SUBJECT:	CATEGORY:	NO.
Data Management	**Information Management**	**802**

PREAMBLE

Successful collection and management of data is critical to the academic and administrative functions of SIAST. Through active planning, organization, and management of this institutional asset, data and information become one of SIAST's most important resources and investments.

The purpose of this policy is to establish the fundamental principles and guidelines by which SIAST's data will be classified, managed, maintained and secured.

POLICY

SIAST recognizes the importance of data and the information derived from that data. To realize the maximum benefit of institutional data, SIAST will actively manage activities related its creation, collection, storage, maintenance and sharing regardless of whether the data is:

- stored electronically or in hard copy,
- held in centrally managed databases/systems, or in academic or administrative offices,
- exists in structured, unstructured, summarized or aggregated format

SIAST data will be managed as an institutional resource using the following data management principles designed to safeguard data integrity, security and access.

1. Data Ownership

a. All SIAST data, and information derived from that data, are owned by SIAST as a whole, not an individual, program, department or division.
b. All SIAST data and information are considered shareable resources.
c. SIAST will determine how its data and information will, or may, be shared.

2. Data Classification, Definition & Standards

a. SIAST will establish and maintain institutional data classification standards.
b. SIAST will establish and maintain institutional definitions for data including how data is derived and how it is intended to or can be used.

3. Data Stewardship

a. SIAST will manage its institutional data using the principles of data stewardship and data sharing.
b. Data stewards are responsible to define and classify the data within their purview according to standards established by SIAST.
c. Data stewards have overall responsibility and authority for the creation, collection, quality, access and security of data within their respective areas according to standards established by SIAST.
d. Day to day implementation of data stewardship activities within subsets of functional area may be delegated to a data manager.

4. **Data Collection & Management**
   a. Authoritative sources of SIAST data will be identified and maintained. SIAST will discourage the creation of redundant or duplicate data sources.
   b. Institutional data will be collected as close to source as possible regardless of whether the department or individual collecting the data will have future interest in that data.
   c. Institutional data will be entered and maintained in the appropriate data repository in a timely manner and with utmost care.
   d. SIAST will store data in databases and servers that are integrated, consistent, reliable, accessible and secure.
   e. Any database acquired or developed to hold SIAST data must be registered with Information Technology Services.
   f. Data stored in databases and servers external to SIAST is subject to the provisions of SIAST policy 805 External Application and Data Hosting.
   g. When electronic data is no longer required for legal or historical reasons, it should be deleted in such a way that recovery is not possible.

5. Data Quality
   a. The quality of SIAST institutional data will be actively managed. Standards for data quality, validity, availability, access, definition, and use will be established, monitored and enforced to provide the highest quality data.
   b. Data stewards are responsible to establish procedures and practices to ensure data quality is maintained and that data requiring update or correction is processed in a timely manner.

6. Data Access
   a. Institutional data will be made readily available to any employee of SIAST with a legitimate business need to access the data. Unnecessary restrictions to its access will be avoided.
   b. Data stewards are responsible for determining data access levels and distribution.
   c. Data access rights are not transferable. Any SIAST employee granted access to institutional data cannot copy or redistribute data or information for the purpose of giving access to someone who would not normally have access to that data or information.
   d. Data must only be accessed and used for its intended purpose. Data must not be accessed or manipulated for personal gain, or out of personal interest or curiosity.

e. Data users must be aware of their responsibilities under SIAST's privacy policy and *The Local Authority Freedom of Information and Protection of Privacy Act* (LAFOIP).
f. Data users must respect the privacy of individuals whose records they may access. No subsequent disclosure of personal information contained in files or databases may be made. Disclosure is understood to include (but is not limited to) verbal references or inferences, correspondence, memoranda and sharing of electronic or paper files.

7. Data Security

a. All members of the SIAST community have a responsibility to protect SIAST data from unauthorized access, modification, disclosure or destruction.
b. Secure storage of institutional data is a joint responsibility of system and network administrators, database designers, application designers, data stewards, data managers, and the data user who must ensure appropriate security mechanisms are established and utilized.
c. Institutional data will be safeguarded and protected from deliberate, unintentional or unauthorized alteration, destruction and/or inappropriate disclosure or use in accordance with established institutional policies and procedures and federal and provincial laws.
d. Institutional data must be stored in such a way as to ensure the data is secure, and that access is available to authorized users only.
e. Institutional data stored in paper or other formats must also be safeguarded, distributed, and disposed of appropriately.
f. Institutional data stored on laptop computers or portable storage devices, including USB memory sticks, should be encrypted to prevent accidental or unintended disclosure of SIAST data in the event of theft or loss of the device.
g. Deliberate misuse or inappropriate disclosure of SIAST data or information may result in disciplinary measures, or suspension or dismissal.

DEFINITIONS

Institutional Data: - Institutional data is data that is created, collected, and stored by any office of SIAST in support of its academic and administrative functions. It is generally referenced or required for use by more than one organizational unit; included in an official SIAST administrative report; or used to derive an element that meets one or more of the criteria above.

Institutional data is not limited to data and information stored on centrally managed databases and servers. Institutional data can also be data and information stored on hosted services, individual desktops, paper files, software such as spreadsheets, and portable storage devices such as handheld computers, cds, dvds, and memory sticks.

Structured Data: - Data that resides in fixed fields within a record or file or data that can be tagged and accurately identified (ie XML).

Unstructured Data: Any document, file, image, report, form, etc. that has no defined, standard structure. Examples of unstructured data include email, spreadsheets, documents, etc.

Data Owner: - SIAST is the owner of the institutional data. Individual units or departments have stewardship responsibilities for specific data elements or portions of institutional data.

Data Steward: - Individuals with the overall responsibility and authority for data definition, classification, quality and access within their functional area.

Data Manager: - Individuals with operational level responsibilities for specific portions of institutional data. Data managers are typically responsible for procedures supporting the creation, storage, maintenance, use and disposal of data within guidelines established by the data steward.

Data Users: - Individuals who need and use institutional data as part of their assigned duties or in fulfillment of their role at SIAST. Data users have particular responsibilities to ensure timely and accurate data entry, use and dissemination of data consistent with privacy and security guidelines.

PROCEDURES

Development and maintenance of procedures specific to this policy are the responsibility of the Information Technology Services Enterprise Architecture and Data Services units.