INSTITUTIONAL DATA GOVERNANCE AND MANAGEMENT POLICY

RESPONSIBLE ADMINISTRATOR: ASSOCIATE VICE PROVOST, DECISION SUPPORT
RESPONSIBLE OFFICE(S): OFFICE OF DECISION SUPPORT
ORIGINALIY ISSUED: JULY 22, 2010
APPROVALS:

APPROVED BY:

Nancy B. Rapoport, Executive Vice President & Provost  4/27/16

APPROVED BY THE PRESIDENT:

Len Jessup  5-6-16

REVISION DATE: APRIL 2016

STATEMENT OF PURPOSE

Institutional data are valuable resources of the University of Nevada, Las Vegas (UNLV) that directly support its central mission of education, scholarship, and service. These data are not only used to inform routine operational functions, but also utilized to guide policy formation, program development, assessment, and strategic planning. Because the utility of data derives from its quality, security, and ease of access, sound data governance and management are essential to the attainment of institutional goals.

UNLV is the owner of institutional data even though individual units have been entrusted with the management of those data. The university intends for its data to be regarded as key institutional assets and shared with all employees and authorized non-employees having a legitimate business need for information, in accordance with its business, legal, and ethical obligations to maintain data security and confidentiality of sensitive information in its care.

Data governance at UNLV arises from a purposeful intent to maximize the value of its data resources. It is grounded in the University’s underlying values of excellence, innovation, and collaboration, and is centered around a tenet of shared responsibility for the stewardship and protection of institutional data.

This policy provides a framework for a formal system of data governance and management in order to achieve the following objectives:
- Establish clearly-defined roles and responsibilities with corresponding accountability for the effective and transparent management of institutional data as critical enterprise resources.
- Institute best practices for robust data management aimed at enhancing data quality and integration, mitigating data security risks and privacy concerns, increasing data accessibility and utilization, and improving data definitions and metadata.
- Foster a culture of skillful and responsible data use as an integral part of institutional management and planning.

ENTITIES AFFECTED BY THIS POLICY

This policy applies to all users of UNLV’s institutional data, regardless of their institutional affiliation (internal to UNLV or external), the location of data access (on-campus or off-campus), the medium of data delivery (electronic, paper, or verbal), the form of data storage (internal or external server), the mode of data presentation (system view or extraction), or the level of data transformation (raw, revised, or derived).

WHO SHOULD READ THIS POLICY

This policy should be read by any person granted access, or seeking access, to UNLV institutional data, including faculty, staff, students, contractors, consultants, agents, volunteers, and guests.

POLICY

UNLV has developed the Institutional Data Governance and Management Policy to ensure proper data management and maximize the value of its data resources. Data Governance is the coordinated and cross-functional practice of making strategic and effective decisions regarding UNLV’s information assets. Compliance with this policy will ensure positive outcomes by defining the use of data, maintaining data quality, and sustaining data documentation and reduce negative consequences by securing data and controlling access.

1. Data Governance Structure

The responsibility for data governance at UNLV is a shared one. All authorized users of institutional data are assigned to one or more roles within the governance structure that will work in collaboration to ensure proper stewardship and protection of those data.

Executive Sponsors

Appointed by and accountable to the President and the Executive Vice President and Provost, executive sponsors are senior administrative officials who serve as trustees of institutional data, charged with the stewardship and protection of these valuable university assets. As a group, they are known as the Council of Executive Sponsors. They may include the following administrative positions: Associate Vice Provost for Decision Support, Vice Provost for Information
Technology, Associate Vice President for Enrollment and Student Services, Vice Provost for Undergraduate Education, Vice President for Research and Economic Development, Chief Human Resources Officer, Controller, and Dean of the Graduate College.

Responsibilities:

- Establish and refine the data governance policy.
- Provide overall strategic direction for the data governance program and hold final authority over institutional data in their operational units.
- Track the progress of on-going data governance projects and perform an annual evaluation of the overall data governance initiative.
- Promote a culture of data-driven decision-making by offering continual high-level support for proficient and responsible data use to fulfill the institutional mission.
- Serve as a board of arbitration on issues of contention surrounding institutional data (e.g., denial of access to data, violations of data governance policies, etc.) and address concerns and resolve conflicts from data stewards.
- Conduct oversight to ensure compliance with institutional policies and with state and federal regulations.
- Ensure that each data element in their purview has a named steward responsible for its management and protection.
- Provide approval of system of record designations for new campus information systems that hold valuable institutional data.
- Provide approval of classifications of privacy sensitivity for data elements, which are initially assigned by the associated steward.
- Perform review and approval of data documentation produced by data stewards (e.g., data definitions, data models, data maps, training materials, etc.).

Data Stewards

Data stewards are appointed by executive sponsors to put established data governance and management policies into action. As managers of functional areas within the university, data stewards have direct operational responsibility for institutional data in their respective domains, including supervision over the collection, maintenance, and dissemination of those data. Collectively, they are known as the Committee of Data Stewards. Included among data stewards are the following management positions: Registrar, Executive Director of Undergraduate Admissions, Director of Graduate Admissions and Records, Executive Director of Financial Aid and Scholarships, Assistant/Associate Controller, Assistant/Associate Budget Director, Human Resource Systems Manager, and Director of Academic and Research Space.

Responsibilities:

- Implement procedures to provide proper access to institutional data in their purview, maintain the quality of those data, and safeguard the data from unauthorized access and misuse.
• Assign a sensitivity level to each data element, which governs its accessibility and disclosure for data security purposes.
• Set guidelines for data access and review of data requests to institutional data. It is the steward’s responsibility to understand institutional business needs and facilitate appropriate access to data.
• Investigate reports of data inaccuracies and initiate remediation if necessary.
• Promote consistent data interpretation and usage, prevent data loss and misuse, and provide greater reporting capacity and accuracy so that relevant and timely data of the highest quality possible is available for university decision-makers.
• Provide adequate training and documentation to support data users, including data definitions to be stored in the university data dictionary.

Data Users

A data user is any individual who makes use of institutional data in the course of performing his or her assigned duties or otherwise fulfilling his or her authorized role at the university. Although data users are typically permanent, full-time employees of the university such as academic faculty, administrative staff, and classified staff, temporary employees or non-employees such as students, contractors, consultants, agents, volunteers, and guests who have demonstrated a legitimate business need for data in order to carry out their approved function at UNLV may become a data user for the duration of their work or affiliation.

As active participants in the university data governance structure, data users share responsibility for the stewardship and protection of institutional data and accountability for the appropriate use and dissemination of data. Their role requires them to understand and follow all established data policies and IT security regulations and to report concerns about data security, quality, integration, documentation to the associated executive sponsor and/or data steward.

2. Data Security

Institutional data must be secured and protected to comply with state and federal regulations and to ensure their integrity and availability to members of the UNLV community. Failure to maintain data security may not only result in the corruption, loss, or devaluation of important data, but also lead to legal penalties, financial repercussions, and impairment of institutional progress. Everyone at UNLV must commit to safeguard institutional data against misuse or abuse, comparable to their treatment of any valued material or financial asset of UNLV.

It is important for data security plans and procedures to maintain an appropriate balance between security and accessibility. Security measures should be implemented in a manner that poses the least possible burden upon the efficient conduct of business.

Classification of Institutional Data

The foundation for data security at UNLV is formed by a system of data classification, which establishes a framework for handling institutional data based on the criticality and sensitivity of the data. Data stewards implement security controls in accordance with data elements’ assigned
classification levels and any other applicable laws and regulations.

The level of protection stipulated for each class of data is prompted by proprietary, strategic, legal, and ethical considerations. The higher the level of criticality or sensitivity of a data element, the stricter its required security protocol. The University’s institutional data covered by this policy are assigned to one of three categories (in order of least critical/sensitive to most critical/sensitive):

- **Public data** are institutional data approved for release to members of the university community and external parties (including the general public and the media) without access restrictions because their disclosure poses little or no risk to the university, affiliated individuals, or non-affiliated persons. Examples of public data include names of university employees, their workplace email addresses, their workplace telephone numbers, and other directory information as well as aggregated information available on the institutional research website without user authentication.

- **Internal data** are institutional data intended to be protected from external dissemination and public consumption on account of business, regulatory, and ethical concerns. Selective access to particular elements or subsections of these data is provided to individuals from the university community and affiliated organizations that possess a business need for the data in order to carry out their required job duties or satisfy their role at the institution. Internal data may be released to individuals outside the university community only with approval from the registrar, designated executive sponsor, or when required by law. Examples of internal data include employee identification numbers, faculty and staff personnel records, student admission and enrollment records, and purchase requisition records.

- **Restricted data** are institutional data of a highly sensitive nature and whose inappropriate handling or disclosure could result in detrimental consequences for the university and individuals associated with the institution. These data warrant the administration of stringent security measures, and their access should be limited to only university employees with a demonstrated business need. Because restricted data are typically subject to federal or state regulations, a security breach would require the institution to notify the affected individual(s) as well as law enforcement authorities. Examples of restricted data include protected health information, social security numbers, financial account numbers, driver’s license numbers, and username and password credentials for university information systems.

3. **Data Access**

In alignment with its culture of collaboration and transparency, the University, as the data owner, intends for its institutional data to be readily available to all authorized members of the campus community who demonstrate a legitimate business need for information, subject to any limitations that may be posed by state and federal regulations (e.g., FERPA, HIPAA, HITECH, etc.). If any questions arise about the business need of a particular requester, the requester’s supervisor and/or the appropriate executive sponsor should be consulted.
Individual campus units or departments may not deny access to institutional data under their control on the basis of proprietary rights. For the advancement of the university, institutional data must be securely shared among eligible campus members whose work can be improved as a result of data availability, irrespective of whether these individuals belong to the unit or office that collects or maintains the data, unless such sharing of data is restricted by state and/or federal regulations.

Every person in need of access to institutional data must make a request through the formal processes established by data stewards responsible for developing guidelines for data access.

- Data access procedures must require specification of the data elements requested for access, explanation of the requester’s need for information, documentation of approval for data access from the requester’s immediate supervisor or an appropriate university sponsor, and certification of training completion.
- The user agreement serves as a formal acknowledgement of the rules and responsibilities of internal and restricted data use. Any requester who violates the terms of the user agreement, institutional data policies, state or federal regulations, etc. will have their data access terminated.
- Authorization for access to data is not transferable from one individual to another.
- When appropriate, data files may be provided in lieu of system access. For example, in instances where full access to information systems or particular functions of information systems may make those systems vulnerable to application crashes or instabilities, access to systems or particular system functions may be limited.
- Review of data requests are to be conducted in a timely manner and the decision provided to the requester in writing. Approvals of restricted access or denials of data access must be accompanied by an explicable statement. Any employee or non-employee given restricted access or denied access may appeal to the steward for additional review. If unsatisfied with the outcome of the subsequent review, the requester may submit a final appeal to the council of executive sponsors.
- For research use, data access may be granted for the academic study of an individual faculty member even though such research does not directly support university management and planning. However, certain data elements may be restricted and personal identifiers removed. The processing of data access requests related to scholarly research has lower priority than the processing of requests for work with broader institutional impact. Academic research is also subject to additional university policies on intellectual property, research ethics and protection of human subjects, etc.
- Individuals who are not full-time employees of the university, including graduate or undergraduate students, must have a university sponsor who is a full-time employee attest to the need for information.
- A training program is required for all users of internal data and/or restricted data. Such training seeks to ensure knowledge and understanding of this policy, other institutional policies on the use of campus information technology resources, Board of Regents of the Nevada System of Higher Education policies, relevant State of Nevada laws, and federal laws including FERPA regulations. Individual data stewards may require additional training.
specific to the use of data in their functional area.

The above data access policies are applicable to internal requests from UNLV employees or other authorized agents affiliated with the university. If an external request for data is made pursuant to the Nevada Revised Statutes Public Records Act, it should be forwarded to the Office of Media Relations: https://www.unlv.edu/mediarelations/makerequest.

4. Data Use

Individuals with access to institutional data have an obligation to engage in responsible, proficient, and scrupulous use of those data. They must access and use institutional data only in the conduct of official university business to which they have been assigned and in a manner that advances the institutional mission.

- Data users are responsible for protecting their access credentials, maintaining the confidentiality of data, and accurately presenting institutional data.
- Data users needing clarification on appropriate use and release of data should consult the applicable data steward. Concerns regarding the compromise of data security (e.g. unauthorized access, disclosure, loss, etc.), data errors, missing data, or other data quality concerns must be immediately reported to the responsible steward. An updated listing of data stewards will be maintained on the institutional research website for the reference of the campus community.
- Each data user is accountable for the consequences of any misuse or abuse. Those who fail to comply with user agreements, institutional data policies, campus information technology policies, state laws, or federal regulations (e.g., FERPA, HIPAA, HITECH, etc.) may be subject to disciplinary action, as well as criminal and/or civil penalties in some instances.

5. Data Quality

The availability of high quality data ensures effective operational decision-making and strategic planning in support of the institutional mission. Dimensions of data quality include integrity, integration, relevance, and timeliness.

- Data Integrity refers to the accuracy and consistency of data. The overall integrity of data starts with physical and logical integrity of the database that houses them. Data stewards are responsible for protecting information systems from data corruption caused by hardware failures, power spikes and outages, corrosion and material degradation, natural disasters, etc. and for establishing data backup and recovery procedures. They also have responsibility for the inclusion of appropriate logical integrity constraints (e.g., entity integrity and referential integrity) in the database. In addition, data stewards are responsible for establishing data collection standards and mechanisms for data validation, data synchronization, and error detection to ensure the accuracy of institutional data.
- Data Integration is the process of combining data from different sources. Data integration promotes conservation of resources, economy, efficiency, and effectiveness. The council of executive sponsors endorses the integration of data across organizational boundaries in the
university. Data stewards are responsible for establishing interfaces to connect information systems in different functional areas, develop synchronization mechanisms, and assimilate key data elements. Duplication or redundancy of data in multiple systems should be minimized. Along with the integration and synchronization of critical data elements across source systems, large-scale data integration must occur within the UNLV Enterprise Data Warehouse, which serves as a central repository for historical data preserved from numerous source systems across the university.

- Relevance of Data refers to consistency between the data content and the area of interest of the user. To improve business processes and deliver quality services, data users must have access to data that inform them about key dimensions of their work and outcomes of their efforts.
- Timeliness of Data is the availability of data at the time they need to be utilized. To be of value, data must be available on a timely basis and on the expected schedule. Data stewards bear responsibility to coordinate with each other and with managers in their functional units to ensure that data are up to date.

6. Data Documentation

The utility of data is maximized by the availability of documentation to guide users. Data stewards have a shared responsibility to maintain updated data definitions/data dictionaries, data models, and training materials for the reference of the campus community.

- A data definition is composed of business definitions and metadata (e.g., source, format, range of values, etc.) about a data element that facilitate the interpretation and use of the element. A data dictionary is a compendium of common data definitions applied throughout the enterprise, functioning as a reference for data users. To support a culture of informed and effective data use for institutional management and planning, updated definitions for data in their purview must be maintained by data stewards. Data definitions, once approved through formal processes, serve as a binding agreement for the usage and interpretation of data by data stewards and data users.
- A data model is a schematic representation of data elements or groups of data elements and the relationships among them. An enterprise data model offers a high-level view of an organization's data, while a detailed data model offers a specific view of a particular area of data. Data stewards are charged with maintaining updated models for the data in their area. The committee of data stewards works collaboratively to maintain accurate enterprise data models for the university that incorporate institutional data across all functional areas as well as the UNLV Enterprise Data Warehouse.
- Data stewards are responsible for developing training materials to train individuals on data security and responsible data use and to inform them about the interpretation and context of data.

Updated information regarding the activities surrounding institutional data governance will be available to employees of the university and to external stakeholders on the institutional research website.
7. Data Warehouse and Business Intelligence

The UNLV Enterprise Data Warehouse is a large central repository of integrated data obtained from different campus source systems to support institutional decision-making and business intelligence. The data warehouse is a critical part of institutional data management and usage because it provides data users with a mechanism to obtain historical transactional data and offers them the most efficient means to conduct complex analyses involving data from multiple operational areas.

The data warehouse is utilized to perpetually store important data from transactional information systems. The data warehouse is considered a system of record for all historical data that have been purged from or updated within the source systems.

The development and progress of a robust enterprise data warehouse requires collaboration among executive sponsors and data stewards to select data tables and elements for inclusion in the repository. Data stewards must work with data warehouse developers to ensure that data are captured within the warehouse from the appropriate source. Any changes within a source system that may impact the collection of data in the warehouse must be immediately communicated to warehouse developers to ensure uninterrupted and accurate data capture.

Reporting and research using institutional data from the data warehouse are facilitated through special business intelligence tools. These tools may range from basic software applications requiring no training to sophisticated applications requiring special training. Executive sponsors work with the data warehouse/business intelligence development team to prioritize the creation of reports, dashboards, and other interactive visualizations to aid institutional management and planning.

---

**Related Documents**

Family Educational Rights and Privacy Act (FERPA):

Federal Trade Commission (FTC) Red Flags Rule:

Health Insurance Information Portability and Accountability Act (HIPAA):
http://www.hhs.gov/ocr/privacy/

Health Information Technology for Economic and Clinical Health Act (HITECH):
https://www.healthit.gov/policy-researchers-implementers/health-it-legislation-and-regulations

Nevada Revised Statute - Chapter 239 (Public Records):
http://www.leg.state.nv.us/nrs/nrs-239.html

Nevada Revised Statute - Chapter 284 (State Personnel System):
http://www.leg.state.nv.us/Nrs/Nrs-284.html

Nevada Revised Statue - Chapter 603A (Security of Personal Information):
https://www.leg.state.nv.us/NRS/NRS-603A.html

Nevada System of Higher Education, Procedures and Guidelines Manual, Records Retention and Disposition Schedule:
http://system.nevada.edu/tasks/sites/Nshe/assets/File/BoardOfRegents/Procedures/PGMCH18RECORDSRETENTIONANDDISPOSITIONSCHEDULE.pdf

UNLV Acceptable Use of Computing and Information Technology Resources Policy:

UNLV Computer Security Policy:

UNLV Data and Media Sanitization Policy:
http://www.unlv.edu/sites/default/files/24/Provost-Policy-Data-Media-Sanitization.pdf

UNLV Network Access Compliance Policy:
http://oit.unlv.edu/about-oit/policies/network-access-compliance-policy

UNLV Password Policy:

UNLV Policy on Research Involving Human Subjects:

UNLV Records Management Manual:
https://www.unlv.edu/sites/default/files/24/records-retention.pdf

UNLV Rules and Procedures for Conducting Human Subject Research:

**CONTACTS**


**DEFINITIONS**

**Committee of Data Stewards** – Collective designation for the group of campus data stewards. All appointed data stewards belong to the committee.

**Council of Executive Sponsors** – Collective designation for the group of campus executive
sponsors. All appointed executive sponsors belong to the council.

**Business intelligence** – A set of applications, tools, and techniques used to transform data into information useful for business management and planning.

**Data definition** – A set of business definitions and metadata (e.g., source, format, range of values, etc.) about a data element that facilitate the interpretation and use of the element.

**Data dictionary** – A repository of shared and consistent enterprise-wide data definitions that serves as a reference tool to understand the data belonging to an organization.

**Data element** – A single item of data. For example, “building code” is a data element that can have values such as “FDH,” “CBC,” “SCS,” and “MSU.”

**Data governance** – The coordinated and cross-functional practice of making strategic and effective decisions regarding UNLV's information assets that is centered around a tenet of shared responsibility for the stewardship and protection of institutional data.

**Data owner** – The owner of institutional data. Data governance at UNLV stipulates that the university is the sole owner of all institutional data.

**Data steward** – A manager of a functional area within the university who is charged with the implementation of established data policies and has operational responsibility for the quality, availability, and security of institutional data in his or her domain.

**Data user** – An individual who utilizes institutional data in order to perform his or her assigned duties or fulfill his or her role at the university. By definition, executive sponsors and data stewards are also data users.

**Enterprise data warehouse** - A large central repository of integrated data obtained from different campus source systems to support institutional research and business intelligence.

**Executive sponsor** – A senior university official who sets the priorities and strategic direction of campus data governance. As a group, executive sponsors establish policies and processes, facilitate collaboration, monitor compliance, track progress, address concerns and conflicts, and evaluate the overall data governance initiative.

**FERPA** – An acronym for the Family Educational Rights and Privacy Act (20 U.S.C. § 1232g; 34 CFR Part 99), which is a federal law that protects the privacy of individually identifiable student education records.

**HIPAA** – An acronym for the Health Insurance Portability and Accountability Act of 1996, which is a federal law that protects the privacy of individually identifiable health information records.
HITECH – An acronym for Health Information Technology for Economic and Clinical Health Act, enacted as part of the American Recovery and Reinvestment Act of 2009 (HITECH) which is a federal law that promotes adoption and meaningful use of health information. HITECH addresses the privacy and security concerns associated with electronic transmission of health information, in part, through provisions that strengthen the civil and criminal enforcement of HIPAA rules.

Institutional data – Any data element, or collection of such elements, that is (a) relevant to the management, oversight, or planning function of an administrative or academic unit within the university; (b) included in an official university-, college-, department-, or program-level administrative report; or (c) used to derive or is derived from an element, or collection of elements, that meets either or both of the criteria above. Institutional data may exist in the form of text, graphics, audio, video, or other media; comprise a variety of electronic, printed, or other formats; be maintained under shared or individual control; and be stored internally (via institutional servers or physical records) or externally (via remote servers or cloud computing). Operational data held by units including but not limited to the Division of Research and Economic Development, Office of Sponsored Programs, School of Medicine, School of Dental Medicine, and William S. Boyd School of Law are considered to be institutional data and are governed by this policy. However, clinical or client data generated from the provision of services by such entities; data produced from research or scholarly activities; instructional notes and materials; and other intellectual property, even though they may reside in institutional systems, are outside the scope of the definition of institutional data. Such data may be subject to other university policies.

Internal data – Institutional data with a median level of sensitivity and need for protection. These data are not intended for external release or public use and should only be accessible to authorized individuals for the conduct of university business.

Metadata – Data that provide descriptive, structural, or administrative information about other data.

Public data – Institutional data with the lowest level of sensitivity and need for protection. These data are approved for general release without access restrictions because their disclosure poses little or no risk to the university, affiliated individuals, or non-affiliated persons.

Restricted data – Institutional data with the highest level of sensitivity and need for protection. These data require strict security controls and access limitations because their inappropriate handling and disclosure poses significant risk to the university and associated individuals.

Source system – An information system in which particular elements of institutional data are initially captured.

System of record – An information system endorsed as holding the official values of particular elements of institutional data, even if those data were originally entered or stored elsewhere. In cases of discrepancy around the values or interpretation of data elements stored in multiple
locations, the system of record holds precedence over other systems (including source systems) and is used to resolve the conflict.