Seacoast Indigenous Guardians Network
Data Access Policy

Effective: March 3, 2025

Section 1
BACKGROUND, PURPOSE, AND SCOPE

The purpose of this Data Access Policy (Policy) is to establish guidelines for accessing, managing, and protecting tribal data in accordance with tribal sovereignty, privacy rights, and ethical standards. This Policy ensures that data is used responsibly, securely, and in a manner that benefits the tribal community. Use of and/or access to the ISN-SIGN platform constitutes consent to be bound by the terms of this Policy.

Seacoast Indigenous Guardians Network (SIGN) seeks to empower Southeast Alaska Tribes with the tools and resources they need to steward and restore balance to their traditional homelands and waters, in perpetuity. As part of reaching this goal, SIGN is partnering with the Indigenous Sentinels Network (ISN), whose mission is to support the collection of Indigenous, Traditional and Local knowledges (ITLK) and scientific information to empower ecosystem- and community-centered natural resource management and decision-making at multiple levels (i.e., generate actionable data along-side creative and broad reaching science communication). ISN is one environmental monitoring network that operationalizes Indigenous Data Sovereignty through practices of Indigenous Data Governance as "the enactment of Indigenous Data Sovereignty referring to the mechanisms that support Indigenous decision-making on how data are controlled, collected, interpreted, accessed, stored, and used" (Walter et al. 2020).

SIGN's partnership with ISN will establish a SIGN-specific database that features customizable data collection survey forms, audio recording capabilities, and reporting, where our tribal partners will be able to collect and store data while retaining sovereignty over the data they collect. ISN has over 20 years of experience in Tribal environmental monitoring, data collection, and development of tribally owned environmental monitoring software. ISN remains grounded in goals to rebuild sovereign capacity for the stewardship of lands and waters. ISN has partnered with SIGN, as administered by Central Council of Tlingit & Haida Indian Tribes of Alaska (Tlingit & Haida), to bring ISN-SIGN Database architecture, data collection methodology, training and capacity building to Southeast Alaska.

Tribal sovereigns exercise their rights of self-determination and self-governance over their members, territory, and resources. Tribal sovereigns may also elect to exercise authority over environmental and natural resource matters impacting their Tribal citizens, including emerging threats and other related needs in their communities. As sovereign governments, Tribes also have important goals both including and beyond environmental health, such as the promotion of

individual, family, and community wellbeing. These matters and corresponding goals may require the collection and provision of proprietary data.

This Policy applies to all individuals, organizations, and entities seeking access to tribal data, including but not limited to tribal government agencies, external researchers, contractors, and third-party vendors. The purpose of this Policy is to establish a SIGN-wide policy for how SIGN will:

- Provide Tribes with data, including the scope of data available
- Implement the process to obtain data within the expected timelines for processing Tribal requests for data; and
- Respond to requests from Tribes for data in the custody and control of SIGN and its Staff and Operating Division (known as the Indigenous Stewardship Programs (ISP) Division).

This Policy will help ensure SIGN is sharing data with Tribes to the maximum extent permissible under applicable laws, regulations, and existing agreements and enhance the social, physical, spiritual, economic, and health status of Indigenous Peoples. This Policy is applicable to all of SIGN, including any program(s) that it or its Guardians oversees and/or administers, and is intended to provide expectations and best practices for SIGN to manage and respond to tribal data requests and inquiries. Organizations with data covered by this Policy shall implement protocols for managing and responding to Tribal requests for data administered by or held under that Organization's custody and control that are consistent with this Policy.

Section 2
GUIDING PRINCIPLES

- **Tribal Sovereignty:** Tribes retain full ownership and control over their data. Access to tribal data must be granted through proper tribal governance structures.
- **Privacy and Confidentiality:** Personally identifiable information and sensitive data must be safeguarded against unauthorized access and disclosure.
- **Transparency:** Data access decisions and usage must be clearly communicated to the tribal community.
- **Benefit to the Tribe:** Access to tribal data must align with the tribe's priorities and be used to advance the well-being of its citizens.
- **Cultural Sensitivity:** Data use must respect tribal customs, traditions, and values.

Section 3
AUTHORITY

The SIGN Chief Data Officer (CDO) shall oversee the implementation of this Policy in collaboration and consultation with ISP Division CDOs and the Indigenous Sentinels Network

CDOs. The SIGN CDO shall manage and update a public access website that facilitates access to this Policy, points of contact, and guidance as described below. The Guardians will serve as community Administrators to their respective Tribes' programs and data collection, use and application, including on the ISN-SIGN platform referenced herein. Access to data will be granted based on predefined roles, minimizing exposure to unauthorized personnel.

Section 4
PROCEDURES

Section 4.1 Training and Awareness

All ISN-SIGN database users will be provided with a copy of the Policy to educate users about the guidelines, terms of use, and promoting awareness of data governance principles.

- **Mandatory Training:** All Administrators and Programs granted access to tribal data must complete training on data privacy, security, and ethical use.
- **Ongoing Education:** Regular workshops and updates may be provided to ensure continued awareness of best practices and evolving policies.
- **Cultural Sensitivity Training:** Specific training will be conducted to ensure respect for tribal customs and traditions in data handling.
- **Compliance Monitoring:** Participation in training will be tracked, and refresher courses may be required periodically.
- **Encryption Standards:** All sensitive data must be encrypted in storage and transmission to prevent unauthorized access.
- **Regular Security Audits:** Periodic security assessments will be conducted to identify vulnerabilities and enhance data protection measures.
- **Incident Reporting Protocol:** A formal process will be in place for reporting and addressing data breaches or security incidents.
- **Backup and Recovery Plan:** Secure and redundant backups will be maintained to prevent data loss and ensure business continuity.

Section 4.2 Data Requests

When a Tribe requests Tribe-specific data that it has submitted previously to the ISP Division, every effort should be made to share back those data submitted directly by the Tribe in a timely manner by the recipient Program. A Tribe may also request datasets that can be made available to another government entity in furtherance of carrying out services and functions and promoting the health and well-being of its population and homelands. This includes, but is not limited to, datasets that contain aggregate data or individual-level data about the Tribe or general datasets pertaining to events impacting the Tribe.

Each Program with data covered by this Policy shall develop operating protocols and guidance for responding to data requests from Tribes that are specific to each Organization's internal operations, data systems, and applicable legal authorities. Such protocols and guidance must comply with this Policy. Such protocols and guidance shall ensure data is secure and sufficiently available, consistent with this Policy. Such protocols and guidance shall ensure access to data,

datasets, monitoring systems, evaluation systems, delivery systems in possession of the Program are provided to the maximum extent permitted by applicable law, regulation, existing agreements, and Organization privacy and security policies without the imposition of administrative conditions that are not otherwise generally applicable to Tribes or other government entities. Organization protocols and guidance shall include the components necessary for efficient and effective review, evaluation, and fulfillment of data requests from Tribes. Protocols and guidance shall include at a minimum:

- Procedures for submitting data requests, including the identification of any associated documents that may be required (e.g., standard forms, templates); this shall include any additional details regarding Traditional Knowledge requests.
- Procedures for ensuring timely access by Tribes to requested data, including specific deadlines for processing data requests, with a maximum of 15 business days to acknowledge receipt of a request and 90 calendar days to grant or deny the request, and provide a description of steps necessary for the Tribe to take in order to receive such data (such as completing a data sharing agreement or credentialing users).
- Procedures for internal review of data requests, including for assessing and tracking compliance.
- A list of existing potentially available datasets that are of likely interest to Tribes.
- Procedures for handling denials include issuing a written notice to the requestor with a reason for the denial.
- Procedures for expediting data requests, where possible, in the event of an emergency (whether a formally declared or other urgent response scenario). This shall include a process for the requestor to inform the relevant Administrator of the nature of the emergency.
- Procedures to access technical assistance resources, if any, that can potentially assist Tribes with requesting data and complying with data security requirements. Each Administrator with data covered by this Policy should consider how best to securely transmit responses to tribal data requests to facilitate greater accessibility when possible and appropriate for public health activities (e.g., through machine-readable datasets, summary tables, graphs, and narratives). Program Administrators are encouraged to consider use of a “Disclosure Request Checklist” (Appendix A) as part of developing their operating protocols and guidance.
- Each Program Administrator shall complete the requirements of this section within twelve (12) months of this Policy's Effective Date.

Section 4.3 Data Retention and Deletion

Deletion Requests: Individuals have the right to request the deletion of their personal data under the following circumstances:

- The data is no longer necessary for the purposes for which it was collected.
- The individual withdraws consent (where consent is the legal basis for processing).
- The data must be deleted to comply with data sharing agreements.

To request data deletion, individuals may contact their program Administrator or Division leads. Requests will be processed within 15 days of request.

Data Deletion Methods: Data will be deleted using one or more of the following methods:

- **Digital Data:** Secure erasure using industry-standard tools and techniques to ensure complete removal from all systems, databases, and backups.
- **Physical Data:** Secure shredding or incineration of paper records and documents.

Section 5
SECURITY MEASURES

The mechanism for operationalizing Indigenous Data Sovereignty is the ISN software infrastructure and built-in multi-level privacy protections through ISN-SIGN database technology. All Users of the ISN-SIGN database are inherent owners of their data. The data entered into the ISN-SIGN applications and uploaded to the ISN-SIGN Database Platform is wholly owned by the ISN-SIGN User and can only be used in the ways outlined in the Network Agreement and End User Agreement that are shared with project administrators and community members at the start of the monitoring programs, subject to any additional provisions adopted by Administrators on a project- or program-specific basis. The SIGN database is a private database only accessible to Users of ISN with express allowances. Through the settings within an App, an Administrator may designate the extent to which user wishes to share data with other Community members. An Administrator may, in its sole discretion, invite other Community members or external organizations to view or download user data as designated by the Administrator. By extending such an invitation, and/or by adopting any provisions in addition to the Network Agreement and End User Agreement on a project- or program-specific basis, Administrators retain all responsibility to obtain End User consent to disclose shared information. No data held on the ISN-SIGN platform is accessible to Users outside of those specific programs unless designated by the appropriate SIGN Administrator(s). Each data collection project is managed by the designated Organization, Community, or Program Administrator. Multiple layers of Administrative roles and capabilities have been built into the ISN-SIGN system for further Indigenous Data Governance and control over who, within a data collection program, has access to what data, including external and internal program partners.

Section 5
COMPLIANCE

To align with data protection and privacy regulations, SIGN will inform, operationalize, and protect Indigenous Peoples' rights to Free, Prior and Informed Consent (FPIC) - a specific right that pertains to Indigenous Peoples and reaffirms and asserts Indigenous Peoples' rights to self-governance and self-determination over their collection, use, and ownership of data. These principles, coupled with the universal right to self-determination, are the foundation to give and withhold consent to participate in research, science, and other projects, promote equitable participation, and protect Indigenous knowledge. SIGN operates under and upholds the CARE (Collective Benefit, Authority to Control, Responsibility Ethics) Principles and FAIR (Findable, Accessible, Interoperable, and Reproducible) Principles to strengthen Indigenous data sovereignty in our region. The CARE principles for Indigenous Data Governance complement the more data-centric approach of the FAIR principles, introducing social responsibility to open

data management practices. Violations of this Policy may result in penalties, including revocation of access, legal action, and other measures deemed necessary by SIGN or ISN, as applicable.

Section 6
REVIEW AND REVISION

This Policy shall be reviewed periodically and updated as needed to reflect changes in tribal priorities, applicable legal requirements, and technological advancements. SIGN shall stand up a data forum to periodically solicit individual feedback and individual input from Tribal officials and Tribal subject matter experts regarding Tribal data access, which may include but not be limited to issues such as the efficacy and efficiency of ISP Division operating protocols and guidance, as well as gaps in data practices, collection, and reporting methods as they relate to tribal data requests. These communications will be in the form of consensus advice or recommendations. At the forums, SIGN will also share updates, highlight relevant datasets and projects, and provide relevant information about Tribal data. SIGN may also convene periodic Tribal listening and engagement sessions.

Section 7
CONTACT INFORMATION

Each Community with data covered by this Policy shall designate an official point of contact or points of contact (PoCs), which may be a general inbox or inboxes and/or specified personnel position(s), for external correspondence related to Tribal data requests. The SIGN CDO shall make the master list of PoCs. Community CDOs will notify SIGN CDO of any updates and changes impacting accuracy of information.

Section 8
DEFINITIONS

For the purpose of the Policy, terms are defined as follows:

Application or App - the programming or code that is accessible to users of the ISN Platform. The App will consist of base Platform configurations and in some cases additional code (Feature Request and/or enhancements) needed to deploy the App to a participating SIGN Community or Organization.

Chief Data Officer – a person who is responsible for the overall data strategy, governance, and management within an organization. The CDO oversees data-related policies, ensures compliance with data protection regulations, drives data-driven decision-making, and enhances data security, quality, and accessibility.

Community – the SIGN user community that consists of members and users of participating communities.

Confidential Data - highly sensitive data requiring explicit permission for access (e.g., personal records, sacred knowledge).

Data - any collection of facts, statistics, or information that is stored, processed, or transmitted in digital or physical formats.

Division –Tlingit & Haida's Indigenous Stewardship Programs Division.

Form – a list of questions to collect observations under a program.

Indigenous data - data that is created, collected, or related to Indigenous peoples, communities, lands, cultures, knowledge systems, and governance. It includes information about Indigenous individuals, groups, resources, and environments, whether generated by Indigenous peoples themselves or by external entities.

Indigenous Data Governance - the frameworks, principles, and practices that enable Indigenous peoples, communities, and organizations to have authority over the collection, ownership, use, and management of their data. It ensures that Indigenous data is handled in a way that aligns with Indigenous values, sovereignty, legal traditions, and cultural protocols. This governance approach supports self-determination, ethical data stewardship, and responsible data sharing to benefit Indigenous communities.

Indigenous data sovereignty – the right held by Indigenous peoples to control the collection, ownership, and application of data about them, ensuring its use aligns with their values, governance, and self-determination.

Intellectual Property Rights - all patents, inventions (whether patentable or not), trademarks, service marks, trade dress, logos, and domains, (together with all of the goodwill associated therewith), copyrights, trade secrets and all other intellectual property rights, in each case whether registered or unregistered and all similar or equivalent rights or forms of protection provided by applicable law, regulations or rules in any jurisdiction throughout the world.

Indigenous, Traditional, and Local Knowledges (ITLK) - the accumulated knowledge, practices, and beliefs developed and sustained by Indigenous peoples, traditional societies, and local communities over generations. This knowledge is deeply rooted in cultural heritage, environmental stewardship, and lived experiences, often transmitted orally or through practice. ITLK informs sustainable resource management, biodiversity conservation, and social governance, and is recognized for its value in scientific and policy discussions while requiring respectful and ethical engagement.

ISN Network - the group of Users (including Administrators and Observers) that use the ISN Application and Platform, programs they initiate, and wider stakeholder connections.

Organization - an organization with a purpose, usually representing/governing a community that provides administrative oversight of a data collection program. Typical ISN Organizations at the

moment include Tribal Governments, Municipal governments, Universities, NGOs, Federal and State agencies, and other non-profits.

ISN-SIGN Platform -the full ISN-SIGN software technology 'stack' and community. This is the foundation for the App functionality and any other Feature Request.

Observer - an individual or entity that monitors, assesses, or records events, data, or processes and enters this information into the App. Observers may collect information for analysis, compliance, research, or oversight purposes.

Personally Identifiable Information (PII) - information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information, that is linked or linkable to a specific individual.

Program – a data collection effort managed by an organization with clear target observations and protocols (i.e. marine mammal observing program).

Program Administrator –responsible for overseeing the implementation and management of data-related policies, procedures, and governance frameworks within a Community or Organization. This role includes ensuring data security, compliance with regulations, and efficient data lifecycle management. The Administrator works closely with data officers and users to facilitate data integrity, access control, and proper data deletion practices.

Public Data - information intended for general dissemination (e.g., public reports, announcements).

Restricted Data - information available only to authorized tribal personnel and partners (e.g., internal governance documents).

Survey - a public facing form that anyone can use and submit information/observations without the app (i.e., posting a link on Facebook, or sending a link out in an email).

Section 9
REFERENCES

Walter, M., Kukutai, T. Carroll, S. and Lonebear-Rodriguez, D. (Eds) (2020) Indigenous Data Sovereignty and Policy. Routledge: London.

Appendix A. Disclosure Request Checklist

☐ Ensure that the disclosed data serves a clear and beneficial purpose for the tribal community.
☐ Limit the scope of data shared to the minimum necessary to fulfill the request.
☐ Apply anonymization techniques where possible to protect sensitive information.
☐ Conduct a risk assessment before approving high-sensitivity disclosures.
☐ Require periodic reviews of data-sharing agreements to ensure ongoing compliance.
☐ Establish clear consequences for misuse or unauthorized redistribution of tribal data.