**Data Governance Framework**

Data Governance Policy Manual

<NAME OF NATION>



Distributed on: Month DD, YYYY

Version: V1.0

Warranty Disclaimer

This document and all of the information it contains are provided "as is" without warranty of any kind, whether express or implied. All implied warranties, including, without limitation, implied warranties of merchantability, fitness for a particular purpose, and non-infringement, are hereby expressly disclaimed. We do not make any warranties about the completeness, reliability and accuracy of this information. Any action you take upon the information in this document is strictly at your own risk.

Limitation of Liabilities

Under no circumstances will the Mustimuhw Information Solutions Inc. be liable to any person or business entity for any direct, indirect, special, incidental, consequential, or other damages based on any use of this document, including, without limitation, any lost profits, business interruption, or loss of programs or information, even if the Mustimuhw Information Solutions has been specifically advised of the possibility of such damages.

For more information contact Mustimuhw Information Solutions Inc. at 778-403-5473.

© Mustimuhw Information Solutions Inc. March 2015. To be freely used by First Nations and mandated and owned First Nations owned organizations, with clear acknowledgement to source.

Table of Contents

Preface 6

Data Governance Decision Matrix 7

Data Flows 11

Inventory of Data Assets 12

Data Sensitivity Classification 14

Data Quality 20

Data Standards 23

Nation Member / Customer Registry 31

Change Management 33

Data Sharing and/or Linking 34

Awareness and Training 38

Research 41

Validating Job Descriptions 42

Monitoring Data Governance 48

Definitions 50

Document Versioning 50

Appendices 51

Data Flow Index – Template and Sample 52

Data Standard Template 54

Data Governance and Privacy and Security Awareness Training 55

Tracking Log 55

Confidentiality and Acceptable Use Agreement / Acknowledgement 56

Adhoc Information Sharing Tracking Log 59

# Preface

The Data Governance Framework has been developed with the vision that *“Our Nation governs and protects all Nation data and information, wherever it resides, supporting the needs of our Nation, communities, Nation Organizations, and Members, as well as the needs of the partners we collaborate with.”* ***[[1]](#footnote-1)***

The Framework is a collection of strategy, structure, legislation, policy and related tools. It will evolve and grow in iterative cycles of expansion and refinement as our needs and capacities change and grow over time.

This document contains the Data Governance policies, procedures where necessary, and tools that will be used to govern the Nation’s data.

Implementation Tip: If Panorama has been implemented in your Nation, this Framework will supersede the Privacy & Security policy implemented from that project. Therefore incorporate any procedures already applied in the health centre and then retire the Panorama P&S policies and implement this framework. Additionally other staff (e.g. Data Custodian(s)) or departments may have related policies/procedures that need to be absorbed into this framework and subsequently retired.

Note: This document is a supplementary portion to the Framework document – provisioned separately to make it easier to incorporate updates. The author and reader of this document are required to be familiar with the current Data Governance Framework document before applying or updating this document.

# Data Governance Decision Matrix

**Applicable To:** All types of data

**Approval Date:** [mmm/dd/yyyy]

**Approved By:** Nation Leadership

**Any Related factors:** none

**Purpose:**

The Data Governance Framework includes a set of accountability mechanisms that ensures there is evidence of accountability to our Nation Members, non-member clients/customers, Nation managers, and Nation partners. One of these mechanisms includes the creation and maintenance of a Decision Ledger, which is used to track decisions that affect the Data Governance Framework. In order to make decisions it is important to understand who is assigned the responsibility to put forward decision requests, who has the authority to make decisions and who is accountable to implement the decisions.

**Policy**

The following Decision Matrix must reflect every type of decision that is needed to support the Data Governance Framework. In the event that a decision is required but the decision type does not fall within the following table the Executive Steward / Chair would:

1. Seek approval of an amendment to this policy before a decision on the specific item can be initiated; or,
2. If time is of the essence the Executive Steward / Chair can seek a decision from the Nation Leadership in conjunction to requesting approval for an amendment to this policy.

In order to provide the Nation Leaders with the opportunity to fully understand and evaluate the best decision model for a given type of decision it is preferred that first option (i.e. option ‘a’) be exercised whenever possible.

| **Decision Matrix** |
| --- |
| Decision Type | Decision Requestor | Decision Approver | Implementation Accountabilities |
| Decision Matrix | Executive Data Steward / Chair | Nation Leadership | * Communication: Executive Data Steward
* Implementation:
* Primary: Data Stewards
* Secondary: Data Custodian, Data Steward Subject Leads, Nation managers, employees
 |
| Data Governance Framework – Vision | Executive Data Steward / Chair | Nation Leadership | * Communication: Executive Data Steward
* Implementation:
* Primary: Data Stewards
* Secondary: Data Custodian, Data Steward Subject Leads, Nation managers, employees
 |
| Data Governance Framework – Vision and Principles | Executive Data Steward / Chair | Nation Leadership | * Communication: Executive Data Steward
* Implementation:
* Primary: Data Stewards
* Secondary: Data Custodian, Data Steward Subject Leads, Nation managers, employees
 |
| Data Governance Framework – Governance Structure | Executive Data Steward / Chair | Nation Leadership | * Communication: Executive Data Steward
* Implementation:
* Primary: Data Stewards
* Secondary: Data Custodian, Data Steward Subject Leads, Nation managers, employees
 |

| Decision Type | Decision Requestor | Decision Approver | Implementation Accountabilities |
| --- | --- | --- | --- |
| Data Governance Framework – Accountability Mechanisms | Executive Data Steward / Chair | Nation Leadership | * Communication: Executive Data Steward
* Implementation:
* Primary: Data Stewards
* Secondary: Data Custodian, Data Steward Subject Leads, Nation managers, employees
 |
| Data Governance Framework – Data Governance Policy | Executive Data Steward / Chair | Nation Leadership | * Communication: Executive Data Steward
* Implementation:
* Primary: Data Stewards
* Secondary: Data Custodian, Data Steward Subject Leads, Nation managers, employees
 |
| Data Governance Framework – Privacy and Security Policy | Executive Data Steward / Chair | Nation Leadership | * Communication: Executive Data Steward
* Implementation:
* Primary: Data Stewards
* Secondary: Data Custodian, Data Steward Subject Leads, Nation managers, employees
 |
| Data Governance Framework – Legal Instruments | Executive Data Steward / Chair | Nation Leadership | * Communication: Executive Data Steward
* Implementation:
* Primary: Data Stewards
* Secondary: Data Custodian, Data Steward Subject Leads, Nation managers, employees
 |
| Data Governance Agreements and/or Information Sharing Agreements | Data Governance Board and Nation Manager(s) | Executive Data Steward | * Communication: applicable Data Steward(s)
* Implementation: applicable Nation Manager(s)
 |
| Compliancy Procedures | Data Governance Board | Nation Leadership | * Initiate: Executive Data Steward
* Include in implementation plan: Executive Data Steward
 |
| Compliancy Action Plans | Executive Data Steward / Chair | Nation Leadership | * Communication: Executive Data Steward
* Implementation:
* Primary: Data Stewards
* Secondary: Data Custodian, Data Steward Subject Leads, Nation managers, employees
 |
| Consent posters, pamphlets, and telephone scripts | Data Steward | Data Governance Board | * Poster Implementation: Data Steward
* Pamphlet and Telephone Script: Nation Manager
 |
| Business Continuity Plans | Data Steward | Data Governance Board | * Develop/maintain: Nation Manager and Data Steward
* Action Plans: Executive Data Steward and Nation Manager
* Implementation: Applicable Nation Manager
 |
| Access procedures | Data Custodian | Data Governance Board | * Communication: Executive Data Steward and Nation Manager(s)
* Implementation: Data Custodian
 |
| Access audit procedures | Data Custodian and Data Steward | Data Governance Board | * Communications: Executive Data Steward and Nation Manager(s)
* Implementation: Data Custodian and Data Stewards
 |
| Ministry of Health Software Conformance Standard | Data Steward and applicable Nation Manager | Executive Data Steward and Nation Manager | * Report submission to Ministry of Health: Executive Data Steward
 |

For data stored externally the Data Governance and Information Sharing Agreement between our Nation and the other Party must specify a decision matrix.

# Data Flows

**Applicable To:** All types of data

**Approval Date:** [mmm/dd/yyyy]

**Approved By:** Nation Leadership

**Any Related factors:** none

**Purpose**

Understanding holistically where data flows provides our Nation with a better understanding of where the data is stored and how it is connected. Furthermore, this is the starting point for the Data Governance Board to create and maintain the Data Asset Inventory Log to ensure we are governing all of our data. Data Flows are captured in Data Flow Diagrams with supporting details documented in the Data Asset Inventory Log (refer to next section). Together, these tools aid in identifying overlaps of data, data dependencies, linkages, and redundancy. The Data Flow Diagrams will grow organically as we gain a better understanding of how we collect and use our data and whom we disclose it to.

**Policy**

Using the Data Flow Index in the appendix each Data Steward must develop and maintain Data Flow Diagrams for the departments that they support. These diagrams will represent:

* Data stored internally: who collects/uses the data; what data is disclosed to other departments/entities within our Nation and Nation Organizations; and what data is disclosed to other Parties
* Data stored externally: who collects/uses our data; what data do they disclose to our Nation and Nation Organizations; and what data do they disclose to other Parties
* Identification of the data sector (Corporate, Cultural, Human Related, or Land and Resources)
* Descriptions of current identifiers and/or attributes that uniquely identify the data

**Roles and Responsibilities**

|  |  |
| --- | --- |
| **Role** | **Responsibilities** |
| Executive Data Steward | Ensuring the Data Flow Diagrams are created/maintained |
| Data Stewards | Creating/maintaining the Data Flow Diagrams |
| Data Steward Subject Leads | Contributing to the development of the Data Flow Diagrams and validating them with the Nation manager(s). |

# Inventory of Data Assets

**Applicable To:** All types of data

**Approval Date:** [mmm/dd/yyyy]

**Approved By:** Nation Leadership

**Any Related factors:** This policy aligns with the Ministry of Health Software Conformance Standards

**Purpose**

Having an inventory of the Nation Data regardless of where it is stored is integral to governing the data and having involvement in owning and controlling it. This inventory will aid in identifying priorities for implementing the Data Governance Framework, and maintaining data governance. It describes the methods that will be used to track Data Assets and important characteristics/specifications of these assets.

**Policy**

The Data Asset Inventory Log must be created to include all data stored internally and externally. It must include information on the original data and any copies that are made of it.

At a minimum, the Log must be updated and validated annually by the Data Stewards and reviewed/approved by the Data Governance Board.

**Roles and Responsibilities**

|  |  |
| --- | --- |
| **Role** | **Responsibilities** |
| Executive Data Steward | Ensuring the Data Asset Inventory Log is being maintained |
| Data Stewards | Creating/maintaining the Data Asset Inventory Log |
| Data Steward Subject Leads | Contributing to the development of the Data Asset Inventory Log and validating them with the Nation manager(s). |

**Procedures**

Each respective Data Steward creates/updates records in the Data Asset Inventory Log.

The Executive Data Steward/Chair includes an annual agenda item that requires the Data Governance Board to review the Data Flows, Data Asset Inventory Log and Data Storage Inventory Log. The Board reviews these logs to look for any omissions and issues and resolves these accordingly.

The Data Asset Inventory Log must track the following:

* All Nation data regardless of where it is stored or who manage it
* Name of the corresponding Data Flow from the Data Flow Diagram
* Data description: including data type, data sensitivity classification, and related programs/services
* Current data storage details: format (e.g. electronic, paper), location, data backup requirements
* If it is internal data and it is stored electronically it must identify the Data Storage that is used to store the data; and the Data Storage Asset must be identified on the Data Storage Inventory Log
* Specify whether the data is mission critical
* For mission critical data specify how often the data changes and define how frequently the data must be backed-up
* Data retention requirement (refer to the Privacy and Security Policy – Data Retention and Disposal).
* Specify whether the data is the original data or a copy of the original, or both
* Data Governance details: (i.e. name of current Data Steward and identify required changes; name of current Data Custodian and identify required changes; special notes, name of the Data Steward Subject Lead, history of changes, etc.)
* Specify whether the data is protected with a business continuity plan, the location of the Business Continuity Plan and date last reviewed.
* Data sharing/linking requirements; identify any formal/informal arrangements/agreements if they exist
* Known data quality issues and plans to resolve, if any
* Degree of alignment with our Data Standards Policy
* Status of Privacy and Security Impact Assessment if one exists including information on any known privacy/security risks and supportive action plans currently in place, if any
* Known data governance or privacy/security incidents and supportive action plans, if any
* Date record was created/updated and name of person who edited the record, and date Governance Board approval date

# Data Sensitivity Classification

**Applicable To:** All types of data

**Approval Date:** [mmm/dd/yyyy]

**Approved By:** Nation Leadership

**Any Related factors:** This policy aligns with the Ministry of Health Software Conformance Standards

**Purpose**

Understanding the level of sensitivity associated with the data provides guidance on how the data governance and privacy and security policies should be applied to adequately and appropriately protect data. It aids in determining the priorities for conducting privacy and security impact assessments, and assists in reviewing data governance or privacy breach incidents.

**Policy**

A classification is assigned to provide an understanding of what the potential impacts could be if the data were lost, corrupted, stolen, or disclosed to an unauthorized person(s)/Party.

Each data asset must be assessed to determine the specific sensitivity classification. When assessing the classification always error on the side of caution.

A situation may arise where several different kinds of data are stored in the same location but their assessed classification is different, or the data is a cross section of data sector and have different assessed classifications. In these situations, the data sensitivity classification must align to the highest classification level assigned to any of the individual pieces of data.

Aggregated de-identified data assets must be classified to the level of their corresponding identified data asset because there is the potential that the data could be either re-identified or parties could infer that the data is associated to a specific individual or circumstance.

The classification assigned to the data must be recorded in the Data Asset Inventory Log. This Log must be updated and validated at least annually.

The following table provides a description of each classification for each of the four data sector identified in our Data Governance Framework; examples of the privacy and security safeguards that must be in place, and examples of the data. The tables also provide examples of data that may be associated to each classification.

|  |
| --- |
| **Data sector: Corporate** |
| Sensitivity Classification | Privacy and Security Safeguard Examples | Examples of Data |
| **Low** – could cause no injury/harm or very little injury/harm, such as minor embarrassment | Generally no need to have any safeguards in place | Approved meeting agendas including the names of individuals attending the meeting. |
| **Medium** – could cause injury or harm to the Nation or legal entity/entities | * Limited access for authorized Staff that need access (e.g. Staff that support payroll).
* Privacy and security safeguard example: locked filing cabinet with policy and procedures for managing locks/keys and audit controls, or information management system controlled by unique User ID and Password policies/procedures that can be audited
 | Approved meeting minutes, approved financial budgets |
| **High** – could cause extremely serious personal injury or harm such as illness, increased health risks because the individual does not seek access to health care services, suicide, social hardship, loss of employment causing economic hardship, negative impact to personal relationships, etc. | * Limited access for authorized Staff using privacy principle of ‘need-to-know least privilege’
* Disclosed to another approved Party based on them accessing as required to support needs of the Nation
* Privacy and security safeguard examples: same as above with audit review procedures supported by a robust data governance framework including the application of all policies including assessments and monitoring
 | Unapproved meeting minutes, financial plan, or budgets. |

|  |
| --- |
| **Data sector: Cultural** |
| Sensitivity Classification | Privacy and Security Safeguard Examples | Examples of Data |
| **Low** – could cause no injury/harm or very little injury/harm, such as minor embarrassment | Generally no need to have any safeguards in place. | A dictionary of our language |
| **Medium** – could cause injury or harm to the Nation or legal entity/entities | * Limited access for authorized individuals/families
* Privacy and security safeguard example: Training received and a confidentiality agreement signed by all employees; and awareness training for all Members receiving services
 | Certain traditional practices/knowledge |
| **High** – could cause extremely serious injury, harm to delivery of services, suicide, social hardship, loss of employment causing economic hardship, negative impact to personal relationships, etc. | * Limited access for authorized Staff using privacy principle of ‘need-to-know least privilege’
* Disclosed to another approved Party based on them accessing as/when required to support needs of the Nation
* Privacy and security safeguard examples: same as above with audit review procedures supported by a robust data governance framework including the application of all policies, including assessments and monitoring
 | Certain protected/sacred knowledge – e.g. around traditional medicines.  |

|  |
| --- |
| **Data sector: Lands and Resources** |
| Sensitivity Classification | Privacy and Security Safeguard Examples | Examples of Data |
| **Low** – could cause no injury/harm or very little injury/harm, such as minor embarrassment | Generally no need to have any safeguards in place | A formal designation of our lands or resources |
| **Medium** – could cause injury or harm to the Nation or legal entity/entities | * Limited access for authorized Staff that needs access
* Privacy and security safeguard example: locked filing cabinet with policy and procedures for managing locks/keys and audit controls, or information management system controlled by unique User ID and Password policies/procedures that can be audited
 | Approved water contamination report: contamination, impact assessment, action plan, and outcome. |
| **High** – could cause extremely serious personal injury, harm such as illness or increased health risks because the individual does not seek access to health care services, suicide, social hardship, loss of employment causing economic hardship, negative impact to personal relationships, etc. | * Limited access for authorized Staff using privacy principle of ‘need-to-know least privilege’.
* Disclosed to another approved Party based on them accessing as/when required to support needs of the Nation
* Privacy and security safeguard examples: same as above with audit review procedures supported by a robust data governance framework including the application of all policies, including assessments and monitoring
 | Unproven water contamination that affects all individuals living on our land |

|  |
| --- |
| **Data sector: Human Related** |
| Sensitivity Classification | Privacy and Security Safeguard Examples | Examples of Data |
| **Low** – could cause no injury/harm or very little injury/harm, such as minor embarrassment | Generally no need to have any safeguards in place | First name, middle name, and last name of an individual, and ageFor example, perhaps the individual’s middle name is an embarrassment. If disclosed it would not likely cause injury/harm to the person but it may cause minor embarrassment. |
| **Medium** – could cause personal injury or harm such as identity theft | * Limited access for authorized Staff that needs access
* Privacy and security safeguard example: locked filing cabinet with policy and procedures for managing locks/keys and audit controls, or information management system controlled by unique User ID and Password policies/procedures that can be audited
 | Same as above, plus the individual’s SIN#, birth date, home address and phone number, personal cell #.(Note, excludes bank information for situations where there are automatic payroll deposits.) |
| **High** – could cause extremely serious personal injury, harm such as illness or increased health risks because the individual does not seek access to health care services, suicide, social hardship, loss of employment causing economic hardship, negative impact to personal relationships, etc. | * Limited access for authorized Staff using privacy principle of ‘need-to-know least privilege’
* Disclosed to other health care providers based on them accessing as/when required to support the health care needs of the client or to protect the health of a population (e.g. preventing or management of a communicable disease).
* Privacy and security safeguard examples: same as above with audit review procedures supported by a robust privacy and security framework that includes an assessment and monitoring process
 | Client`s health file; payroll information including bank information for payroll deposits. |

For data stored externally the Data Governance and Information Sharing Agreement between our Nation and the other Party must specify the data sensitivity classification.

**Roles and Responsibilities**

|  |  |
| --- | --- |
| **Role** | **Responsibilities** |
| Executive Data Steward | Ensuring the data is classified |
| Data Stewards | Responsible for facilitating the classification assessment and validating it with the Nation manager(s). |
| Data Steward, Subject Leads | Responsible for facilitating the classification assessment and validating it with the Nation manager(s). |

# Data Quality

**Applicable To:** All types of data

**Approval Date:** [mmm/dd/yyyy]

**Approved By:** Nation Leadership

**Any Related factors:** This policy aligns with the Ministry of Health Software Conformance Standards

**Purpose**

The quality of Nation data is paramount to providing accurate information and knowledge that will support charting our path. Quality is achieved when we know that the data can be used for operational needs, decision-making, and planning; and that it represents the real world. The components that make up data quality are: completeness, validity, consistency, accuracy and timeliness. This policy outlines how these components will be achieved.

Our Nation recognizes that we have a legal and ethical responsibility to manage information, including data quality, in a matter that promotes confidence and assurance with our members, clients, and partners. In turn we expect our Staff, members, clients, and partners to support data quality.

**Policy**

The cost to achieve an exact level of data quality for existing data can be expensive. Therefore, data quality procedures must always be applied at the point of recording and storing original data.

Existing data must undergo a Data Quality Assessment and reviewed/approved by the Data Governance Board.

Applying data cleansing routines (manual or systematic) to existing data for the purpose of maximizing data quality must be undertaken when there is sufficient value to the Nation.

For data stored internally it is expected that the cost of data cleansing must be a one-time activity that will be financed via the Nation or a specific nation-based project. For data stored externally it is anticipated that the ownership of the problem/solution will vary therefore the financial supporter will also vary. Any data cleansing routines must be accompanied by new procedures so that the cleansed data and new data are aligned and no further data cleansing would be required.

Each Nation Manager is accountable to ensure that newly created data is entered and updated that ensures the data is accurate and complete. Supervisor or delegate must monitor new Staff for six (6) months and an annual review must be performed for all Staff. Any issues resulting from these reviews must be documented and an action plan put into place to remediate the issue(s).

Implementing new services, computer-based information management tools, manual or systematic data exchanges/interfaces require a Data Quality Impact Assessment to be completed and reviewed/approved by the Data Governance Board before implementation can proceed.

Data obtained from a 3rd party or disclosed to a 3rd party must be supported by a Data Quality Impact Assessment form that has been completed and reviewed/approved by the Data Governance Board before disclosure can proceed.

The following table provides a set of guidelines to determine data quality.

|  |
| --- |
| **Quality** |
| Mandatory data elements must be identified and recorded for each record in the data set. |
| The Data Standards policy must be applied appropriately to each record. |
| Users or clients responsible for recording the data have a consistent understanding of each data element and capture it consistently, completely, and accurately. |
| If there is more than one data set that is being used to develop a report or link data the following must be considered:* The data standards have to be consistent across each data set.
* The reference data has to be consistent across each data set.
* The meaning of linked data has to be the same (i.e. last name is only the last name, it cannot be the first, middle, last name in one data set and the last name in another data set).
* Determining whether or not other records exist elsewhere but are not part of the combined set of data. This then determines the level of completeness that exists.
* Determine whether or not the meaning of the data change after it is linked or aggregated such that it degrades the value of the information derived from the data.
* The data must be relevant to the current period (i.e. do not merge or link old health data with new housing data).
 |
| The data must be accurate. |
| Inaccurate data must be corrected in a timely fashion. |
| A history of the changes must be maintained when the data element is used to make a decision (i.e. service delivery, operational, planning, etc.) or used in a report. |
| All records must include the name of the user that created/updated/deleted the record and the date and time the record was created/amended. For system routines that add/update data the name of the user is the system or some other agreed upon and documented value. |
| A data element that contains data cannot be used in a new way without the approval of the data governance board. |

For data stored externally the Data Governance and Information Sharing Agreement between our Nation and the other Party must specify roles and responsibiltiies

**Roles and Responsibilities**

|  |  |
| --- | --- |
| **Role** | **Responsibilities** |
| Executive Data Steward | Providing guidance so data quality can be maintained |
| Data Stewards | Developing Data Quality Assessments, developing recommendations and validating Data Quality with the Nation manager(s). |
| Data Steward, Subject Leads | Developing Data Quality Assessments, developing recommendations and validating Data Quality with the Nation manager(s). |
| All Staff | Maintain data quality and bring forward any concerns/issues/recommendations to their Nation manager, Data Steward Subject Lead, or Data Steward. |

# Data Standards

**Applicable To:** All types of data

**Approval Date:** [mmm/dd/yyyy]

**Approved By:** Nation Leadership

**Any Related factors:** This policy aligns with the Ministry of Health Software Conformance Standards

**Purpose**

To provide our Nation with the opportunity to access and govern Nation data, the data must be structured to support our requirements to deliver services, provide reports that will inform our Nation, conduct research in support of our Nation, etc. To achieve this some of the data must be structured using a consistent set of data collection rules. Furthermore understanding who is the primary data collector must also be defined in order to understand who holds the source of truth. This policy outlines the data structure for each data type including the unique identifiers, data rules and data collection requirements.

**Policy**

Data Standards are to be developed for the purpose of:

* Defining how the data will be uniquely identified
* Where applicable aligning a common business understanding between departments and partners to support the implementation of data standards
* Where applicable aligning data collection tools (e.g. forms, computer-based tools, interfaces, etc.) to support data governance of Nation Data regardless of where the data resides
* Where applicable aligning data elements when the same data is stored in multiple data domains
* Identify the ‘source-of-truth’ for data that is stored in multiple data domains
* Implement, validate, and monitor data quality

To maintain data integrity a Data Standard cannot have more than one meaning.

Each Data Standard must be expressed using the Data Standard Template located in the Appendix.

For data stored externally the Data Governance and Information Sharing Agreement between our Nation and the other Party must specify these standards and identify any other standards.

In addition to our Nation defining specific data standards we recognize that an individual may have specific identifiers and/or an organization is supporting programs/services that requiring identifying our First Nations Members or Aboriginal Customers. The following is a guideline that is intended to support the ongoing development of the Nation Data Standards.

* AANDC operates an identifier for each Band and each registered Band member (also referred to as INAC or status number).

Recording our Nation’s Band # or a Member’s Band # is mandatory for our Nation’s Member Registry process; and must be recorded for all Nation delivered services.

The AANDC # may only be collected/used by Nation delivered services. Other service delivery providers must receive approval by our Data Governance Board to collect/use a member’s AANDC number.

Our Nation will use the AANDC # to uniquely identify our Nation Members for the purpose of delivering services, approved Nation-based reporting, approved Nation-based research. Any other purposes must receive the approval of our Data Governance Board.

We must retain history associated with changing a Band # or a Members Band #.

* Other identifiers (e.g. federal or provincial identifiers such as the Driver’s License #, Provincial Health Number, etc.) assigned by other organizations must be collected and used only when a Member/Customer is receiving services that require the need to collect/use the identifier. Each service area must present the identifier requirements to the Data Governance Board for review/approval. Once approved the identifier must be included in this policy.
* The provincial government has defined the Aboriginal Administrative Data Standard (AADS). Our Data Governance Board will support and collaborate with provincial and federal agencies in identifying our Nation Members and the Aboriginal population in general to achieve the goals of the BC Provincial Government Aboriginal Data Standard (AADS). This includes refining the AADS and linking/sharing data to support the needs of our Nation. The following list identifies the current standards for the AADS and specifies how our standards may alignment to the AADS standards.
1. Identifying as ‘Aboriginal’ (values: yes, no, or null) – mandatory for those government agencies implementing AADS

*Alignment: Our Data Governance Framework will support provincial agencies recording this data element on the proviso that there is a specific Aboriginal program in place and agency provides Cultural Sensitivity Training to employees prior to the employee collecting the data.*

1. If ‘yes’ to the above data element, specify the Aboriginal Group (values: First Nations, Inuit, and Metis) (mandatory for those agencies implementing the standard)

*Alignment: Our Data Governance Framework will support provincial agencies recording this data element on the proviso that: there is a specific First Nations program in place; the agency provides Cultural Sensitivity Training to employees prior to the employee collecting the data; the individual’s membership name (i.e. our Nation’s name); and the agency has a signed Data Governance and Information Sharing Agreement with our Nation*

1. First Nations Status Indicator – optional

*Alignment: Our Data Governance Framework will support provincial agencies recording this data element on the proviso that: there is a specific First Nations program in place; the agency provides Cultural Sensitivity Training to employees prior to the employee collecting the data; the individual’s membership name (i.e. our Nation’s name); and the agency has a signed Data Governance and Information Sharing Agreement with our Nation*

1. First Nations On-reserve Indicator – optional

*Alignment: Our Data Governance Framework does not support this part of the AADS standard.*

*What is recognized is when a shared service delivery model is provided there is a need to identify as part of an individual’s Address whether the individual is currently living on-reserve. Refer to the standard above called ‘Data Element – Address’.*

**Procedures**

To develop the initial set of Standards the Data Stewards will review the data dictionaries to:

* Identify and draft Data Standards and put them forward to Nation Managers for review and present for review/approval to the Data Governance Board
* Identify the unique identifiers
* Determine cross-pollination of data elements across the multiple data sets and establish the ‘source-of-truth’
* Identify any data quality risks and establish recommendations
* Review data collection tools and make recommendations to the Nation Managers and partners to align
* Advocate for support and implementation of the Data Standards both internally and externally

The following tables identify the data standard of each respective data element.

Data Standards for Corporate types:

*The standards will be completed as part of working with the Data Governance demonstration sites.*

Data Standards for Cultural types:

*The standards will be completed as part of working with the Data Governance demonstration sites.*

Data Standards for Land and Resources types:

*The standards will be completed as part of working with the Data Governance demonstration sites.*

Data Standards for Human Related types:

*The standards will be completed as part of working with the Data Governance demonstration sites.*

|  |
| --- |
| **Data element: Alignment to the Provincial Aboriginal Administrative Data Standard** |
|  |

**Roles and Responsibilities**

|  |  |
| --- | --- |
| **Role** | **Responsibilities** |
| Executive Data Steward | Working with partners to assess their requirements and update the AADS or our standards accordingly. |
| Data Stewards | Analyze the requirements and provide recommendations to the Data Governance Board; provide input into the Cultural Sensitivity Training. |
| Data Steward Subject Leads | Support the Data Stewards in the analysis of the requirements. |
| Nation Managers | Support the Data Stewards in the analysis of the requirements. |
| All Staff | Report challenges and/or recommendations to the Data Governance Board. |

# Nation Member / Customer Registry

**Applicable To:** All types of data

**Approval Date:** [mmm/dd/yyyy]

**Approved By:** Nation Leadership

**Any Related factors:** None

**Purpose**

Governing Human Related data is dependent on having an accurate list of our Nation Members and customers and their key attributes such as family relationships, contact information, AANDC registration, etc. A Nation Member/Customer Registry that supports current technology provides the ability for us to link data for the purpose of planning and delivering services, assessing nation wellness, providing accurate nation-based reporting, and building a stronger future. The Nation Member/Customer Registry is the cornerstone and source of truth that our Nation and partners would use to manage and link our Nation’s Human Related information. This policy provides a foundation for establishing the Nation Member/Customer Registry.

**Policy**

The Nation Member / Customer Registry must support:

* Data must reside in Canada
* Data must be governed by our Nation
* Data must be stored electronically
* Support system-to-system interfaces to allow all nation-based service providers to exchange data in real-time
* Support system-to-system interfaces and synchronization processes to allow external service providers to exchange data in real-time
* Support system-to-system synchronization processes between our registry and AANDC’s registry, provincial registries where applicable, and First Nations Health Authority
* Manage member/customer Consent for Disclosure approvals (e.g. consent to disclose specific human related data elements for nation-based reporting; consent to disclose specific human related data elements for a specific research initiative, etc.)
* Provide an electronic audit trail for data collection, use, and disclosure
* Other requirements as defined by the Data Governance Board and the Nation operational manager

**Roles/Responsibilities**

|  |  |
| --- | --- |
| **Role** | **Responsibilities** |
| Data Governance Board | Advocate and promote the acquisition of the Member/Customer Registry system. |
| Data Stewards | Support the development of the data requirements. |
| Data Steward Subject Leads | Support the development of the data requirements. |
| Nation Manager Responsible for Membership | Plan, budget, and manage the registry; define functional and data requirements, test and support the solution. |
| Other Nation Managers | Work to interface with the registry. This includes planning, budgeting, identifying opportunities and requirements, implementing and supporting the solution. |

# Change Management

**Applicable To:** All types of data

**Approval Date:** [mmm/dd/yyyy]

**Approved By:** Nation Leadership

**Any Related factors:** None

**Purpose**

Making changes to data may impact related activities (e.g. reporting, service delivery, etc.). Therefore our Nation must consider the holistic impacts of changing our data.

**Policy**

The Data Governance Board must support proactive and reactive change management activities in the spirit of supporting the Data Governance Framework (e.g. changing data to improve data quality or apply the data standards, etc.).

Any changes affecting the Framework must be brought forward to the Data Governance Board. Where possible, this should be done as a planning activity so that the Board can assess the impact and provide guidance.

For data stored externally the Data Governance and Information Sharing Agreement between our Nation and the other Party must specify how changes will be reviewed/approved.

**Roles/Responsibilities**

|  |  |
| --- | --- |
| **Role** | **Responsibilities** |
| Data Governance Board | Assessing the impact of the change and providing recommendations. And where applicable updating the Data Governance Framework. |
| Data Stewards | Assessing the impact of the change, drafting recommendations, and bring the issues forward to the Data Governance Board. |
| Data Steward Subject Leads | Assessing the impact of the change, drafting recommendations, and bring the issues forward to the Data Governance Board. |
| Nation Managers | Considering the Data Governance Framework when they are planning changes and for consulting with the Data Governance Subject Lead and/or Data Steward. Implementing Data Governance Board recommendations. |

# Data Sharing and/or Linking

**Applicable To:** All types of data

**Approval Date:** [mmm/dd/yyyy]

**Approved By:** Nation Leadership

**Any Related factors:** This policy aligns with the Ministry of Health Software Conformance Standards

**Purpose**

Our Nation recognizes that Nation Data may be stored/managed by a 3rd party, which may result in a requirement to access/collect the data from the 3rd party. Additionally our Nation works with partners to support the delivery of services that may be dependent on sharing or linking data (e.g. health care and social services, water management, etc.). Extending governance over Nation Data stored externally must be done in a collaborative way that incorporates our Data Governance Framework and operational needs and considers the requirements of our partners. This collaboration must be formal in nature and ensure that all parties have a clear understanding of the collective expectations and the collaboration process must demonstrate transparency for Nation Members, clients/customers, Staff, and Nation Leaders. This policy outlines the methods that must be used to formalize governance over data stored externally and internally between departments or disclosed to / collected by with another party.

**Policy**

A Data Governance and Information Sharing Memorandum of Understanding must be in place to support data sharing between internal operational departments. (Note: refer to the Privacy and Security policies and procedures for additional requirements that must be met before data can be exchanged between departments.)

A Data Governance and Information Sharing Agreement must be in place between the Nation and any external party who is storing, governing or managing our Nation’s data.

A Data Governance and Information Sharing Agreement must be in place between the Nation and any external Party prior to exchanging data with that party. (Note: refer to the Privacy and Security policies and procedures for additional requirements that must be met before data can be exchanged with another Party.)

Sharing Human Related information between departments or with an external Party requires one of the following authorized methods in place prior to sharing the data:

1. Legislative authority and an Information Sharing Agreement (ISA), or
2. Client / Guardian consent

These agreements must address all aspects of our Data Governance Framework and strike the correct balance to protect the interests of all stakeholders. They must also address the auditing methods that must be used to confirm that the terms of the Agreement are being adhered to.

In an emergent situation that requires the immediate sharing of personal information that doesn’t have one of the above mechanisms in place, the Staff must direct the request to the Nation manager or a regulated professional who is guided by their professional accreditation obligations (e.g. a nurse may be obligated to share the information to ensure a client receives the necessary health care that would prevent harm to the client). An emergent situation may be considered to be:

* Where sharing of Human Related information is clearly in the interests of the client/ guardian and consent cannot be obtained in a timely way.
* Where sharing of Human Related information is necessary for medical treatment of the individual and the individual is either unable to give consent or does not have the legal capacity to give consent.

If this situation occurs on a regular basis, every effort must be made to establish a Data Governance and Information Sharing Agreement. To determine if there is a regular occurrence, the Human Related Data Steward would:

* Work with the Manager to direct Staff to track these emergent information-sharing events associated with sharing personal information using the ‘Adhoc Information Sharing Tracking Log’
* The Human Related Data Steward conducts a review of the log and works with the applicable Manager to identify the requirement for new Data Governance and Information Sharing Agreements for events that are recurring.

**Roles/Responsibilities**

|  |  |
| --- | --- |
| **Role** | **Responsibilities** |
| Data Governance Board | Pursue data governance and information sharing agreements based on the findings of the log. |
| Data Stewards | Assess the log and provide recommendations to the Data Governance Board. |
| Data Steward Subject Leads | Support the logging of adhoc information sharing events in the applicable log and work collaboratively to identify recurring events of adhoc information sharing. |
| Nation Managers | Support the logging of events in the log and reporting findings to the Data Steward. |

**Procedures:**

This is an optional procedure that is implemented as/when the Executive Data Steward, Human Related Data Steward, Data Steward Subject Lead, or Nation manager determine it is necessary.

An Adhoc Information Sharing Tracking Log is used to record events when data is shared between Nation Organizations/departments without an approved data sharing agreement in place.

The following procedure is performed by the Human Related Data Steward.

1. Using the applicable Appendix located within this document, insert the Start Date, print the log.
2. Work with the Manager to determine appropriate location(s) where Staff will use the log. Note, a log can be placed in more than one place. Once the log(s) is positioned the Steward records where the log(s) is located and makes an entry in their calendar to pick up the logs on a monthly or quarterly basis.
3. Request the applicable Manager to instruct Staff to use the log. Note, it is preferred that Staff record the events the same business day that they disclose the information. The Manager is accountable to instruct their Staff accordingly; and monitor its use.
4. On a monthly or quarterly basis the Steward picks up the any log sheets that have events recorded. A copy is provided to the Manager and the original is retained by the Steward.
5. The Steward reviews the log and makes recommendations to the Data Governance Board and in turn the Data Governance Board creates action plans accordingly. Recommendation considerations may be:
	1. Verification of adherence to our Data Governance Framework.
	2. Verification that our Members and customers are made aware of unauthorized information sharing events pertaining to their personal information.
	3. Verification that our Members and customers are aware of our consent model.
	4. Verification that Data Governance and Information Sharing Agreements are being developed and managed as required and appropriate.
	5. Overall verification of who is accountable / responsible for applying the Data Governance Framework policies and procedures.
	6. If necessary enhancing training and communication amongst our Staff (employees and contractors).

# Awareness and Training

**Applicable To:** All types of data

**Approval Date:** [mmm/dd/yyyy]

**Approved By:** Nation Leadership

**Any Related factors:** This policy aligns with the Ministry of Health Software Conformance Standards

**Purpose**

Our Staff and the Staff of 3rd parties who store/maintain Nation Data need to be aware of our Data Governance Framework in everything they do. Conducting Data Governance training raises and maintains awareness. This policy outlines the training requirements.

**Policy**

All Staff (part-time and full-time employees and contractors), who enter into our facilities and have access to Nation Data, must complete Data Governance and Privacy Awareness Training prior to accessing the facility. For Human Related data stored on paper, the training must be completed prior to issuing keys or access codes to the physical location; For Human Related data stored electronically, the training must be completed prior to allowing the User Accounts to be used to access the data. In the case of someone who does not have access to Nation Data but has access to our facilities, the training may be conducted within 5 business days of being employed by our Nation Organization(s).

All Staff must complete a Data Governance and Privacy Awareness Training refresher session on an annual basis or when directed by the Executive Data Steward.

A Data Governance and Privacy Training Tracking Log must be kept to prove Staff training was completed. At a minimum it must include the following:

* The name of the trainee
* The name of the training materials, including version
* The date training was completed
* The name of the person who verified training was completed
* The target date for the next training session

Any Staff members who have access to Nation Data at the time this policy is approved must receive Data Governance and Privacy Awareness Training within two (3) months of approving this policy.

For data stored externally the Data Governance and Information Sharing Agreement between our Nation and the other Party must specify equivalent details.

**Roles and Responsibilities**

|  |  |
| --- | --- |
| **Role** | **Responsibilities** |
| Data Governance Board | Approve awareness and training materials. |
| Data Stewards | Develop awareness and training materials. Implementation of the procedures outlined below. |
| Nation Managers | Maintain the Data Governance Awareness Tracking Log |

**Procedures: Data Governance Awareness Tracking Log**

This procedure describes how our Nation Organizations must deliver and track the delivery of our Data Governance Awareness training.

The Data Governance Awareness Training Tracking Log must be developed and managed by each Data Steward as follows:

1. Copy the document entitled ‘Data Governance Awareness Tracking Log’ from tand set the version to 1 (i.e. one).
2. Store the log electronically in a secure location only accessible by the Data Governance Board.
3. Record the name of each current Staff member (employees and contractors).
4. Executive Data Steward must arrange for the applicable Data Steward to be advised of the onboarding of any new Staff members.
5. Data Steward works with the Nation Managers to deliver Data Governance Awareness Training to all current Staff and to new Staff. As part of training delivery the Data Steward facilitates Staff to review the Confidentiality and Acceptable Use Agreement form (see Appendix) and seeks to have each Staff member sign the agreement. The log is then updated.

If a Staff member does not sign the agreement the Data Steward is to immediately advise the Nation Manager and Executive Data Steward. The Nation Manager is required to remove any and all access privileges until such time the issue can be resolved to the liking of the Executive Data Steward.

1. On a quarterly basis the Data Steward must validate that the log is accurate/complete with the Nation Manager(s).
2. The Data Steward must deliver training (see Appendix) on an annual basis. This arrangement is to be coordinated by the Data Steward and Nation Manager. Once delivered the Data Steward must receive a signed updated Confidentiality and Acceptable use Agreement from each Staff Member. The log is then updated.

If a Staff member does not sign the agreement the Data Steward is to immediately advise the Nation Manager and Executive Data Steward. The Nation Manager is required to remove any and all access privileges until such time the issue can be resolved to the liking of the Executive Data Steward.

1. If training cannot be delivered it is to be classified as a Privacy Breach. The Privacy Breach policy and procedures are then applied.

The Confidentiality and Acceptable Use Form must include affirmation that a Staff member is in good standing if they are in a profession governed by a College; and the Staff member must commit to notifying our organization if they are no longer in good standing and they agree to not access data if they are not in good standing.

# Research

**Applicable To:** All types of data

**Approval Date:** [mmm/dd/yyyy]

**Approved By:** Nation Leadership

**Any Related factors:** None

**Purpose**

(To be developed during Demonstration Site implementations.)

**Policy**

(To be developed during Demonstration Site implementations.)

**Roles and Responsibilities**

|  |  |
| --- | --- |
| **Role** | **Responsibilities** |
|  |  |
|  |  |
|  |  |

# Validating Job Descriptions

**Applicable To:** All types of data

**Approval Date:** [mmm/dd/yyyy]

**Approved By:** Nation Leadership

**Any Related factors:** Ministry of Health Software Conformation Standards

**Purpose:**

All Staff have a role in ensuring Nation data is governed, managed, and protected in accordance to the Data Governance Framework. This policy outlines how Staff are made aware of their related responsibilities.

**Policy**

Nation Leaders are required to describe the Data Governance Framework duties and responsibilities in Nation Leadership and Nation Manager job descriptions.

Nation Managers are required to describe the Data Governance Framework duties and responsibilities in the job descriptions for all Staff (Staff includes paid employees and contractors).

The following table provides a guideline of the roles/responsibilities:

|  |  |
| --- | --- |
| Nation Leaders | * Understand the Data Governance Framework and support its implementation and maintenance of the framework
* Support the Data Governance Board
* Assign roles to fulfill the Data Governance Board and support team members
* Review and upon agreement approve the Data Governance Framework, implementation plans, decision requests, change management, and breach investigation action plans. Where agreement cannot be provider Nation Leaders must provide supportive guidance and direction to the Data Governance Board
* Report any potential privacy breach incidents
* Identify data governance requirements to the Data Governance Board
* Ensuring all Leadership job descriptions include these roles/responsibilities
* Consider data governance and protection of Nation data in the process of considering any changes to Nation data or processes affecting Nation data
* Protect Nation data against unauthorized access, theft, and corruption
* Assist in ensuring Nation data is governed by our Nation
* Lead Privacy Breach Investigation when the breach may involve a Data Steward
 |
| Executive Data Steward and Chair of the Data Governance Board  | Refer to the Data Governance Framework document – section entitled ‘Data Governance Board Roles and Responsibilities’ |
| Data Steward |
| Data Custodian | Refer to the Data Governance Framework document – section entitled ‘Support Team Members Roles and Responsibilities’ |
| Data Steward Subject Leads |
| Nation Managers | * Understand the Data Governance Framework and implement policies/procedures within the scope of their area of management
* Support the Data Governance Board
* Assigning Data Steward Subject Leads as required and supporting skill development
* Ensure all Staff receive Data Governance Awareness training and sign a Data Governance Awareness and Confidentiality Agreement prior to accessing Nation data
* Work collaboratively with the Data Governance Board to implement and maintain the Data Governance Framework
* Co-lead the engagement of external parties to acquire Data Governance and Information Sharing Agreements wherever Nation data is stored externally or shared with external parties
* Participate in the development of procedures for assigning access to Nation data using the principle of ‘need to know’ and ‘least privilege’
* Conduct access audits
* Report any potential privacy breach incidents and participate in the investigation
* Identify data governance requirements to the Data Governance Board
* Validate Data Flow Diagrams and Data Inventory Asset Log
* Maintain data quality and bring forward concerns/issues/recommendations to the Data Governance Board
* Capture any unauthorized information sharing events and report them to the applicable Data Steward
* Manage and support the implementation of a central Nation Member / Customer Registry as per the applicable Data Governance Policy
* Ensuring all Staff job descriptions include applicable roles and responsibilities in context of the Data Governance Framework
* Implement data governance policies and report any challenges or change requirements to the Data Governance Board
* Consider data governance and protection of Nation data in the process of considering any changes to Nation data or processes affecting Nation data
* Protect Nation data against unauthorized access, theft, and corruption
* Assist in ensuring Nation data is governed by our Nation
* Delegate data governance roles/responsibilities by providing written direction to Staff. Written direction includes providing a high-level description of the role/responsibility in the job description and providing written instructions via memo or email to the specific incumbent. As/when staff changes occur the Nation Manager must ensure the new incumbent is aware of the written instructions.
* In collaboration with the Data Steward prepare compliancy reports (e.g. Ministry of Health Software Conformance Standard Report), prepare consent notifications, business continuity plans, and other duties as outlined in the Data Governance Framework.
 |
| All Staff | * Be aware and knowledge in our Nation’s Data Governance Framework, including Stewardship, data governance policies, and privacy and security policies
* Protect Nation data against unauthorized access, theft, and corruption
* Work collaboratively with the Data Governance Board and support team members in the implementation of our Nations’ Data Governance Framework
* Sign a Data Governance Awareness and Confidentiality Agreement prior to accessing Nation data
* Upon request support the development and implementation of Data Governance and Information Sharing Agreements
* Upon request support the development of data governance and/or privacy and security policies or procedures
* Upon request process access audits
* Report any potential privacy breach incidents and participate in the investigation to a member of the Data Governance Board or Nation manager
* Identify data governance requirements to the Nation manager or Data Steward Subject Lead
* Maintain data quality and bring forward concerns/issues/recommendations to the Data Governance Board or Nation Manager
* Capture any unauthorized information sharing events and report them to the Nation manager
* Support the implementation of data governance policies and privacy and security policies and report any challenges or change requirements to the Data Governance Board
* Consider data governance and protection of Nation data in the process of considering any changes to Nation data or processes affecting Nation data
* Protect Nation data against unauthorized access, theft, and corruption
* Assist in ensuring Nation data is governed by our Nation
 |

For data stored externally the Data Governance and Information Sharing Agreement between our Nation and the other Party must specify equivalent details.

**Roles and Responsibilities**

|  |  |
| --- | --- |
| **Role** | **Responsibilities** |
| Executive Data Steward | Support Nation Leaders and Managers in incorporating Data Governance roles and responsibilities into Staff job descriptions and contracts. |
| Data Stewards | Support Nation Leaders and Managers in incorporating Data Governance roles and responsibilities into Staff job descriptions and contracts. |
| Data Steward Subject Leads | Support Nation Leaders and Managers in incorporating Data Governance roles and responsibilities into Staff job descriptions and contracts. |
| Nation Leaders | Ensure applicable Data Governance roles/responsibilities are incorporated into job descriptions and ensure the incumbents are aware of these responsibilities. Update job descriptions based on approved changes. |
| Nation Managers | Ensure applicable Data Governance roles/responsibilities are incorporated into job descriptions and ensure the incumbents are aware of these responsibilities. Update job descriptions based on approved changes. |

**Procedures**

1. The Executive Data Steward must communicate to all Nation Managers the requirement to review and update all job descriptions as outlined in this policy and to seek the support of the Data Stewards as needed. This task is to be completed within one year. The Executive Data Steward must communicate with Nation Managers as/when future Data Governance changes occur that may affect job descriptions.
2. Nation Managers are to review all job descriptions and if required update the job descriptions to incorporate Data Governance roles/responsibilities as per this policy; and formally review the changes with each incumbent. This task must be completed within one (1) year of approval of this policy. Nation Managers are responsible to update job descriptions based as/when applicable changes to the Data Governance Framework occur.
3. Staff is required to support Nation Managers in updating their job descriptions and be aware of their job descriptions.
4. Data Stewards support Nation Managers in reviewing and if required amending job descriptions. Support means providing clarification and providing a copy of this policy. Support does not mean amending the job description as this is the role of the Nation Manager.

# Monitoring Data Governance

**Applicable To:** All types of data

**Approval Date:** [mmm/dd/yyyy]

**Approved By:** Nation Leadership

**Any Related factors:** None

**Purpose**

Understanding whether or not the Data Governance policies are being adhered to provide us with the opportunity to update the policies, increase awareness, and/or identify risks and action plans. This policy outlines a set of questions that need to be answered annually.

**Policy**

Data Governance and Privacy and Security must be assessed to validate that our Nation is compliant with the Data Governance Framework. Assessments must occur:

* One year after initial implementation of a new policy or procedure, and
* Every 3 years thereafter

The scheduling of the assessments must be included in the annual Data Governance Implementation and Management Plan.

The outcomes of the assessment, risk assessment, and action items must also be included Data Governance Implementation Plan.

Assessments must be performed by one of the following resources:

* Two Nation Members who are qualified but are not members of the Data Governance Board; or
* A qualified third party consultant provided there is no privacy risk by engaging the third party and/or conflict of interest. If this option is exercised a contract must exist between our Nation and the third party. This contract must be authorized by the Executive Data Steward and a Nation Leader.

The assessment procedures and tools must be reviewed/approved by the Nation Leadership. At a minimum the approved procedures and tools provided as part of this policy are to be used. Additional procedures and/or tools may be used to augment the assessment. The Data Governance Board must present alternative procedures and tools to the Nation Leadership for review/approval prior to using the proposed new procedure(s)/tool(s).

**Roles and Responsibilities**

|  |  |
| --- | --- |
| **Role** | **Responsibilities** |
| Executive Data Steward | Support Nation Leaders and Managers in incorporating Data Governance roles and responsibilities into Staff job descriptions and contracts. |
| Data Stewards | Support Nation Leaders and Managers in incorporating Data Governance roles and responsibilities into Staff job descriptions and contracts. |

**Procedures**

(To be developed as part of the next steps.)

# Definitions

Please refer to the definitions represented in the Data Governance Framework primary document.

# Document Versioning

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Date** | **Author** | **Version** | **Change Reference** | **Reviewed By** |
| Mar 31 2015 | Mustimuhw Information Solutions Inc. | V0 (Template) | Initial template document | n/a |

# Appendices

## Data Flow Index – Template and Sample

| **High Level Data Group Descriptor** | **Unique Identifiers:** | **Primary Data Sector:** | **Includes other Data Sectors:** | **Sensitivity Classification:** | **Created by:** | **Used by:** | **Disclosed to:** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| e.g. Band Council Agenda and Supporting Materials, excluding minutes | Community Name(s) | Corporate | All | High | Staff in all departments | Staff in all departments; and applicable special guests | Authorized special guests |
| Band Council Minutes | Community Name(s) | Corporate | All | High | Staff in <dept name>Band CouncilExternal Special Guests | Same as created by | ---- |
| Financial Reports | Community Name(s) | Corporate | All | High | Staff in <dept name> | Same as created byBand CouncilNation Program Managers | AANDC, FNHA, … |
| Community and Public Communication | Community Name(s) | Corporate | All | Low | <dept name> | Staff, Community Members and Residents, Partners, and the public | Same as Used by |
|  |  |  |  |  |  |  |  |

## Data Standard Template

Data Standard Inventory List: The following list summarizes all of the data elements that form the consolidated list of Data Standards approved via the Data Governance Board. Refer to the Data Governance Board approval process for further details on background of the Standard.

|  |  |  |  |
| --- | --- | --- | --- |
| **Data Sector:** | **Data Element:** | **Purposes for collection and use of the data** | **Purposes for disclosure of the data** |
|  |  |  |  |

Data Standard Specifications: The following list outlines the technical specifications for each data element. Refer to the Data Governance Board approval process for further details on background of the Standard.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Data Sector:** | **Data Element:** | **Mandatory or Optional?** | **Does the data need to support alphabetical (mixed case or all uppercase or all lowercase), numeric, and/or special characters? If numeric what are the values? If special characters what are they?** | **Will the data be included in an aggregated report? If ‘yes’, what are the list of values that must be available for the staff to select? If ‘no’, it means the staff can enter free form text.** | **Is there a requirement to know who changed data and when it was changed? If so is there a requirement to know what the data was prior to it being changed?** | **Business rules:** |
|  |  |  |  |  |  |  |

## Data Governance and Privacy and Security Awareness Training

## Tracking Log

| **Name of Legal Entity** | **Department Name** | **Trainee Name** | **Training Materials****(e.g. Training Package Version #1)** | **Date of Training Session** | **Confidentiality and Acceptable Use Form Signed** | **Target Date for Next Training Session (Must be less than one year)** |
| --- | --- | --- | --- | --- | --- | --- |
|  |  |   |   |   |   |   |
|  |  |   |   |   |   |   |
|  |  |   |   |   |   |   |
|  |  |   |   |   |   |   |
|  |  |   |   |   |   |   |
|  |  |   |   |   |   |   |
|  |  |   |   |   |   |   |
|  |  |   |   |   |   |   |
|  |  |   |   |   |   |   |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

## Confidentiality and Acceptable Use Agreement / Acknowledgement

I acknowledge that I am required to read and accept each of the following terms and acknowledgement them before accessing any information systems or paper records containing Nation data (Corporate Data, Cultural Data, Human Related Data, and/or Lands and Resource Data) pertinent to <insert name of Nation> or <insert name of Community/Communities>, referred hereafter as ‘Nation’:

□ I have received the Nation Data Governance and Privacy and Security Awareness Training and I understand the content contained in the associated education material that has been provided to me. I acknowledge that I am required to review this material before I access and/or use Nation data and annually thereafter.

□ I acknowledge that I will hold the Nation Data I create, view, update, access and/or use, in the strictest of confidence as per applicable legislation, practice standards, and the Nation Data Governance and Privacy and Security policies and procedures, and that this applies regardless of whether I am performing my job duties on or off premises.

□ I agree to only create, view, update, and access Nation Data that directly pertains to the specific role(s) and responsibilities that I perform and an employee/contractor for the Nation.

□ I acknowledge that when I create and/or update Nation Data I will ensure that the data is accurate and complete to the best of my knowledge.

□ I agree that I will share Nation Data only with individuals who need to know because of their specific role(s) and job responsibilities.

□ I agree that I will not share Nation Data that may be revealed to me in the process of supporting, maintaining, administering and/or resolving work- and/or system-related issues.

□ I agree that my access accounts (e.g. User Names, User Identifiers, and passwords) are equivalent to my electronic signature and that I will not share my access accounts with anyone. I acknowledge that I will be held accountable for all activity performed under my access accounts.

□ I acknowledge that paper-based Human Related Data and confidential or sensitive Nation Data are to be kept in a locked filing cabinet that is owned and managed by the Nation, and that they are to be accessed only for the purpose of performing my job duties. I acknowledge that paper records are to be returned promptly to the locked filing cabinet and are not to be left unattended. I agree that I will keep the key to the locked filing cabinet on my person or in a locked desk drawer at all times and will not share that key with any other person who should not have access to the information contained within the locked filing cabinet.

□ I understand that all my activity relating to data maintained within computer-based systems in use within our organization (e.g. creation, accesses, searches, updates) is monitored and recorded in an audit trail or log, and that access compliancy audits and/or reviews will be conducted on a regular basis.

□ I understand that I may not, and I undertake that I will not, access my own human related personal information data or anyone’s human related personal information (including family and friends) unless legitimately required to do so as defined by my role(s) and job responsibilities.

□ Should I have reason to believe that there is potential for a privacy or security incident/breach to occur, that a privacy or security incident/breach may have occurred, or that a privacy or security incident/breach has occurred, I will notify the Nation Data Steward, Manager, or Supervisor immediately.

□ I agree to change my user account password on a regular basis as required by the Nation’s privacy and security policy and to not access my account from a location outside of Canada.

□ By signing this Confidentiality and Acceptable Use Acknowledgement, I affirm, if applicable, that I am in good standing with the organization that governs my profession. Furthermore, if applicable, I will notify this the Nation immediately if I am not in good standing.

□ I agree that by signing this Confidentiality and Acceptable Use Acknowledgement, I am bound to uphold each of the terms herein and that my acknowledgement of these terms will continue after my role and/or responsibilities change; or after the termination of my employment.

□ I hereby acknowledge that failure to comply with these terms can lead to disciplinary action, which may include termination of access, withdrawal of privileges, termination of employment, loss of contract, professional sanctions, and/or legal action.

This Acknowledgment supersedes any previous Confidentiality and Acceptable Use Acknowledgement that I may have been requested to complete for the Nation.

|  |  |
| --- | --- |
| Date: |  |
| Name: |  |
| Name of legal entity: |  |
| Department: |  |
| Email: |  |
| Signature: |  |

*(Entering your email above will be accepted as your signature if this document is attached to an email which has been sent from your email account.)*

## Adhoc Information Sharing Tracking Log

| **Start Date: <insert date>** |
| --- |
| ***Purpose:*** *the purpose of this log is to track scenarios that require our Nation to share human related information in situations when we do not have a formal and documented information sharing arrangement.For more information about this log refer to our Data Governance Policy manual.* | **Instructions:**1) Insert Start Date, print form and place in an appropriate location for staff. II) Instruct Staff to complete. III) 1-3 months later record the ‘End Date’, scan and email to the Human Related Data Steward. IV) Place original in applicable administrative file and retain as per the Privacy and Security Data Retention Policy and Schedule.  |
| **Item #** | **Date Information Is Being Shared** | **Requesting / Receiving Party** | **Employee Name** | **Purpose for sharing the information** | **Approver** | **Was the individual advised that information was being shared? If so specify the date and record any special notes associated.** |
| 1 |  |  |  |  |  |  |
| 2 |   |   |   |   |   |      |
| 3 |   |   |   |   |   |      |
| 4 |   |   |   |   |   |      |
| 5 |  |  |  |  |  |  |
| 6 |  |  |  |  |  |  |

1. Data Governance Framework [↑](#footnote-ref-1)