



## Procedure

Procedure Name	<b>Data Sharing Procedure</b>		
Procedure #	IT 2.3	Parent Policy	IT 2.0 Data Governance
Policy Owner	Vice President Administration & CFO	Effective Date	January 16, 2025
Procedure Owner	AVP Information Technology & CIO	Next Review Date	January 2030
Approved by	AVP Information Technology & CIO	Approval Date	January 16, 2025

### 1.0 Purpose/ Background

NAIT recognizes that data is an asset. However, data is rarely static and may need to be shared across its lifetime, both internally and externally, to the Institute. This procedure seeks to ensure that data is shared responsibly within and external to NAIT and in line with data classification and privacy best practices and applicable law.

### 2.0 Definitions

Term	Definition
Data	Information in a specific representation, usually as a sequence of symbols that have meaning.
Data Sharing	Data sharing is the process of exchanging, transferring, or granting access to data between individuals, departments, organizations, or systems.
Data Sharing Agreement	A written record of understanding between two parties that will be sharing information or data with each other that sets the conditions on the collection, use, or disclosure of data.
Need-to-know Principle	The need-to-know principle (or the principle of least privilege) states that a user shall only have access to the data required for their job function, regardless of their leadership level.
Source of Truth	A source-of-truth is the designated authoritative repository or system where the most accurate, current, and reliable version of information, data, or documentation is maintained. It serves as the definitive reference point for ensuring consistency, accuracy, and alignment across all related processes, systems, and stakeholders within an organization.
Data Trustee	The individual accountable for the management of a specific domain of data. Data Trustees resolve escalated data or escalate issues to the Data Governance Steering Committee, approve access to data, and assess the security, quality, and value of data.
Data Steward	An individual for a department or school is assigned the responsibility for coordinating data management for their unit. Data Stewards have expert knowledge of business processes and how data is used; resolve data issues identified inside their department or escalate issues to Data Trustees; and communicate changes to data governance policies, procedures, standards, and projects.

Data Custodian	A staff member, vendor, or contractor who is responsible for the technical environment and structure for electronic data or the handling of physical data media. A data custodian ensures technical processes sustain the confidentiality, integrity, and availability of data. They also ensure access to data is authorized and controlled.
----------------	---

### 3.0 Procedures

- 3.1 Data sharing is approved by Data Trustees, with input from Data Stewards and Data Custodians, as appropriate for the type of data sharing request and before any data exchange between parties. Data Trustees are accountable for understanding risks and mitigations dependent on data sensitivity classification before sharing occurs.
- 3.2 Confidential and Restricted data must be shared based on the 'need-to-know' principle and in accordance with its data classification (see *IT 2.2 Data Classification Procedure*).
- 3.3 Impact Assessments should be used as appropriate and in accordance with applicable law.
- 3.4 Shared data must be of appropriate quality for the purposes for which it is being shared, including being as complete, accurate, and up-to-date as needed (see *IT 2.4 Data Quality Procedure*).
- 3.5 Before data is shared, procedures and accountabilities must be in place, which may include:
  - 3.5.1 Adherence to NAIT's policies and procedures.
  - 3.5.2 Clear understanding of what data is being shared and the purposes for that sharing. Where personal information is shared, this must align with consent agreements at the time of collection and applicable law. Where there is any uncertainty regarding NAIT's obligations regarding sharing personal information, NAIT's General Counsel Services department should be consulted before any disclosure.
  - 3.5.3 Clear retention and disposition outlined for shared data.
  - 3.5.4 Ensuring reasonable security, checks and controls for data sharing.
  - 3.5.5 The ability to audit or monitor data when shared with other parties.
- 3.6 Clear and documented understandings of data use and formal Data Sharing Agreements will be used where appropriate.
- 3.7 The Data Governance Program Team will facilitate data sharing agreements and maintain a catalogue of approved data sharing agreements. The Data Governance Program Web Page, under the ITS Department section of the staff intranet site, will provide the information needed to complete data sharing processes.
- 3.8 Data must be shared in a controlled manner appropriate to its circumstances and classification that minimizes risk, prevents unauthorized duplication of data outside of NAIT's control, and complies with all applicable laws and any agreements to which NAIT is a party.
- 3.9 Source of Truth data must be clearly identified and managed in data sharing processes, with controls in place to prevent divergence of authoritative records in situations where shared data may be modified.
- 3.10 Any concerns about data sharing must be reported via the Data Governance Program's data issues process. Concerns regarding sharing data containing personal information must also be reported to General Counsel Services.

- 3.11 When requested, The Data Governance Steering Committee will provide oversight for complex data sharing requests with third parties to NAIT, such as for media requests or external research requests.
- 3.12 Data sharing activities must be reported to Data Trustees, who will share with the Data Governance Steering Committee as appropriate.

#### **4.0 Exceptions to the Procedure**

Exceptions to this procedure must be documented and formally approved by the Procedure Owner.

Procedure exceptions must include:

- The nature of the exception
- A reasonable explanation for why the procedure exception is required
- Confirmation that the exception aligns with the general principles
- Any risks created by the procedure exception and how they will be managed.

#### **5.0 Related Documentation**

- Freedom of Information and Protection of Privacy Act
- Data Governance Intranet Site

##### ***Document History***

<i>Date</i>	<i>Action/ Change</i>