Original Approval Date: December 15, 2015
Most Recent Approval: July 11, 2024
Amended: n/a

Parent Policy: Records Management Policy

Institutional Data Management and Governance Procedure

Office of Administrative Responsibility:	Performance, Analysis and Institutional Research (PAIR)
Office of Accountability:	Vice-President (University Services, Operations and Finance)
Approving Authority:	Associate Vice-President and Chief Analytics Officer

Purpose

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

This procedure supports the Information Management, Information Technology, and Records Management Policies (including the University's Privacy and Access to Information and Protection of Privacy Policy) by clarifying activities which relate to the creation, collection, storage, maintenance, protection, cataloging, use, dissemination and disposal of administrative **institutional data**, henceforth referred to as 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.

Definitions

A definitions table as attached establishes the terms used in this policy document and any unique rules of interpretation that apply to this policy document.

Scope/Application

Compliance with this policy document extends to all academic, support and excluded staff, student employees and academic colleagues as outlined and defined in the Recruitment Policy (Appendix A and Appendix B: Definitions and Categories).

Procedure

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

1. Wherever possible, data should be collected, entered and maintained once, at the source, and made available to all members of the University who have a legitimate business need for the data.

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 set in collaboration with the respective **Data Steward**, the Chief Information Security Officer (CISO) and the Information and Privacy Officer, and 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, inform the Data Stewards of any data issues, 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, cataloging, 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 based on their roles. 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.

13. Institutional data should be assigned one of the four information security classifications:

    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 a business-related purpose. (e.g., grades, dates of birth, and personal contact information other than University email addresses).

    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

The Governors of the University of Alberta is the legal entity that owns the University's institutional data, however, operational responsibility is carried out by the roles defined within this procedure.

To promote the integrity and security of, and appropriate access to institutional data, the following roles and responsibilities are defined:

A. **Data Owner**

Data Owners are senior members of the University of Alberta (UofA) that are ultimately accountable for the data quality of the University's institutional data and are assigned the authority to make decisions and enforce those decisions as it pertains to UofA institutional data. They are also voting members of the Enterprise Information Governance Committee.

B. **Enterprise Information Governance Committee (EIG Committee)**

Membership of the EIG Committee is made up of senior members of the university who are empowered to collectively move, approve, support, promote and enforce information governance activities throughout the university. Their primary responsibilities, as defined in the EIG Committee charter, are to approve policies, standards, roles, responsibilities and any other body required for information governance activities. They also have supporting roles which include developing and promoting information governance strategies, enforcing governance activities and resolving issues escalated from the Enterprise Information Governance Council.

C. **Data Steward**

Data Stewards are generally Director and Associate Vice -President level staff that champion and promote EIG Committee decisions. They take on operational and tactical roles for institutional data and are responsible for the data quality within their data sub-domains. They manage the storage, use, quality checks, processes and procedures needed to maintain the expected data integrity within their data sub-domains.

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. 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.

Further responsibilities of a Data Steward include the maintenance of documents pertaining to their functional areas which include, but are not limited to, processes, procedures, definitions, use, access, monitoring, measuring and reporting on data quality, defining and cataloging data, and ensuring the information governance RASCI is maintained and kept up to date.

D. Enterprise Information Governance Council (EIG Council)

The EIG Council is generally made up of Data Stewards and provides operational oversight, management, measurement and required monitoring on the effectiveness with respect to the university's institutional information.

They collectively support the development of strategies to be approved at the EIG Committee, form a point of escalation for data users on data matters, provide oversight, guidance and recommendations to the EIG Committee, and provide guidance and support on data integrity checks, naming conventions, categorization, and catalog details.

E. Report Developers

Report Developers are responsible for the development of reports and ensure that all data requirements from Report Owners are met and that all policies and procedures are followed with respect to the University's Information, Technical, Security and Privacy policies and procedures. They are also responsible for adhering to all information governance best practices, standards and guidelines that would be defined by the EIG Council. They must also have all reports fully cataloged and documented prior to release to the data owners.

F. Report Owners

Report Owners take on the role of the main point of contact for all matters related to those reports. They are responsible for the consistency and sustainability of their reports and that all fields are defined and cataloged before release to their stakeholders.

They are also responsible for the training and education needed on the use of their reports to ensure proper use is adhered to. This includes, but is not limited to, the intent of the report, the use, access, and sharing of the reports. They also take on the documentation pertaining to their reports which include processes, procedures, definitions, use, access and end user data quality expectations.

They are also responsible for reporting any issues that affect the performance, data integrity, or non-adherence to the University's policies, procedures and any standards thereof.

G. Information Technology (IT) Data Administrators

IT Data Administrators are individuals in IT who have operational level responsibility for data management activities related to the creation, storage, maintenance, security, and disposal of data.

Data administrators have responsibility for promoting policies, guidelines, procedures and standards that allow the University to ensure the integrity, security, accessibility and usefulness of data. These roles include, but are not limited to, architects, DBAs and data integration specialists.

Data administrators collaborate with Data Stewards to implement data transformations, resolve data issues, and collaborate on system changes. Generally, this role would apply to directors, managers or supervisors that have a direct responsibility for one of more institutional information systems and include information technology and data architecture experts.

H. **Data users**
Individuals who 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 stewards. Since data may cross functional lines, data used by any one data user may have different technical data experts and data stewards. All data users are responsible for reporting data issues to the respective data steward. Data quality, integrity and security is everyone's responsibility.

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 EIG Committee.

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, 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.
- Legal action that could result in criminal or civil proceedings.

Definitions

Any definitions listed here apply to this policy document only with no implied or intended institution-wide use.	
Data Owner	Data Owners are senior members of the University of Alberta (UofA) that are ultimately accountable for the data quality of the University's institutional data and are assigned the authority to make decisions and enforce those decisions as it pertains to UofA institutional data. They are also a voting member of the Enterprise Information Governance Committee.
Data Steward	Data Stewards are generally Director and Associate Vice President level staff that champion and promote EIG Committee decisions. They take on

	an operational and tactical role for institutional data and are responsible for the data quality within their data sub-domains. They manage the storage, use, quality checks, processes and procedures needed to maintain the expected data integrity within their data sub-domains 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 sub-domains. They are responsible for identifying the security classification (restricted, confidential, protected, and unrestricted) of data elements under their authority, and for determining what limitations or conditions apply to access.
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 stewards . Since data may cross functional lines, data used by any one data user may have different technical data experts and data stewards. All data users are responsible for reporting data issues to the respective data steward. Data quality, integrity and security is everyone's responsibility.
Enterprise Information Governance Committee (EIG)	Membership of the EIG Committee is made up of senior members of the university who are empowered to collectively move, approve, support, promote and enforce information governance activities throughout the university. Their primary responsibilities, as defined in the EIG Committee charter, are to approve policies, standards, roles, responsibilities and any other body required for information governance activities. They also have a supporting role which includes responsibilities in developing and promoting strategies, enforcing governance activities and are also a point of escalation for the Enterprise Information Governance Council.
Enterprise Information Governance Council (EIG Council)	The EIG Council is generally made up of Data Stewards and provides operational oversight, management, measurement and required monitoring on the effectiveness with respect to the university's institutional information. They collectively support the development of strategies to be approved at the EIG Committee, form a point of escalation for data users on data matters, provide oversight, provide guidance and recommendations to the EIG Committee, and provide

	guidance and support on data integrity checks, naming conventions, categorization, and catalog details.
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.
Information Technology (IT) Data Administrators	Individuals in IT who have operational level responsibility for data management activities related to the creation, storage, maintenance, security, and disposal of data. Data administrators have responsibility for promoting policies, guidelines, procedures and standards that allow the University to ensure the integrity, security, accessibility and usefulness of data. These roles include, but are not limited to, architects, DBAs and data integration specialists. Data administrators collaborate with Data Stewards to implement data transformations, resolve data issues, and collaborate on system changes. Generally, this role would apply to directors, managers or supervisors that have a direct responsibility for one of more institutional information systems and include information technology and data architecture experts.
Report Developers	Report Developers are responsible for the development of reports and ensure that all data requirements from Report Owners are met and that all policies and procedures are followed with respect to the University's Information, Technical, Security and Privacy policies and procedures. Report Developers are also responsible for adhering to all information governance best practices, standards and guidelines that would be defined by the EIG Council. They must also have all reports fully cataloged and documented prior to release to the data owners.
Report Owners	Report Owners take on the role of the main point of contact for all matters related to those reports.

	They are responsible for the consistency and sustainability of their reports and that all fields are defined and cataloged before release to their stakeholders. Are responsible for the training and education needed on the use of their reports to ensure proper use is adhered to. This would include, but not limited to, the intent of the report, the use, access, and sharing of the reports. They also take on the documentation pertaining to their reports which include processes, procedures, definitions, use, access and end user data quality expectations. They are also responsible for reporting any issues that affect the performance, data integrity, or non-adherence to the University's policies, procedures and any standards thereof.

Related Policy Documents (UAPPOL)

- Access to Information and Protection of Privacy Procedure
- Records Management Policy
- Research Records Stewardship Guidance Procedure

For questions surrounding policy document interpretation or implementation, please contact the Office of Administrative Responsibility.

For the most recent version of this document please visit https://www.ualberta.ca/policies-procedures/index.html