relevant data for *Elements* for consideration under the *Data Relevant to Program Relations* Category.
3. The Agency/Organization will establish a regular review period (recommend 2-3 years)
4. The *Data Security Committee* will review risk to Managing Program Relations by evaluating demonstrated or perceived risk to Agency/Organization 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 *Elements or subsets of data for Elements* for consideration under the *Data Relevant to Managing Program Relations* Category to the relevant Data Custodian(s) for approval.
7. The Agency/Organization may, at their discretion, choose to consult with the relevant affected parties in the relationship.
8. The Agency/Organization will publish the list of *Elements* for which datasets have been considered *Sensitive Ecological Data* under the *Data Relevant to Managing Program Relations* category.

Procedure: Identifying and Managing Data and Information Relevant to Indigenous Cultural Interests

Preamble:

This is an **optional procedure** of a comprehensive **Data and Information Security Policy**.

This procedure outlines steps required to ensure that any restrictions associated with the protection of Indigenous Cultural Interests are labelled where necessary upon receipt of the data in the relevant data system. In this procedure, the risk to the interests Indigenous Cultural Interests must be 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.

Procedural Steps:

1. The Agency/Organization will establish a process with relevant Indigenous Authorities to facilitate the identification of sites of cultural importance where the distribution of data and information for *Elements* could result in the degradation of the culturally significant site or resource or be expected to interfere with the conservation of sites having an anthropological or heritage value or aboriginal cultural significance.
2. The Agency/Organization will ensure that when data and information are received that are collected from sites with Indigenous Cultural Importance and the pertinent Indigenous Authority has requested restrictions on their distribution 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 (if any).
    d. Rationale for restrictions.
    e. Relevant contact information.

Where associated restrictions allow some form of distribution the Agency/Organization will strive to enter into a formal Data Sharing Agreement with the relevant Indigenous Authority to formalize terms for that distribution.

Procedure: Identifying and Managing Data and Information Subject to Public Safety Restrictions

Preamble:

This is an **optional procedure** of a comprehensive **Data and Information Security Policy**.

This procedure outlines steps required to determine whether an *Element* warrants any data and information being labelled as *Sensitive Ecological Data* due to the risk that unrestricted distribution may result in an unacceptable safety risk to the public (e.g., provision of locational data for dens of dangerous animals).

Consistent with the intent of the **Data and Information Security Policy**, the standards by which data and information are restricted for these purposes will be governed by strict adherence to criteria that demonstrate substantive real or perceived public safety risk. In this procedure, the risk public safety must be 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.

Procedural Steps:

1. The Agency/Organization will establish a *Data Security Committee* to oversee this designation (see Identifying *Elements Susceptible to Harm Procedure*).
2. The *Data Security Committee* will consult with relevant wildlife management and enforcement authorities to determine if any *Element* data and information or subset of *Element* data and information warrants designation as *Sensitive Ecological Data* under this category. The *Data Security Committee* will consider only those risks with a substantive real or perceived public safety risk.
3. The Agency/Organization will establish a regular review period (recommend 2-3 years)
4. The Agency/Organization will facilitate emergency evaluations for inclusion to the list of data and information restricted under this category.
5. The *Data Security Committee* will provide recommendations and rationale for inclusions to and deletions from the list of *Elements* or subsets of data and information *for Elements* for consideration as *Sensitive Ecological Data* due to public safety concerns to the relevant *Data Custodian* for approval.
6. The Agency/Organization will publish the list of data and information restricted under this category.

Procedure: Identifying Relevant Legislation and Regulations

Preamble:

This is a **required procedure** of a comprehensive **Data and Information Security Policy**.

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

Procedural Steps:

1. The Agency/Organization will be bound be relevant Federal, Provincial and Territorial statutes and will label and restrict access to all data whose distribution would violate such statutes (e.g., FOIPP, ATIPP).
2. Data and information considered *Sensitive Ecological Data* under this category will only be released by the relevant statutory authority.

Procedure: Responding to Requests for *Sensitive Ecological Data*

Preamble:

This is a **required procedure** of a comprehensive **Data and Information Security Policy**.

This procedure outlines steps required to provide effective and timely responses to *Client* requests for access to *Sensitive Ecological Data*. The procedure provides guidance to facilitate clear responses and decisions with respect to these requests.

Procedural Steps:

1. The Agency/Organization will routinely receive, review, and respond to *Client* requests for access to *Sensitive Ecological Data*.
2. The Agency/Organization will use a standard request form and will make that available to *Client*s in a manner consistent with its operations.
3. The Agency/Organization will publish service standards for data request response times such that *Client*s are aware of these.
4. The Agency/Organization will assess the *Client's Business Case* (see Business Case Procedure). In situations where the *Client's Business Case* is uncertain the Agency/Organization will communicate further with the *Client* to clarify its needs, and where appropriate communicate with operational staff within the Agency/Organization to better understand the operational requirements relevant to the request.
5. If the *Client* is unable to establish a business case, the Agency/Organization will not provide the *Sensitive Ecological Data* and the Agency/Organization will communicate that decision and the rationale for it to the *Client* in a timely manner.
6. The Agency/Organization will provide an opportunity and process for a *Client* to appeal a decision to deny access to *Sensitive Ecological Data* to the designated *Data Custodian.* The Agency/Organization will ensure that the appeal process is published so that *Clients* are clearly aware of it.
7. The staff that manage data requests within the Agency/Organization may routinely communicate the results of requests for *Sensitive Ecological Data* to relevant staff within the Agency/Organization.
8. The Agency/Organization will keep a record of responses to data requests where either *Sensitive Ecological Data* are provided to the *Client* or where such a request is denied. The record will include at a minimum:
    a. Date.
    b. *Client* name and contact information.
    c. Entity the *Client* is representing (if the *Client* is not a member of that organization).
    d. *Sensitive Ecological Data* requested.
    e. Decision (provide or deny).
    f. Reasons for any denied requests.
9. The Agency/Organization will ensure that the *Client* is informed of the fact that a record of their request is being generated and archived.

Procedure: Determining a *Client's* Business Case for Access to *Sensitive Ecological Data*

Preamble:

This is a **required procedure** of a comprehensive **Data and Information Security Policy**.

This procedure outlines steps required to determine whether a prospective *Client* has demonstrated a reasonable business case to be granted access to *Sensitive Ecological Data*. In addition, the procedure is designed to determine, refine, and restrict the spatial and taxonomic extent of the *Sensitive Ecological Data* provided as warranted. The procedure presumes that the Agency/Organization responding to the request has done its due diligence to objectively and transparently determine what data and information are deemed to be *Sensitive Ecological Data* (see relevant procedures for identifying *Sensitive Ecological Data*). As such, these procedures are premised on providing only that component of *Sensitive Ecological Data* required by the *Client*.

Procedural Steps:

1. The Agency/Organization will ensure that a *Client* has demonstrated a reasonable *Business Case* to be granted access to *Sensitive Ecological Data* for the *Elements* included in the request by executing the steps outlined in Step A below.
2. The Agency/Organization will refine and limit the spatial and taxonomic extent of the *Sensitive Ecological Data* provided to a *Client* by executing the steps outlined in Step B below.
3. The Agency/Organization will take measures to assess whether the *Client's* needs would be sufficiently served with data and information of a more general precision (potentially, but not necessarily, eliminating the need for *Sensitive Ecological Data*) such as generalized locality data that would reduce the amount of precise *Sensitive Ecological Data* released to the *Client*. This will require the Agency/Organization to work with the *Client* to tailor the data and information provided to both meet their needs and preserve the integrity of any *Sensitive Ecological Data* ultimately provided to the *Client*.
4. The Agency/Organization will weigh the perceived benefits of providing *Sensitive Ecological Data* to the *Client* against the potential risks to the security of the *Sensitive Ecological Data* (i.e., data breaches). In the absence of legitimate reasons to the contrary, the Agency/Organization will always provide *Sensitive Ecological Data* to *Client*s with legitimate requests.

A. Determining a *Client's* Business Case

The entity holding and managing the requested *Sensitive Ecological Data* will determine whether a *Business Case* has been established through evaluation of the following criteria:

1. The *Client* has a legal, regulatory, or policy requirement to consider *Sensitive Ecological Data* within their business activities and/or,
2. The *Client* has an established management responsibility for the *Elements* included in the request for *Sensitive Ecological Data* and/or,
3. The *Client's* activities will further conservation of the *Elements* included in the request for *Sensitive Ecological Data* and/or,

4. The *Client's* use of the data requested will improve knowledge for the *Elements* included in the request for *Sensitive Ecological Data* and/or,
5. 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 *Elements* included in the request for *Sensitive Ecological Data* and/or,
6. The *Client* has a mandate specific to the *Elements* included in the request for *Sensitive Ecological Data* (e.g., develop status assessments, management plans, recovery strategies, conduct relevant academic research and/or,
7. The *Client* requires the data for the *Elements* included in the request for *Sensitive Ecological Data* to make recommendations regarding the management of specified lands or waters and/or,
8. The data for the *Elements* included in the request for *Sensitive Ecological Data* are required by legislation or are required for legal enforcement purposes.

B. Determining the Scope of Data Requirements

The entity holding and managing the requested *Sensitive Ecological Data* will take measures to determine and potentially limit the geographic and/or taxonomic scope of *Sensitive Ecological Data* required by a *Client* by:

1. Evaluating whether the *Client's* needs might be more appropriately served by the provision of *Sensitive Ecological Data* of a more limited taxonomic scope or data and information of a more generalized nature than originally requested.
2. Working with the *Client* to clearly delineate the spatial bounds of the activities for which *Sensitive Ecological Data* may be required and limiting the data provided consistent with those spatial bounds.

a. Determining whether the nature of the *Client's* activities (timing, scope) might be further grounds for reducing the geographic scope of the *Sensitive Ecological Data* provided.

Procedure: Data Agreements, Data Licenses and Confidentiality Agreements

Preamble:

This is a **required procedure** of a comprehensive **Data and Information Security Policy**.

This procedure enables the Agency/Organization to establish requirements for *Clients* to enter into *Data Agreements* (e.g., Data Sharing Agreements), *Data Licenses* and/or *Confidentiality Agreements* prior to receiving access to *Sensitive Ecological Data*. *Data Agreements* or *Data Licenses* are means by which affected parties may formally detail the interests of the Agency/Organization in the use of, and identify any restrictions on the distribution of, *Sensitive Ecological Data*. *Data Agreements* may be used to establish formal data sharing arrangements between agencies/organizations. *Data Licenses* are typically used to provide one-time or ongoing *Client* access to *Sensitive Ecological Data*. Agencies/Organizations may choose to use *Confidentiality Agreements* as a component of managing *Client* use of *Sensitive Ecological Data*. These may be used as the sole means of managing *Client* use of *Sensitive Ecological Data* or in concert with *Data Agreements* and/or *Data Licenses*. *Confidentiality Agreements* prescribe the terms of *Client* access, constraints to the use of, and redistribution of *Sensitive Ecological Data*.

Procedural Steps: Data Agreements and Data Licences

1. The Agency/Organization will publicize any requirement for *Client*s to enter into *Data Agreements* or *Data Licenses* to facilitate access to *Sensitive Ecological Data*.
2. The Agency/Organization may institute time limits associated with signed *Data Agreements* and *Data Licenses*.
3. The Agency/Organization will publish template *Data Agreements* or *Data Licenses* on relevant platforms and portals.
4. The Agency/Organization will publish any other *Client* requirements related to entering into *Data Agreements* or *Data Licenses* (e.g., Training Requirements, *Confidentiality Agreements*) on relevant platforms and portals.
5. The Agency/Organization will maintain records that document established *Data Agreements* and *Data Licenses*.

Procedural Steps: Confidentiality Agreements

1. The Agency/Organization will publicize the requirement for *Client*s to enter into *Confidentiality Agreement*(s) prior to receiving access to *Sensitive Ecological Data*.
2. The Agency/Organization will publish a template *Confidentiality Agreement* on relevant platforms and portals.
3. The Agency/Organization may institute time limits associated with signed *Confidentiality Agreements*.
4. The Agency/Organization will publish any other *Client* requirements related to entering into *Confidentiality Agreements* (e.g., Training Requirements, *Data Licenses*) on relevant platforms and portals.
5. The Agency/Organization will maintain records that document *Confidentiality Agreements* (including *Client*, completion date, and expiry date).

Procedure: Training

Preamble:

This is an **optional procedure** of a comprehensive **Data and Information Security Policy**.

This procedure facilitates any requirement an Agency/Organization might have for *Client*s to undertake relevant training prior to receiving access to *Sensitive Ecological Data*. This procedure is optional and only relevant to those agencies/organizations that institute such requirements.

Procedural Steps:

1. If the Agency/Organization has a requirement for *Client*s to undertake training prior to receiving access to *Sensitive Ecological Data* that requirement will be clearly articulated on data access platforms and sites, and on relevant data request portals and forms (see Responding to Requests for *Sensitive Ecological Data* Procedure).
2. The Agency/Organization will clearly articulate the frequency at which training is required to continue to maintain opportunities to acquire access to *Sensitive Ecological Data*.
3. The Agency/Organization will facilitate ready access for *Client*s to its training materials.
4. The Agency/Organization will maintain records that document *Client* training completion and relevant dates.

Procedure: Displaying *Sensitive Ecological Data*

Preamble:

This is a **required procedure** of a comprehensive **Data and Information Security Policy**.

This procedure outlines steps an Agency/Organization may take to make known the presence of *Sensitive Ecological Data* and facilitates the steps an Agency/Organization may take if it wishes to routinely provide a generalized product for data that is classified as *Sensitive Ecological Data* in a manner consistent with the Agency/Organization's procedures associated with provision of *Non-sensitive Ecological Data.*

Procedural Steps:

1. The Agency/Organization 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, direct request services).
2. If the Agency/Organization utilizes a request-based method of managing *Client* requests for data, they will develop and utilize a standard response to *Client*s to inform them of the presence of *Sensitive Ecological Data* within their area of interest.
3. If the Agency/Organization utilizes web-based portals and/or data services they will spatially obscure location data (e.g., fuzzing) and/or withhold taxonomic identifiers for the *Elements* in question. The Agency/Organization may choose, as necessary, to withhold additional data attributes to maintain the security and integrity of the *Sensitive Ecological Data.*
4. The Agency/Organization will obscure *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 Agency/Organization will choose to display taxonomic identifiers for spatially obscured/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 Agency/Organization will strive to provide taxonomic identifiers for obscured *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 Agency/Organization may develop a *Sensitive Ecological Data* product that could be displayed and routinely distributed as *Non-Sensitive Ecological Data* by spatially generalizing *Sensitive Ecological Data* to a scale whose routine distribution would not interfere with the security and integrity of the *Sensitive Ecological Data.*
7. The Agency/Organization may provide the de-sensitized product as an integral component of their standard suite of data offerings through their relevant data portals, platforms, or other data services.
8. The Agency/Organization will clearly communicate to *Client*s where data has been generalized or otherwise obscured on data portals or through relevant data services.

Procedure: Release of *Sensitive Ecological Data*

Preamble:

This is a **required procedure** of a comprehensive **Data and Information Security Policy**.

This procedure outlines the steps necessary to ensure that *Sensitive Ecological Data* is released to *Client*s in a manner that enables and promotes effective use and ensures that data is not mis-used.

Procedural Steps:

1. The Agency/Organization will release *Sensitive Ecological Data* subject to an appropriate *Business Case* (See Business Case Procedure) and other conditions as required by the Agency/Organization (e.g., Training, Data Agreements, Data Licenses, Confidentiality Agreements).
2. The Agency/Organization may limit the geographic scope of *Sensitive Ecological Data* released to only that necessary to meet a *Client's* stated purpose, consistent with procedural steps outlined in the *Business Case* Procedure.
3. The Agency/Organization may limit the (scope of) details of *Sensitive Ecological Data* released to only that necessary to meet a *Client's* stated purpose, consistent with procedural steps outlined in the *Business Case* Procedure
4. The Agency/Organization may, in an emergency and under the relevant designated authority, release *Sensitive Ecological Data* where not releasing *Sensitive Ecological Data* would further jeopardize the relevant *Elements* or other considerations that led to the *Sensitive Ecological Data* designation.
5. In the case of emergency release, the Agency/Organization will only release *Sensitive Ecological Data* to those personnel who have an immediate need-to-know.
6. In the case of emergency release, the Agency/Organization will retroactively ensure that personnel with whom *Sensitive Ecological Data* were provided meet the standard conditions associated with routine provision (e.g., Training, Data Agreements, Data Licenses, Confidentiality Agreements).
7. The Agency/Organization will provide necessary guidance regarding limitations of use and interpretation of *Sensitive Ecological Data* in conjunction with all data releases.
8. 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.*
9. The Agency/Organization will clearly communicate, at the time of data release, any restrictions and/or guidance regarding subsequent use and display of *Sensitive Ecological Data* in *Client* documents, reports and maps.

Procedure: Administration

Preamble:

This is a **required procedure** of a comprehensive **Data and Information Security Policy**.

Procedural Steps:

1. The Agency/Organization will publish the position of their designated Data Authority (*Data Custodian*) and relevant contact information on relevant data portals, data platforms, web sites, and within relevant meta-data for data systems.
2. The Agency/Organization will maintain searchable electronic records that at a minimum document:
    a. Establishment of Data Licenses, Data Agreements, Confidentiality Agreements or other such instruments and any relevant expiry dates.
    b. Provision of *Sensitive Ecological Data* to *Client*s (See Responding to Requests for *Sensitive Ecological Data* Procedure).
    c. Denial of provision of *Sensitive Ecological Data* to *Client*s.
    d. Training Completion and Expiry information (See Training Procedure).
    e. Meta-data for (a-d) including names, dates, restrictions, and any other relevant details.
3. The Agency/Organization will ensure that their approved operational Data and Information Security Policy and enabling Procedures are published on relevant data portals, data platforms and web sites.