: DALHOUSIE UNIVERSITY **Institutional Data Access Policy**	*Policy Sponsor:* President	*Approval Date:* February 24, 2022
	Responsible Unit: Office of the Provost and Vice-President Academic	*Amendments:*

A. Background & Purpose:

The Institutional Data Access Policy exists to facilitate access to institutional data by University personnel (or employees) for internal use and only for purposes necessary to fulfil work responsibilities. Institutional data is a shared University resource to support data-informed decision making. The policy adheres to the following principles:

1. ***Authority and Ownership***: All institutional data is an institutional asset.

2. ***Governance and Accountability***: As an institutional asset, data is governed by the Data Access Committee and in accordance with all federal and provincial legislation and Dalhousie policies;

3. ***Access***: Authorized decision makers and designated employees have access to the data as required to perform their roles;

4. ***Value and Quality***: Standardized and quality-controlled data support strategic integration and decision-making; and,

5. ***Privacy*****:** The privacy of individuals is respected and ensured through personal information being appropriately protected and managed in accordance with applicable legislation and Dalhousie policies.

B. Application:

The Institutional Data Access Policy applies to all institutional data at Dalhousie University.

C. Definitions:

1. In this Policy:

1.1. "Data Access Committee" is the University committee established by the University's Information Governance Steering Committee (IGSC), approved by the Provost Committee with a mandate to oversee, review and approve access to authoritative university data for planning, analysis and decision-making.

1.2. "**Data Steward"** is the University senior manager of a unit where institutional data resides. The Data Steward is responsible for institutional data in their functional area and is identified

as such on the university's master list of Data Stewards, Data Delegates and related information management systems.

1.3. "**Data Delegate**" is a university employee with delegated responsibility by a Data Steward in accordance with this Policy and is identified as data delegate on the master list.

1.4. "Data Users" are employees who are granted access to Institutional Data.

1.5. "Information Governance Steering Committee" (**IGSC**) is the University committee established by the University's Provost Committee whose terms of reference include oversight of university information and related technology, policy, priorities and associated infrastructure investments for Dalhousie University.

1.6. "**Information Management Systems**" are electronic or other systems, used by the university to administer university operations, programs and activities, and are identified as Information Management Systems on the master list.

1.7. "**Institutional Data**" is data collected by the institution and only to be stored on Institutional (Dalhousie University) Systems.

1.8. "**Master List**" is the list that contains the names of current data stewards, data delegates and Information Management Systems. The list is maintained by the Data Access Committee and published on Dalhousie's website.

1.9. "Functional Area" is the unit headed by and for which the Data Steward is responsible.

D. Policy:

1. Institutional Data is owned by the University.

2. Data Stewards are responsible for the Institutional Data.

3. Institutional Data may be accessed by University employees solely in accordance with this Policy and these procedures. This includes requests for access from one or more information management systems.

4. Access to institutional data is normally granted to data users who demonstrate need to access the data to fulfill the scope of their employment in the performance of authorized duties.

5. Data users must use Institutional Data solely in accordance with the conditions by which access has been granted.

E. Administrative and Governance:

1. This administrative policy falls under the authority of the President.

2. The Vice-Provost, Planning and Analytics, supported by the Data Access Committee, is responsible for the administration, communication, training, review and compliance monitoring of this Policy.

3. The Data Access Committee is accountable to the Information Governance Steering Committee (IGSC).

4. The Data Access Committee is responsible to:

4.1. Collaborate with and support the Vice-Provost, Planning and Analytics per Section E.2. of this Policy;

4.2. Develop protocols and guidelines to support and facilitate access to Institutional Data in furtherance of this Policy;

4.3. Provide guidance and be a resource to Data Stewards;

4.4. Periodically review protocols and guidelines developed by individual Data Stewards;

4.5. Approve the composition of the Master List. Communicate and maintain the Master List; and,

4.6. Provide an annual report to the IGSC and include information received from Data Stewards per Section E.5.3 of this Policy.

5. Data Stewards are responsible to:

5.1. Consider, decide, approve or deny requests for access to Institutional Data within their Information Management System, in accordance with this Policy;

5.2. Maintain a set of protocols and guidelines for data access by Dalhousie employees within and external to the functional area within Dalhousie University;

5.3. Submit, within 90 days of each fiscal year end, an annual report to the Data Access Committee that includes, a summary of all access decisions made in the previous fiscal year;

6. Data Stewards may develop protocols and guidelines that are unique to the Institutional Data within their functional area, provided those protocols and guidelines do not contradict this Policy or any protocols or guidelines established by the Data Access Committee;

7. Data Stewards may delegate some or all their responsibilities to one or more Data Delegates within their functional area in accordance with this Policy;

8. One or more Data Stewards or Data Delegates may work together to grant access to Institutional Data where access relates to more than one functional area, and to develop protocols and guidelines that are unique to those situations provided those protocols and guidelines are in accordance with this Policy or any protocols or guidelines established by the Data Access Committee.

F. Procedures:

1. Procedure to Access Institutional Data

1.1. Employees who work within a Data Steward's functional area may access the Institutional Data within the Information Management System administered by that Data Steward, in accordance with the Data Steward's data access protocols and guidelines;

1.2. All requests to access Institutional Data must be made to the Data Steward of that functional area by completing the on-line request form and directing it to the Data Steward. Access form is available on the Dalhousie website.

1.3. Data Stewards will consider the request and provide a response within ten (10) working days of the request. Extenuating circumstances may influence this response time, and, in that case, the Data Steward will contact the individual making the request to apprise them of timelines and circumstances.

1.4. Where the Data Steward approves the request, certain conditions may be placed on the access to:

a) Minimize risk of the data being misunderstood or misused;
b) Protect the integrity of the data;
c) Enable accessibility and development of appropriate interfaces; and/or,
d) Ensure safeguards are in place to protect the data from unauthorized use, access, disclosure or retention and comply with applicable privacy laws.

1.5. A Data Steward, in determining an access request, may consult the Data Access Committee for guidance.

1.6. A Data User may request the Data Access Committee review a decision of a Data Steward, by submitting a written request to the Chair, Data Access Committee. The Data Access Committee shall decide within **30** days unless extenuating circumstances. An appeal on factors that influenced this decision may be made in writing to the vice-president to which the Data Steward is accountable. The vice-president shall make a final decision.

2. Procedure for Data Steward Delegation of Responsibilities to a Data Delegate

2.1 To delegate some or all responsibilities to a Data Delegate, a Data Steward must notify the chair, Data Access Committee, in writing, of the name of the Data Delegate, the assigned responsibilities, the time period for which the authority is delegated, any limits or restrictions on the delegation and confirmation that no sub-delegation is made.

2.2 A Data Steward is responsible to ensure a Data Delegate understands the University Data Access Policy and data governance in general, and their responsibility with respect to maintaining confidentiality, data integrity and data access protocols.

2.3 The delegation of responsibility to a Data Delegate does not relieve the Data Steward from accountability for compliance with the Data Access Policy. The Data Steward is responsible for all actions and inactions of the Data Delegate.

2.4 The Data Steward may revoke delegation at any time and notify the Data Access Committee chair, in writing, of this revocation.

2.5 If the Data Steward changes, the new Data Steward is responsible to confirm delegation and make necessary changes through the Data Access Committee chair within one of assuming the position.

2.6 The Data Delegate may not delegate access authority to someone else.

2.7 The delegation of access authority will be recorded on the Master List.