NAIT

Procedure

Procedure Name	***Data Classification Procedure***		
Procedure #	IT 2.2	Parent Policy	IT 2.0 Data Governance
Policy Owner	Vice President Administration	Effective Date	May 10, 2023
Procedure Owner	AVP Information Technology	Review Date	May 10, 2028
Approved by	AVP Information Technology	Approval Date	May 10, 2023

1.0 Purpose/ Background

NAIT recognizes that its data is an important strategic asset. This procedure defines the data classification scheme to be used by NAIT and applies to NAIT data, both physical and digital mediums. These classifications will be utilized to determine how the data will be managed, used, and secured in a manner appropriate to its importance and sensitivity.

2.0 Definitions

Term	Definition
Data	Information in a specific representation, usually as a sequence of symbols that have meaning.
Data Trustees	An individual accountable for the management of a specific domain of data.
Personally Identifiable Information	Any recorded information about an identifiable individual.
Third-party	An external organization or individual contracted by NAIT to provide goods or services.
Agent	An agent is a person who has been legally empowered to act on behalf of another person or entity.
Institutional Data	Data created, acquired, stored, maintained, or transmitted by or for the institution to conduct business in any form, whether structured, unstructured, detailed, or aggregated.
Record	Information created, received, and maintained as evidence and as an asset by NAIT, in pursuit of legal obligations or in the transaction of business.
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.

3.0 Procedures

3.1 All institutional data will be classified according to the following scheme based on risk and priority:

- **Public**: Data available to the public, as well as staff, contractors, subcontractors, agents, or students at the Institute.
- **Protected**: Data available to staff, contractors, subcontractors, agents, and students at the Institute with a need-to-know for business operations.
- **Confidential**: Any sensitive data intended for use only by specific groups of employees. Unauthorized disclosure, alteration, loss, or destruction of this data would seriously impact NAIT's reputation and possibly undermine public trust in the Institute. This includes personally identifiable information not publicly available.
- **Restricted**: Any extremely sensitive data whose access is restricted to a limited set of named individuals. Explicit approval of the data trustee is required to release this information, even to those with a need-to-know. Unauthorized disclosure, alteration, loss, or destruction of this data could risk the health, safety, privacy, or reputation of an individual, members of the public, or NAIT students or staff.

A data classification matrix (Appendix A of this procedure) provides examples of data from each category of the above scheme to help staff recognize the classification of data they use during business activities.

3.2 NAIT's default data classification is Protected.

3.3 Data is classified based on its level of sensitivity and impact to NAIT.

3.4 The data classification applied is based on the most sensitive data within a record.

3.5 The data classification informs the security and access controls required to safeguard data appropriately.

3.6 Data classification and associated protections apply regardless of the medium or location of data.

3.7 Access to data is granted only to appropriate individuals as guided by the data classification matrix or the need-to-know principle.

3.8 Access to data is subject to an audit of classification (public, protected, confidential, and restricted). Access found not in accordance with 3.7 may be denied or revoked.

4.0 Exception to the Procedure

4.1 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

IT 4.0 Digital Security Policy
IT 3.0 Third-party IT Service Provider Management Policy
FO 11.0 Records Management Policy

Document History

Date	*Action/ Change*
May 14, 2018	New Procedure
April 4, 2023	Updated to align with IT 2.0 Data Governance Policy. Added Data Classification Matrix, changed document owners, added clarity around default data classification and made purpose statement more concise.
May 10, 2023	Changed numbering from IT 1.12 to IT 4.2.

Appendix A: DATA CLASSIFICATION MATRIX (in order from the least to the most restrictive)

Note: In some cases, classifications may be dependent on the nature of the events and incidents material is connected to, and not based on the type of document or information it is of itself (i.e., materials related to reviews may be confidential or restricted dependent on the nature and risk impacts of the review).

Classification	Definition	Examples (Not limited only to the examples provided)	Risk Impacts
Public	• Non-proprietary data created in the normal course of business where unauthorized disclosure, alteration, loss, or destruction is unlikely to cause harm to NAIT's mission, safety, finances, or reputation. • Available to the public.	• Corporate public website • Communication materials such as brochures, advertising, sponsorships, annual report (printed version) • Approved policy documents • Campus map showing buildings, names, addresses, parking, lighted pathways, emergency phones, etc. • Employee's workplace name, business contact information	• Little or no impact • Minimal inconvenience if not available.
Protected [Protected A][i] (Default Class)	• Data to which staff, contractors, subcontractors, agents, or students may have authorized access possessing a need to know for business-related purposes (role-based access). • Protected data may include business information about how we effectively operate and conduct business as well as non-personal information. • Data is secured and not accessible by the public.	• Draft policy and planning documents • Business procedure manuals • Staff meetings agendas/minutes • Internal communications • Application configuration and reference data (including flags, logically deleted and date stamps related to the system attributes) • As of dates (including effective date, termination date) • Individual grades, academic transcript, class schedule, student coursework and examinations • Building CAD drawings, building standard operating procedures (SOPs) • Student ID # / Employee ID # • Student name, Major/Degree/Program (may be disclosed to third parties with appropriate business need)	• Unfair competitive advantage • Low levels of financial loss to the enterprise • Disruption to business if not available.
Confidential [Protected B][i]	• Data where the unauthorized disclosure, alteration, loss, or destruction would have an adverse impact on NAIT's mission, safety, finances, or reputation. • Confidential data includes: ○ Personally identifiable information not publicly available, ○ financial information or sensitive information uniquely assigned to an individual (in many cases for their lifetime and of high importance, even external to NAIT), ○ personal health related information, ○ details concerning the effective operation of NAIT, ○ business or financial/business information provided to NAIT in confidence.	• Personal information (full legal name, birth date, death date, gender, height/weight, etc.) • Demographic information (individual's street address and postal code, city, province, e-mail address, individual's contact phone number(s), signature, photograph, citizenship/ immigration status) • Previous employer • Personal bank acct info - Electronic Funds Transfer (EFT), including transit number • Employee Salary / Home Address • Passwords • Personal Health Number (PHN) of individual • Social Insurance Number (SIN) • Medical history information (diagnostic and treatment) • Personnel files – HR related information • Third party business information submitted in confidence (in quotations or bids, billing rates of individuals) • Bills for an individual or organization • Internal documentation: marketing & unpublished academic research, survey results, faculty plans, patent applications	• Loss of reputation or competitive advantage and partnerships • Loss of confidence in NAIT products or services • Loss of personal or individual privacy, humiliation and reputational harm • Loss of trade secrets or intellectual property • Loss of business opportunity • Damage to partnerships • Possible legal action or media attention • Risk of identity theft/ financial loss • Loss of employment

	• Access and ability to input or change the information are limited to individuals in a specific function, group, or role, in accordance with a need-to-know principle to perform business operations.	• Payment Card Information • Driver's license/passport information • Institutional Financial records / Donor records • FOIP files • Network/Digital Security configurations/architectures or logging information • Strategic Plan (final version) • Agreements/Signed Contracts	
Restricted [Protected C][i]	• Data where the unauthorized disclosure, alteration, loss, or destruction would severely harm the NAIT's reputation or business position resulting in financial, reputation or legal loss. • Access is specific to a named individual and is very limited. • The explicit approval of the data trustee is required to release this information, even to those with a need to know. Restricted classification should only be used when no alternative exists and such data must be carefully protected.	• Executive documents • Government briefing documents • Annual report prior to public release • Strategic Plan (draft versions) • Criminal investigations or litigation • Solicitor-client privileged material • Settlement documents • Workplace investigation/reviews, claims from termination, and grievances documentation (dependent on severity of incident) • Human rights complaints and response documents/reports • Shared secrets & cryptographic private keys • Back-up media	• Significant damage, including corporate reputation loss • Significant financial loss to NAIT • Compromise of government contracts/negotiations • Destruction of relationships with major customers • Compromise of legal position • Loss of life • Serious injury • Loss of public safety

[i] Protected A, B & C are data classifications that correlate with the Alberta and Federal Government's Data Classification mechanisms.