Original Approval Date: December 15, 2015

Parent Policy: Records Management Policy

Institutional Data Management and Governance Procedure

Office of Administrative Responsibility:	Office of the Vice-President (Finance and Administration)
Approver:	Provost and Vice-President (Academic) and the Vice-President (Finance and Administration)
Scope:	Compliance with this university procedure extends to all Academic Staff and Colleagues and Support Staff as outlined and defined in Recruitment Policy (Appendix A and Appendix B).

Overview

The Records Management Policy intends to provide a common basis of understanding institutional records as a business-critical university resource and asset, and of the responsibilities accompanying use of institutional records and stewardship of the University of Alberta community.

Purpose

This procedure supports the Information Management, Information Technology, and Records Management Policies (including the University's Privacy and Access to information policies) by clarifying activities which relate to the creation, collection, storage, maintenance, protection, cataloguing, use, dissemination and disposal of **institutional data** whether the data is:

- in electronic form or in hard copy,
- held centrally in major administrative systems, or in faculties, departments or other academic or administrative offices, or;
- in raw form or is derived, summarized or aggregated.

PROCEDURE

The following outlines the basic procedure expected for data management, access and use.

1. Wherever possible, data should be collected and maintained once, at the source, and made available to all members of the University who have a legitimate business need for the data for academic, research or administrative purposes.
2. Institutional data must be used only by those persons duly authorized to access and use the data by virtue of their position at the University of Alberta, and only for the purpose for which use has been authorized. Authorization of access to data is not transferable.
3. Every data user must recognize that the University's institutional data and information derived from it are potentially complex. It is the responsibility of every data user to understand the data they use, and to guard against making misinformed or incorrect interpretations of data or misrepresentations of information.
4. Institutional data must not be accessed or manipulated for personal gain, or out of personal interest or curiosity.

5. Data users must carry out all tasks related to the creation, storage, maintenance, cataloguing, use, protection, dissemination and disposal of institutional data responsibly, in a timely manner and with the utmost care and in compliance to the University's Information Management, Information Technology, and Records Management Policies.
6. Data users must not knowingly falsify data, delete data that should not be deleted or reproduce data that should not be reproduced.
7. Access to institutional data for research purposes may be granted by the appropriate **Data Steward** and its use is subject to University policies on privacy, security, intellectual property and research ethics as well as to provincial and federal privacy legislation. Policies and standards for the use and management of research data and information are located in the UAPPOL suite of Research Policies.
8. Institutional data should be readily accessible to authorized users to view, query or update.
9. Institutional data must be stored in such a way as to ensure that the data is secure, and that access is limited to authorized users. Secure storage of institutional data is a joint responsibility of system and network administrators, database designers, application designers, and the data user who must ensure that passwords and other security mechanisms are used. Data stewards shall seek guidance from the University's Information Privacy, Security, and Records Management offices to ensure adequate information management, privacy, and security controls are in place before deploying new (or significantly changed) systems or information flows.
10. When electronic data is no longer required for administrative, legal or historical reasons it should be deleted in accordance with appropriate University records retention and disposition schedules as managed by the University's Records Management Office.
11. Data stewards will be responsible for defining and monitoring data quality standards to reduce risk and improve data reliability.
12. External users accessing data must comply with the Freedom Of Information and Protection of Privacy Act and the University's Information Management, Information Technology, and Records Management Policies.

Institutional data can generally be assigned to one of four categories[1]:

Restricted - This classification is for information that is extremely sensitive and could cause extreme damage to the integrity, image or effective service delivery of the University of Alberta. Extreme damage includes loss of life, risks to public safety, substantial financial loss, social hardship, and major economic impact. Restricted information is available only to named individuals or specified positions. (Examples include restricted spaces, credit card numbers, social insurance numbers, and personal medical records).

Confidential - This is for information that is sensitive within the University of Alberta and could cause serious loss of privacy, competitive advantage, loss of confidence in University programs, or damage to partnership, relationships and/or reputation. Confidential information includes highly sensitive personal information. Confidential information is available only to a specific function, group or role. (e.g. personnel files, including personal salary data, and 3rd party business information submitted in confidence,).

Protected - This is for information that is sensitive outside the University of Alberta and could impact service levels or performance, or result in low to medium levels of financial loss to individuals or enterprises, loss of privacy, loss of confidence in University programs, or damage to partnerships, relationships and/or reputation. Protected information includes personal information, financial information or details concerning the effective operation of the University of Alberta. Protected information is available to employees and authorized non-employees (contractors, sub-contractors and agents) possessing a need to know for business-related purpose. (e.g., grades, dates of birth, and personal contact information other than University email addresses).

[1] These definitions and classifications reflect the Government of Alberta information security classification standard.

Unrestricted - This is for information that is created in the normal course of business that is unlikely to cause harm. Unrestricted information includes information deemed public by legislation or through routine disclosure or active dissemination. Unrestricted information is available to the public, employees and contractors, sub-contractors and agents working for the University. Or, where the information has not been made available to the public, if it were, it would not have any harmful or negative effect. (e.g. university email addresses, accounting chart of accounts).

Roles and responsibilities

To promote and safeguard the integrity and security of, and appropriate access to institutional data, the following roles and responsibilities are defined. It is anticipated that any one person could participate in more than one of these roles.

A. Data Owner

The Governors of the University of Alberta is the legal entity that is the owner of the University's institutional data. Individual units or departments have stewardship responsibilities for particular elements and/or aspects of the data.

B. The University Data Steward

The **University Data Steward** is the Provost and Vice-President Academic for academic data and the Vice-President (Finance & Administration) for administrative data. The University Data Steward is the institutional authority on all matters pertaining to the management and use of the University's institutional data and institutional information identifies and confirms the official version of all university information, and ensures that the university has adequate policies, processes and practices in place to support its needs for information. The authority of the University Data Steward is subject to the authority vested in the Head of the University for the purposes of the Freedom of Information and Protection of Privacy Act and any authority delegated thereunder.

C. Data Steward(s)

Data Stewards are University officials who have planning and policy-level responsibilities for data in their functional areas. These include administrative, operational, academic and information technology staff.

As a group, the data stewards, with the support of technical data experts, are responsible for developing policies, guidelines and standards, and for establishing procedures for university-wide data management activities.

As individuals, the data stewards have specific responsibilities to manage data to maximize its integrity through determining the authority to access, use, define and control the quality of data that pertains to their functional areas and/or is deemed to be under their purview. Data stewards are responsible for identifying the access category (restricted, confidential, protected, unrestricted) of data elements under their authority, and for determining what limitations or conditions apply to access. Caution and judgment appropriate to the nature of the data should be used in determining the classification of aggregate data that, if made widely available, may create inappropriate accessibility to underlying protected information. As such, discretion in reporting small cells should be coincident with the sensitivity of the information. Commonly accepted reporting practice includes suppressing cell counts of 5 or less, but a higher level of suppression may be warranted depending on the nature of the information.

Because data and responsibility for them have traditionally been organized along functional lines, data stewards will generally follow the same organization structures. Some data stewardship responsibilities and authority, however, may not be clearly delineated and may be shared or delegated to a group of data stewards.

Access to institutional data for the purposes of research may be granted by the appropriate data steward, whose responsibility it is to ensure that the access is in compliance with the Access to Personal Information for Research/Studies Procedure.

Both as individuals and collectively, the data stewards have a responsibility to promote and encourage an institutional view of the data resource and to ensure that its use is in line with institutional policy. They will ensure appropriate consultation occurs when significant data changes are contemplated that may impact the work of others using the same data.

To best operationalize the requirements, procedures and processes developed by Data Stewards regarding institutional data should:

- Ensure that institutional data elements and common shared data standards and structures are identified, documented.
- Catalogue the kinds of data contained in various data bases within their area(s), and identify the level of access and security required for access to the data.
- Develop processes for requesting, granting, and documenting access to data elements or data views, including procedures for requesting and granting access to data for legitimate research purposes and to support data-driven decision making in university units.
- Develop processes and schedules for identifying and deleting all institutional data no longer required for the purposes for which it was created or collected (see records retention procedure).
- Coordinate and communicate to other impacted data stewards significant changes or considerations in data definitions, uses or security, particularly those that affect public and institutional reporting.

A listing of administrative areas with data stewardship roles is outlined in Appendix A of this procedure.

D. Technical Data Experts

Technical data experts are responsible for the coordination of institutional data-related activities and data management. The technical data expert(s) must recognize and promote the importance of data as a valuable institutional resource requiring consistent management of the creation, storage, maintenance, protection, cataloguing, use, dissemination and disposal of data. Technical data experts have responsibility for promoting policies, guidelines, procedures and standards that allow the University to ensure the integrity, security, accessibility and usefulness of data.

Technical Data Experts oversee the safe transport and storage of data. While content is important to them, their focus is on the underlying infrastructure and activities required to keep the data intact and available to users. They collaborate with the Data Stewards to implement data transformations, resolve data issues, and collaborate on system changes.

Generally, this role would apply to directors, mangers or supervisors that have a direct responsibility for one of more institutional information systems and include information technology and data architecture experts.

E. Data users

Individuals who produce and use institutional data as part of their assigned duties or in fulfillment of their role at the University are data users. **Data users** are responsible for complying with the institutional data policies outlined in this document, and for following procedures established by data managers. Since data may cross functional lines, data used by any one data user may have different technical data experts and data stewards.

Non-compliance

If questions about access, compliance or use of data arise and cannot be resolved through institutional processes or appear to have a significant impact on data integrity and information processes the matter must be resolved by the University Data Steward(s).

If there is a reason to suspect that laws or university policies have been, or are being violated, or that continued access poses a threat to normal operations or the reputation of the University, access privileges may be restricted or withdrawn by the Data Owner, the appropriate University Data Steward, or the appropriate Data Steward.

Following the relevant University policy, procedure or faculty or staff agreement, the University may take action against anyone whose activities are in violation of the law or of this procedure. The actions taken may include, but are not limited to:

- Revocation of access privileges
- Disciplinary action for employees, following appropriate processes in the faculty and/or staff agreements
- Disciplinary action for students under the Code of Student Behaviour
- Legal action that could result in criminal or civil proceedings

DEFINITIONS

Definitions should be listed in the sequence they occur in the document (i.e. not alphabetical).

Any definitions listed in the following table apply to this document only with no implied or intended institution-wide use. [▲Top]	
Institutional data	That data which is created, collected and stored by the University, or any office of the University, in support of its administrative and operational functions. Such data may relate to students, faculty, employees, donors, members of the Board of Governors, members of the Senate, researchers, alumni, prospects, patients and other members of the University community and may include personal, academic, financial, curricular, and other information Data created by or deriving from research and scholarly activities, however, is outside the scope of this definition of institutional data and is governed by the *Research Records Stewardship Guidance Procedure.*
University Data Steward	The University Data Steward is the Provost and Vice-President (Academic) for academic data and Vice-President (Finance and Administration is the University Data Steward for administrative data. The University Data Steward is the institutional authority on all matters pertaining to the management and use of the University's institutional data and institutional information, identifies and confirms the official version of all university information and ensures that the University has adequate policies, processes and practices in place to support its needs for information.
Data Steward	University officials who have planning and policy-level responsibilities for data in their functional areas. They have responsibility for the management, access, use, definition and quality of data that pertains to their functional areas or is under their purview. The listing of areas with formal data stewardship roles for key institutional data is noted at Appendix A.
Data Users	Individuals who need and use institutional data as part of their assigned duties or in fulfillment of their role at the University are data users. Data users are responsible for complying with the institutional data policies outlined in this document, and for following procedures established by data managers. Since data may cross functional lines,

	data used by any one data user may have different data stewards.
Technical data experts (or custodians)	Technical custodians primarily oversee the safe transport and storage of data (e.g. database administrators, IT application support/development etc.). Information systems content is importance to the experts, but their focus is principally on the underlying infrastructure and activities required to keep the data intact and available to users. They may also ensure consistent application of security and privacy considerations, in collaboration with the appropriate offices. Technical stewards collaborate with the Data Stewards to implement data transformation, resolve data issues and collaborate on system changes.

FORMS

Should a link fail, please contact uappol@ualberta.ca. [▲Top]

No Forms for this Procedure.

RELATED LINKS

Should a link fail, please contact uappol@ualberta.ca. [▲Top]

https://policiesonline.ualberta.ca/PoliciesProcedures/Policies/Records-Management-Policy.pdf

https://policiesonline.ualberta.ca/PoliciesProcedures/Procedures/Access-to-Information-and-Protection-of-Privacy-Procedure.pdf

https://policiesonline.ualberta.ca/PoliciesProcedures/Policies/Information-Technology-Security-Policy.pdf

APPENDIX A – Overview of Administrative Data Stewards.

This is not a complete listing of administrative data held at the institution but is intended to reflect the main institutional data that has use across the institution.

Area of institutional data	**Data Steward Area** (The Vice-Presidents, Vice-Provost, Director etc.. of each areas may assign a position in their area to formally undertake the stewardship role).	**Notes for consideration**
Undergraduate student data	Registrar's Office	Units and faculties may be stewards for additional data maintained.
Graduate student data	Faculty of Graduate Studies and Research	Units and faculties may be stewards for additional data maintained.
Financial reporting information	Financial Services	Units and faculties may be stewards for additional data maintained (e.g., financial transaction support, expense claims, invoices).
Budget information	Resource Planning	
Research grant administration	Research Services Office	
Research ethics (including animal ethics approvals)	Research Ethics Office	
Human resources information (e.g. payroll, benefits and pension support)	Human Resource Services	Units and faculties may be stewards for additional data maintained (e.g., HR competition files, pay records).
Institutional data warehouse	Strategic Analysis	
Alumni and donor data	Advancement	
Building and space related data	Facilities & Operations	
OneCard data	Ancillary Services	
Residence information	Ancillary Services	
Parking Services data	Ancillary Services	
CCID and central log-in information	Information Services and Technology	
University Library Systems	Learning Services	

Area of institutional data	**Data Steward Area** (The Vice-Presidents, Vice-Provost, Director etc.. of each areas may assign a position in their area to formally undertake the stewardship role).	**Notes for consideration**
Directory service information	Information Services and Technology	
Procurement records (contracts and payment information)	Supply Management Services	
Website analytics and related statistics	University Digital Strategy	
Utility Data	Utilities	