University of Toronto

Implementation of an Institutional Data Governance Program

Report & Recommendations – June 2020

Table of Contents

Context

The implementation of a formal institutional data governance program at the University of Toronto provides an enormous opportunity for us to harness our valuable data resources in guiding decisions, policies and strategies and to enhance the skills and capacity of our colleagues and staff. It will require a substantial commitment of time and resources in the initial years, but over time will become embedded in our culture and processes.

This report serves as a companion piece to the foundational report *Towards an Institutional Data Governance Program*, released in January 2020 by the Data Governance Committee. We recommend that the two reports be read together. The foundational report establishes the goal of the institutional data governance program at the University of Toronto – to promote and support the responsible use of high-quality institutional data, to facilitate informed and insightful use of these data, and to increase their value to the university community and beyond. The foundational report also defines data governance and the term "institutional data" and describes the desired outcomes and guiding principles for a data governance program at the University of Toronto. The foundational report acknowledges the "...inherent tension between the *value* created by the appropriate and widespread use of institutional data and the *risks* – of data corruption or misinterpretation, for example – occasioned by greater openness and access. Managing this tension, safeguarding and enriching the value of institutional data, is at the heart of what has come to be called *data governance*." We encourage readers of this report to continually balance these two perspectives as we implement our institutional data governance program.

In this document, we present a high-level description of how that program will operate at the University. The recommendations here are aligned with the guiding principles in the foundational report and are grounded in a review of relevant published literature and processes at peer institutions. We also received input from a wide range of U of T stakeholders including the Institutional Data Hub executive steering committee, Principals, Deans and Chairs (P&D and PDAD&C), senior administrators across academic and shared service divisions, the data analyst and contributor community, information technology, legal, business intelligence and many other colleagues. In addition, our recommendations for the program are informed by a series of in-depth interviews conducted by the Data Governance Committee. These interviews serve as an indicator and initial assessment of the current state of data governance at the University. A summary of our key recommendations is included in Appendix A.

Several existing University policies and guidelines that indirectly relate to data governance also provide context for our recommendations. At this time, we are not introducing a new stand-alone data governance policy. However, we recognize that over time the need for a specific policy may arise. In the meanwhile, accountability and responsibility for data governance reside

within the *2007 Policy on Information Technology* under the authority of the Vice-President & Provost. This policy and other related policies and guidelines are outlined in Appendix B.

The approach presented in this document is influenced by a particular model called "non-invasive data governance"[1] which draws upon an organization's existing people, processes, and infrastructures. This approach is collaborative, empowering and supporting those who are already engaged in a wide range of informal data governance activities. The non-invasive approach suggests the formal program should integrate with, and augment, existing divisional structures and processes. Our broad consultation indicates that this approach fits well with our culture and the highly distributed administrative structure of the University. As the institutional data governance program evolves, new institution-wide best practices, community-of-practice and oversight processes will be developed, and it will be critical to ensure that these processes are well-defined, well-resourced, robust and sustainable. The Director of Institutional Research and Data Governance (IRDG) and the IRDG team will serve as the focal point for the program and as a resource for divisions as they develop their own plans within the broader program.

Scope

Institutional Data

The scope of the institutional data governance program is tied closely to the definition of "institutional data" as defined in the foundational report:

> "Institutional data comprise all of the data that are held by the University for the purpose of supporting its administrative operation, broadly understood.
>
> For the purposes of the Institutional Data Governance Program, research data are data that are held at the University for conducting scholarly research, and are outside the scope of the Institutional Data Governance Program."

While institutional data may be used secondarily for academic research or other purposes, these data continue to be under the purview of the institutional data governance program.

Interpretation of the definition and the scope of institutional data will evolve over time as new types and sources of data and proposed uses arise. Provisionally, institutional data extend to:

- Data about (a) any of U of T's students, faculty, staff, alumni or donors; (b) the teaching and research activities of the University; (c) the University's physical infrastructure,

[1] Seiner RS. Non-Invasive Data Governance. The path of least resistance and greatest success. Basking Ridge, NJ: Technics Publications, 2014.

occupancy, and capital projects; and (d) the University's financial statements and financial records. This includes – but is not limited to – data concerning:
    - student enrolment and financial aid,
    - human resources,
    - library resources and services,
    - administrative services,
    - faculty teaching, and
    - faculty research applications and grants held.
- Data that are collected (a) directly by the University or by a third party on behalf of the University; (b) indirectly, by the university or a third party, in the course of conducting University business; or c) indirectly, by a third party for other purposes outside of University business but which are used secondarily for the purpose of supporting the University's administrative operation.

While the boundaries are not always clear, institutional data include data held in datasets developed for transactional, operational, and analytic purposes. Over time, we will explore these distinctions and the implications for governance over these different types of datasets.

The Institutional Data Governance Program

Operationally, the institutional data governance program will focus on guidance and oversight, as it strives to improve the quality of institutional data and to promote the responsible use of those data. When considering data quality, the general benchmark will be "fit for purpose". This benchmark provides a flexible interpretation, such that data are sufficiently accurate, complete, consistently recorded, and timely for their intended purposes. This benchmark will differ depending on how the data are utilized. When considering "purpose", a systems perspective will be taken. So, in addition to primary uses of the data (e.g. student registration), secondary uses of the data by academic divisions for planning and operations purposes will be considered. Further, attention to data quality extends to metadata, promoting broad agreement and clarity on how key variables in institutional datasets are defined and used. To help improve consistency, over time, the program will promote the development of master datasets, to minimize redundancy in data collection.

Good data governance also promotes responsible data use. Institutional data should be managed securely throughout their lifecycle (collection, storage, access, transfer, retention, and destruction) and in compliance with relevant laws. Access to institutional data must be governed by appropriate procedures, with clear guidance as to the conditions for accessing data and the nature of their use. Access also needs to be timely. Responsible data use includes endorsing recognized standards for data literacy, data analytics and reproducibility. All this will foster the trust of those whose data are being used (i.e. students, staff, and alumni).

The purview of the data governance program extends to all institutional data – whether held on premises, in the cloud, or in the custody of a third-party agent conducting business on behalf of the University. This will also include personal health information that resides in any of the clinics run by the University or held administratively.

People and Culture

People are at the core of a successful institutional data governance program. The program will formalize what has so far been an ad hoc informal approach at U of T, bringing greater consistency in the exercise of data governance throughout the data lifecycle and a culture of good data governance. Ongoing communication and transparency of the data governance program – its progress, challenges and successes – can help build momentum and change. Raising awareness of the program and explaining its value and importance in achieving this goal are critical to fostering this culture shift. It will require a thorough and adequately resourced communication plan. It may include identifying and showcasing individuals or teams within divisions with exemplary data management and analytic practices. Some of these individuals may also serve as formal or informal educators or influencers of their peers. Other informal processes, such as communities of practice, can build collaboration, knowledge sharing and a sense of common purpose. The success of the roll-out of the program will be maximized if, in the early stages, the University identifies and works with a cadre of divisions and individuals willing to champion the advancement of data governance at U of T.

To achieve the desired outcomes outlined in the foundational report, it will be essential to provide robust training, tailored for each type of data governance role, ensuring that the right people obtain the necessary information and skills. A needs assessment should be conducted to inform the development of training programs. Multiple channels for delivery of data governance training will be available. These include – but are not limited to –developing knowledge management materials peer-to-peer workshops, and courses developed in collaboration with expert colleagues at CTSI, the Faculty of Information, the Department of Statistical Sciences, the Library, and so on. One initiative we have learned from Notre Dame University is the creation of a training program to certify analysts are proficient in managing and analysing data responsibly. We could also draw on the vast expertise at U of T to create a “College of Reviewers” whose members could be tasked with a number of duties including vetting and reviewing larger-scale analyses prepared to support institutional or divisional administrative policies and decisions.

Over time, with a shared understanding of good data governance and a deeper appreciation of the value of the data we hold, we envision a culture shift toward more open access to data. As stated in the foundational report, “institutional data, properly understood and studied, can help guide decisions, policies, and strategies. Such data can produce unexpected insights or ideas,

revealing opportunities for the university to improve its operations and better serve its broad community – students, faculty, staff, alumni – and society at large."

Data Infrastructure and Security

The University will require the appropriate infrastructure to support our data governance, data management and analytical activities. This will include an appropriate platform and tools for the creation, management, analysis and storage of data and for the documenting of metadata. We will need to develop physical, technical and procedural approaches to regulating data access and supports for high quality data analysis. As with the introduction of other new technologies at U of T, technology decisions for data governance will be informed by user needs, supported by colleagues in Information Technology Services (e.g. Shared Security Operations and EASI), the IRDG team and other partners.

The University is migrating some of its IT functions from an on-premises environment to a secure Microsoft Azure cloud environment. This next-generation data platform will be available to all divisions to securely store the data that they currently collect and maintain on their own servers. This will relieve divisions of the and logistical burden of developing their own computational resources, secure data infrastructures, and substantial financial human resources to manage the datasets.

While the final specifications for this cloud-based platform will be determined in consultation with divisions, we anticipate the infrastructure will include:

- real time (or near real time) copies of the student information system (ROSI) database and related NGSIS systems such as degree explorer and the course information system, allowing administrators to process operational transactions without putting pressure on the on-premises system during peak activity times;
- copies of institutional databases such as ROSI, FIS, ARBOR and HRIS that have been transformed, cleaned, and enhanced with variables from other institutional databases for analytic purposes. This will include the capacity to retrieve snapshots of data for specific dates in the past. This should obviate the need for divisions to create local shadow databases, eliminating duplication of effort and providing a single source of "truth" for analytics requiring data from ROSI, HRIS, FIS, etc.;
- a secure workspace where authorized users can work with these 'verified' analysis-ready institutional data sets at a granular level and link them, as required, to other 'verified' institutional data sets, including those currently in the possession of the divisions;
- analytic tools to support a range of users' needs, from basic reporting templates through to more sophisticated software such as R, Python and machine learning tools;

- documentation of the datasets in the repository and the data fields within those datasets;
- a system to facilitate documentation of metadata, including information on how the data were derived, to give context and to understand why the same term may have different definitions, sensitivity of the data, and any restrictions on their use;
- a common record-level identifier to improve linkage across databases;
- an identity management system for users to facilitate role-based access;
- physical, technical, and procedural safeguards consistent with U of T's Information Security Council guidelines.

As the institutional data governance program matures, we anticipate that new technology and processes will encourage divisions to migrate their data and join this secure cloud platform. While divisions may choose to not (fully) use the resource, it is important to note that divisions remain responsible for ensuring that any data with which they interact are secure under the U of T Policy on Information Security and Protection of Digital Assets (2016) and conform with FIPPA and all other relevant legislation.

The Institutional Research and Data Governance Team

Through a re-alignment of existing teams within Planning & Budget (P&B), a consolidated Institutional Research and Data Governance (IRDG) team has been created, building on the strength of the existing partnership with the Business Intelligence (UTBI) team. An organizational chart is included in Appendix C. The IRDG team will continue to provide the institutional research[2] and business intelligence services they have always provided, over time repositioning this aspect of their work into a Reporting and Analytics service and expanding as resources permit. The team will also create, implement and oversee the institution-wide data governance program.

Towards an Institutional Data Governance Program lays out the broad mandate of an Institutional Research and Data Governance team:

[2] Institutional research is a set of activities that support institutional planning, policy formation and decision making. (Saupe, J. L. The Functions of Institutional Research (2nd), 1990. Available at https://files.eric.ed.gov/fulltext/ED319327.pdf)

> "The IRDG team should focus on collaborating with, and supporting, the divisions in the development and operation of the Program. The team should promote institutional consistency, sharing and assessing best practices to ensure that the University's institutional data assets are managed so as to enhance their value, in accordance with the University's data governance principles."

We envision that the IRDG team, in collaboration with divisional colleagues, will develop guidelines and procedures for the broader institution-wide data governance program and assist divisions in developing their own more specific data governance plans. Through a combination of its website, communities of practice, training, and personalized assistance, the team will help colleagues navigate the complex and distributed world of data and analysis at U of T. The team will support divisions integrate data governance into their data management and use practices, with the aim to enhance reliable analytics and reporting capacity, to reduce duplication of data, make efficient use of shared technology infrastructure, and streamline data processes wherever possible.

Structuring the Institutional Data Governance Program

Towards an Institutional Data Governance Program lays out several principles which will guide the structure of our program and it is important to keep these in mind as the program evolves. The foundational paper also describes a diverse array of units and offices with which the IRDG team will collaborate and coordinate. As with all services offered at the institutional level, the IRDG team will build a network of subject matter experts and liaison colleagues across divisions. This is similar to the model adopted by the University for FIPPA purposes, whereby each division has a Freedom of Information Liaison (FOIL). We can imagine that each division may designate one or more data governance liaisons. As initiatives are undertaken, this divisional liaison will identify appropriate colleagues with the relevant expertise to participate in specific data governance activities. Examples of common data governance roles and responsibilities are included in Appendix D.

Not only will data governance be implemented institutionally and within divisions, but activities will take place at varying organizational levels:

- Strategic leadership of the program will call for executive oversight of the broad goals and directions of the program;
- Senior leadership in academic and shared service divisions will carry the role of tactical implementation – likely at the level of Vice Dean, AVP, CAO, for example;

- Operational activities will be undertaken by a broad range of staff who interact with data, conduct analysis, write reports, create dashboards and generally provide decision-support.

Initially, we anticipate that considerable activity will occur at the tactical level, with active guidance and support from the strategic level, as guidelines and procedures are being developed, best practices are being shared, communications and training are being rolled out, new technologies are being adopted and the culture is shifting. This will have short to medium-term resource implications that must be taken into consideration. Once the formal data governance program has been established, we anticipate that the majority of data governance activities will be operational in nature and will occur at that level. It would be naïve to believe that long term resourcing of the program will not be required at all, however there is a clear case that modest investments in data governance and the migration to a secure cloud platform could return divisional benefits in terms of optimizing their data management processes, enhancing their IT infrastructure while reducing their IT infrastructure administration, and, perhaps more importantly, reducing risk.

Operational level

The foundational report articulates our overarching principle:

> "Institutional data are a valuable university resource over which the university community has a duty to exercise good stewardship – that is, the careful and responsible management and use of the data entrusted to its care."

All who work with data exercise some aspect of stewardship at the "operational" level. Larger divisions may have several individuals who take on very specific data roles while smaller divisions may have a single individual who does this as one small part of their larger role. Rather than being a position or a title, data stewardship, and the underlying roles, reflect an individual's responsibility or accountability for how they work with data. At the operational level, some staff may be accountable for the quality of data definitions and their metadata. Others may be accountable for making certain that data are produced following the business rules, and are entered in a timely fashion. If not directly responsible for data entry, they may be responsible for ensuring the appropriate people are apprised when data have been updated, when they have not been received, or when there are problems with data accuracy. Staff who use data are responsible for being knowledgeable of the relevant laws, regulations and University guidelines and procedures, for applying appropriate safeguards when using the data, and for using appropriate analytic techniques and documenting these accordingly. They should ensure they have gained sufficient insights into the data they are analysing to appreciate the limits of the validity and reliability of the data and the subsequent impact of this on the limits of any analysis. They will consult with responsible individuals at the tactical level (see below) for guidance.

For those who interact with institutional data, where it makes sense, we propose that their data-related roles be formally recognized in their job descriptions, similar to the way that Finance, HR and IT responsibilities are included in job descriptions. However, it may not be advisable to include formal titles of "data steward" in job descriptions, as it could be inferred that only those designated with this label carry the stewardship responsibilities described above. Some may be formally trained; others may have taken on a data role more informally. In all cases, training of staff will be an ongoing joint responsibility of staff and management, in divisions and institutional offices.

Tactical Level

It is at this level where there is the greatest potential for added value through a formal data governance program. It is also the most challenging level, as this is where we seek to develop common protocols for data access, data quality, responsible data use and to harmonize definitions across divisions to permit cross-institutional analyses.

There are several possible ways to organize this activity. A common approach is by subject matter areas known as "data domains", such as advancement, finance, students, and so on. Examples of common data domains are provided in Appendix E. Each data domain may be led by a subject matter expert at a senior management level who is formally accountable for the data generated and consumed within that data domain. They are also responsible for communicating data governance guidelines and processes to all stakeholders in their domain. These individuals are often called either "data domain stewards" or "data trustees", and they usually are identifiable in the organizational chart. For this report, we will use the term "data trustee". For example, the University Registrar would usually be the data trustee for student data; the Chief Financial Officer for financial data; the Chief Human Resources Officer for employee data. Whereas, at the operational level there may be several people with data stewardship responsibilities in a division, it is more common to have only one data trustee within the organization for any given domain; further sub-domains and other data governance functions may be created and assigned. The IRDG Director will be available to work with divisions to identify the appropriate data domain structure and data trustees, in consultation with, and subject to, the approval of an executive steering committee described below.

Data trustees will strike working groups that draw in subject matter experts from across divisions, to participate in time-limited, cross-divisional, domain-specific working groups. Working groups will include representatives from both the divisions that will be using the data and data custodians, who manage systems that facilitate data collection and/or use.[3] Further,

[3] Examples of enterprise datasets include ROSI, FIS, HRIS, RIS, ACORN, Quercus, Slate, Infosilem, etc.

chairs of each of these domain-specific working groups will meet in one or more cross-domain working group(s), as appropriate, to harmonize the data governance guidelines and processes developed in their respective data domain working groups. Chairs may designate another member from their working group to be represented in the cross-domain working group(s).

The goal of these working groups is to develop common processes, procedures and guidelines around data quality and responsible data use, using existing processes, frameworks and definitions as the starting point, where appropriate. In addition, an early task of these groups will be to advise the IRDG Director on priority matters to pursue. Staff at the operational level have considerable insights into the complexities and issues concerning the datasets with which they routinely interact, and wherever possible, their input will be sought when making decisions that affect day-to-day operations. In addition, these working groups will seek input from students, staff, faculty, alumni and other stakeholders, as appropriate.

There will inevitably be requests for non-routine use of institutional data. A process and guidelines are already under development (led by the Provost's office) for requests related surveys of faculty, staff and students for scholarly research. Access to institutional data for other non-survey based scholarly research will be included in within the overall institutional data governance program. These and other non-routine requests may require consultation with members of the "College of Reviewers".

Strategic level

Accountability and responsibility for data governance reside within the *2007 Policy on Information Technology* under the authority of the Vice-President & Provost. This authority is delegated at the strategic level, to an Institutional Research and Data Governance (IRDG) Executive Steering Committee. It will set the highest level of direction and policy and appoint members of a cross-divisional Data Governance Council and a cross-divisional Reporting and Analytics Council. It will receive and review regular data governance status reports at their meetings. However, some of the responsibility for the oversight function will be delegated to Councils. As the program is being developed, the strategic level will be more actively involved on a number of fronts. Once the program is mature, the strategic level will continue to play an important role, albeit more in an oversight capacity.

The existing Institutional Data Hub Executive Steering Committee has overseen the development of the data governance program to date, and ensured integration with business intelligence activities. This Executive Steering Committee will be reconstituted and adapted to provide strategic direction for the data governance program as well as a more formal reporting and analytics program; the latter evolving from the committee's oversight of business intelligence activity.

New terms of reference will be developed for the Executive Steering Committee and will include the following:

- Establish and champion the data strategy of the University;
- Submit funding proposals for the data governance and reporting and analytics programs to the appropriate budget committees;
- Recommend policies and guidelines for Governing Council approval;
- Appoint members of a Data Governance Council and approve terms of reference;
- Appoint members of a Reporting and Analytics Council and approve terms of reference;
- Provide oversight for the Data Governance Council and the Reporting and Analytics Council;
- Appoint members to the initial "College of Reviewers" and establish mandate; the College of Reviewers will report into the Reporting and Analytics Council

A cross-divisional Data Governance Council, with direct accountability to the Executive Steering Committee, will:

- Provide guidance to the IRDG Director to ensure the DG Program goals, strategic initiatives and operational activities are aligned with the University's mission, objectives and obligations;
- Approve priorities for the data governance program, including the development of a DG Roadmap;
- Approve data domains and appoint data trustees;
- Leverage IRDG team and its working groups to ensure broad consultation on initiatives and/or seek recommendations around best practices;
- Act as a mediation panel to resolve complex data governance issues;
- Provide final approval of processes, frameworks and guidelines that do not require Executive Steering Committee approval;
- Establish standing committees (e.g. Data Disclosure), as required;
- Monitor progress of the DG program including the status of data governance initiatives, activities, risks and issues;
- Approve and monitor data governance metrics to support program evaluation and program audit functions; track progress on remediation of risk items;
- Review and recommend change management, education and communication strategies to ensure the adoption of data governance;

- Act as an oversight body for the DG Program, including recommending annual resource allocations to support implementation of the DG Roadmap and program operations.

The Executive Steering Committee is also expected to oversee a cross-divisional Reporting and Analytics Council, an evolution of the existing BI Leadership Committee. The Executive Steering Committee will appoint members of the Reporting and Analytics Council and approve terms of reference in the near future. Subject to consultation and finalization with divisional partners, the Reporting and Analytics Council may consider some of the following functions:

- Promote the strategic use of data in decision-making at the University;
- Establish strategic investments for institutional analytics programs;
- Leverage IRDG and its working groups to ensure broad consultation on requirements and /or seek recommendation around best practices;
- Identify analytics requirements related to resources, training, services, infrastructure and tools to meet the needs of the analytics community;
- Approve priorities for shared services projects (e.g. development of institutional data marts, dashboards and advanced analytics solutions);
- Oversee standing committees (e.g. College of Reviewers), as required;
- Approve and monitor R&A metrics to support opportunities for program operations;
- Act as an oversight body for the R&A Program, including recommending annual resource allocations to support implementation of key initiatives.

Program Audit

We anticipate that most requests for access to data will be relatively routine. An audit mechanism will be developed to check that those authorized to access the data are using the data appropriately. This can be a combination of random retrospective audit and real-time flagging of particularly sensitive datasets or data fields. The approach to audit should be formative in nature, in the spirit of quality improvement as opposed to penalty. However, as with many breaches of University policy or guidelines, sanctions should be an option available to ensure accountability and integrity within the data governance program.

Program Evaluation

It can be difficult to quantify the impact of an effective data governance program. Data quality measures are relatively easy to establish and evaluate. By contrast, evaluating responsible data use and establishing a causal link with increased data-informed decision making – and

subsequent improvements to university operations and services – are much more difficult to formally evaluate. Consideration should be given to evaluation metrics early on in the program development and in every project plan. The University can look to peer institutions and adapt data governance evaluation models as appropriate. U of T is in the planning stages of engaging with other U15 universities on the subject of data governance and this will further inform our program as discussions ensue.

Appendices

Appendix A: List of Recommendations

R1. Overall approach

We recommend an approach that is influenced by a particular model called "non-invasive data governance" which draws upon an organization's existing people, processes, and infrastructure. This approach is collaborative, empowering and supports those who are already engaged in a wide range of informal data governance activities. We believe it fits well with our culture and the highly distributed administrative structure of the University.

R2. People and culture

We recommend a robust and well-resourced communication strategy and training program. Ongoing communication and transparency of the data governance program – its progress, challenges and successes – will help build momentum and change. Raising awareness of the program and explaining its value and importance in achieving this goal are critical to fostering this culture shift. Training programs should be informed by a needs assessment.

R3. Data Infrastructure

We recommend that divisions be encouraged to use the Microsoft Azure cloud-based platform that is being developed by EASI to securely store their data and conduct their analyses. This platform will also serve as an important vehicle to accelerate the uptake of the data governance program across the institution. Specific infrastructure and technology decisions will be informed by user needs and supported by colleagues in IRDG, Shared Security Operations and other partners. We will develop physical, technical and procedural approaches to regulating data access.

R4. The Institutional Research and Data Governance Team

We recommend that the IRDG team focus on collaborating with, and supporting, the divisions in the development and operation of the institutional data governance program. The team will promote institutional consistency, sharing and assessing best practices to ensure that the University's institutional data assets are managed so as to enhance their value, in accordance with the University's data governance principles.

R5. Structuring the Data Governance Program

We recommend that the program be structured across three levels of activity: operational, tactical and strategic. We also recommend the establishment of an Executive Steering Committee, a Data Governance Council, a Reporting and Analytics Council and operational sub-committees such as a "College of Reviewers". We recommend that responsibility for data stewardship be formally recognized in job descriptions.

R6. Program Audit

We recommend that audit and feedback be incorporated as appropriate into any data quality and responsible data use initiatives to inform our progress in achieving our DG objectives and to meet our accountability obligations.

R7. Program Evaluation

We recommend that evaluation metrics be established early on in the program and in every project plan.

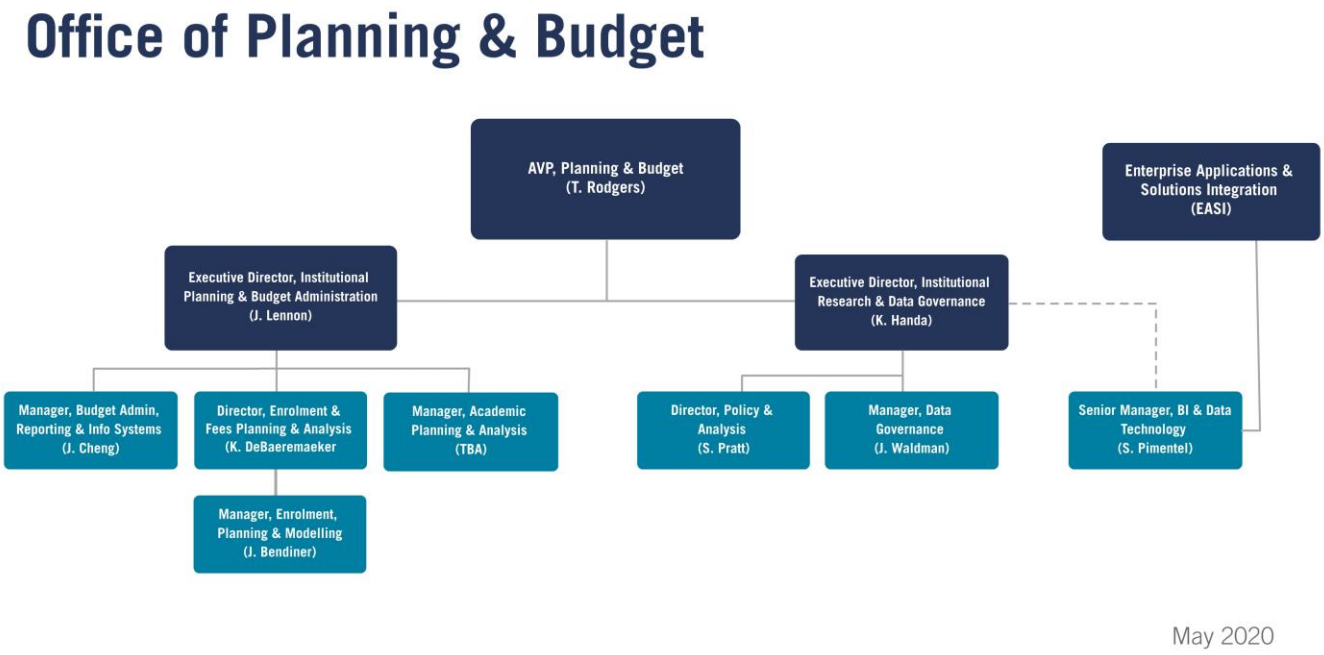
Appendix B: Current U of T Policies and Guidelines for Data Governance Context

Year	Name and Scope	Sponsor / responsible
2006	Access to Information and Protection of Privacy at the University of Toronto, Statement Regarding	Secretary of Governing Council
2016	Information Security and Protection of Digital Assets, Policy on Adopted as a 'measure to protect the privacy, confidentiality, integrity, and availability of Digital Assets, including information systems that store, process or transmit data. This Policy applies to all academic and administrative units, third-party agents of the University, as well as any other U of T affiliate that is authorized to access institutional data, services and systems. All U of T campuses, divisions, departments and other administrative or academic organizational units shall deploy and use IT systems and services in a manner consistent with the University's research and teaching mission, while vigilantly mitigating security risks to Digital Assets, including data during storage, transit, use and disposal. It is the obligation of all University community members to protect information that is created by them and stored by the University and its authorized delegates to its defined principles and standards.' Guidelines • Information Security Guidelines (2013) • Security guidelines mapped to data classification for sensitivity. • Several guidelines related to infrastructure	President or designate (VP-OREP) has overarching responsibility for the protection of U of T's Digital Assets; authorized to approve Procedures & Standards and to promote Guidelines
2007	Information Technology, Policy on Concerned with all of the University's information technologies and services, including, but not limited to hardware and software such as personal computers, servers, personal digital assistants, electronic mail, Web services, learning management systems, Internet and network access, departmental and institutional network infrastructure, telephone, fax and voice-mail and other forms of information and communication technology that exist today or may be developed in the future. Appropriate Use of Information and Communication Technology (Provost)	Vice-President and Provost

2009	Academic Records, Guidelines Concerning Access to Official Student Academic Records The University supports appropriate access to, and privacy of, official student academic records consistent with its commitment to the requirements of Freedom of Information and Protection of Privacy Act (FIPPA). These guidelines are intended to outline university-wide procedures and criteria for access, privacy, custody, and retention of the academic records of students of academic divisions of the University in order to ensure clarity and consistency of practice.	University Registrar
2006 2007	Guidelines and Procedures Regarding Access to University of Toronto Faculty, Students, and Staff as Research Subjects Provides "the principles and processes for researchers who wish to conduct research with students, staff and faculty at U of T or *to gain access to data about students, staff and faculty held by the University of Toronto*. The aim is to prevent survey fatigue, protect confidentiality and employee rights, and ensure that access does not conflict with any current or planned research to be conducted by the University or its administrative/academic units." Requests for data should "protect the confidentiality of students, staff, or faculty and are in accordance with the purpose for which the data was initially collected."	Vice-President and Provost
2007 2016	U of T File Plan University of Toronto Libraries Records Management Services (UTARMS) has developed the U of T File Plan which is described as "the standard of record-keeping practices for all university records".[4] Provided for both institutional administrative records (paper, digital, other). Its scope is to provide "a classification scheme and retention/disposition guidelines for administrative records" and its goals are related to providing a classification framework for University records in five main subject areas (Administration; Buildings & Properties; Equipment & Supplies; Finance; Human Resources).	Chief Librarian/University Archivist

[4] Section 1.1, page 6. https://utarms.library.utoronto.ca/sites/utarms.library.utoronto.ca/files/u-of-t-file-plan/file_plan_introduction_reformatv2.pdf

Appendix C: Organizational Structure of Institutional Research and Data Governance Team



Appendix D: Examples of Common Data Governance Roles and Responsibilities

Data Role	Description	Examples at U of T
Data Consumer	Individual or organization inside or outside the University that consumes or uses institutional data obtained from the University. A data consumer is recognized as any user granted access by the University to view and use institutional data for business, government or research purposes	All who consume data
Data Custodian	A data custodian is a unit that manages any systems or data compilations that enables and facilitates data collection and use of data by data trustees and stewards. A data custodian can also be a trustee in situation where data is auto-generated through systematic data processing and collection.	Business Intelligence units Academic & Collaborative Technologies (ACT) Divisional and central IT units T-card Office
Data Steward	An individual (or designate) that supports the day-to-day management of the data asset. The data steward ensures the quality and integrity of data provided to internal or external stakeholders. The data steward may be a front-line staff member or in a supervisory administrative role.	Staff or supervisors in central and divisional positions: • Financial aid • Student accounts • Enrolment Services • Divisional Registrars • Student Services • Advancement • Research • Facilities & Services • Finance
Data Trustee	A senior director or executive level individual (or designate) that is accountable for the data generated and consumed. They have the authority to collect, use and disclose data under government legislation and policies, to make decisions on the data, such as whether to provide data for disclosed uses, what safeguards should be in place to manage data risks, and classification and	Senior director or executive level individual in central or divisional positions: • Financial aid • Student accounts • Enrolment Services • Divisional Registrars

Data Role	Description	Examples at U of T
	access decisions regarding the collection, transformation, use, retention and disposal.	• Student Services • Advancement • Research • Facilities & Services • Finance

Appendix E: Examples of Common Data Domains in the Higher Education Context

Data domains are typically organized in a hierarchy with the top level representing the most basic areas of administrative activities. As a rule of thumb, data domains, particularly the top level, would change infrequently. Data Governance standards recommend five to nine data domains for the top level of the hierarchy however some flexibility with the number of top-level domains may be better suited for an institution as large and complex as the University of Toronto. The following is an example (i.e. NOT comprehensive) of a multi-tiered model displaying a subset of the many domains that will eventually be established.

Level 1 Domain Areas	Level 2 Domain Areas	Level 3 Domain	Level 4
Advancement	Advancement		
	Alumni Relations		
People	Human Resources		Divisional Breakdown
	Academic HR		
	Equity & High Risk		
	Sexual Violence		
Finance	Finance		
	Budget		
	Audit		
Operations	Facilities		
	IT		
Research & Innovation	Sponsored Research		
	Research Partnerships and Innovation		
	Research expertise / bibliometrics		
Students	Recruitment		Divisional Breakdown
	Admissions	Direct Entry	
		Second Entry	
		Graduate	
	Enrolment	Direct Entry	
		Second Entry	
		Graduate	
	Curriculum		
	Co-curricular		Divisional
	Accessibility Services		
	Housing		
	Student Advising		
	Student Finance	Student Fees	
		Student Aid	
		Student Employment	
Library	Online subscriptions		