OFFICE OF DECISION SUPPORT

INSTITUTIONAL DATA GOVERNANCE AND MANAGEMENT POLICY

RESPONSIBLE ADMINISTRATOR: BRENT DRAKE, VICE PROVOST FOR DECISION SUPPORT
RESPONSIBLE OFFICE(S): OFFICE OF DECISION SUPPORT
ORIGINALLY ISSUED: JULY 22, 2010
APPROVALS: APPROVED BY:

_____ _____
Brent M. Drake *Date*
Vice Provost for Decision Support

_____ _____
Chris Heavey *Date*
Executive Vice President & Provost

APPROVED BY THE PRESIDENT:

_____ _____
Marta Meana *Date*

REVISION DATE: To be determined

STATEMENT OF PURPOSE

This policy provides a framework to allow for maintenance of, prioritization of, access to, and use of a high-quality data environment, and is based on the following guiding principles:

- Data Governance
- Prioritization of Needs
- Collaborative Decision Process
- System of Record
- Accountability
- Availability of Official Data
- Official Reporting
- Data Accessibility
- Data Privacy/Compliance

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).

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.

WHO SHOULD READ THIS POLICY

This policy should be read by any person granted access to, seeking access to, or charged with entry or maintenance of UNLV **institutional data**, including, but not limited to, faculty, staff, students, contractors, consultants, agents, volunteers, and guests.

THE CONTEXT

Institutional data are valuable resources of the University of Nevada, Las Vegas (UNLV) that directly support its central mission of education, scholarship, and service. **Institutional data** are used to both inform routine operational functions and 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.

The data policy at UNLV arises from a purposeful intent to maximize the value of its data resources. It is grounded in the university's data vision of being recognized as a leader in the development of best practices for creating and continually evolving a data-rich culture, and is centered around its data mission of delivering a data-informed environment through a collaborative process that provides high quality, accessible, and widely utilized information to support the university's strategic goals.

POLICY

1. DATA GOVERNANCE - The institution will maintain a robust set of policies, practices, and **data definitions** to ensure the highest quality of **data governance**.

Appointed by the Executive Vice President and Provost, the **Data Oversight Committee (DOC)** consists of senior administrative officials who are responsible for the maintenance of the **data governance** policies and practices for the institution.

2. PRIORITIZATION OF NEEDS - Prioritization of institutional needs come before unit-based needs with the understanding that unit needs are important and will be addressed in a manner that is consistent with institutional needs.

Ultimately the **Data Oversight Committee** is responsible for determining the prioritization of needs and resources to meet those needs within UNLV's environment. Data needs will inevitably arise from and be driven by specific units. However, in establishing the order of priority for those needs in a resource constrained environment those efforts that benefit the broader institution will be worked on first over those that only benefit an individual department.

3. COLLABORATIVE DECISION PROCESS - Decision-making will be collaborative and involve diverse opinions and discussion. Once a decision is reached the institution will move forward with implementation.

UNLV recognizes the benefit of diverse opinions within the decision-making process. As such, the **Data Oversight Committee** will consist of a broad array of members from units across the university, and will include input from various other units. However, once a decision is reached within the **Data Oversight Committee**, the university will move forward with implementation to ensure that forward progress is maintained within the data environment.

4. SYSTEM OF RECORD - The university is the owner of all data about the institution. Official data must reside in an authoritative **system of record**. Only data from an authoritative **system of record** will be used for **official reporting** and decision-making.

While individual units will ultimately be responsible for maintaining the quality of the data over which they have the purview as **custodians**, the university is the owner of all **institutional data**. To allow for high-quality **data governance** and reporting, all official data must reside in a system that the university has designated as an authoritative **system of record**; only data from these authoritative sources will be used for **official reporting** and informing the university's decision-making process. The university will be responsible for ensuring that data needed for **official reporting** and decision making will transfer from the **system of record** to the **institutionally approved data management environments**.

5. ACCOUNTABILITY - To ensure a viable data environment, **data custodians** of **institutional data** are ultimately responsible for the quality of, integrity of, and access to the data for which they have been assigned stewardship. Applicable units are responsible for completion of agreed upon reports about the data in accordance with institutional best practices.

The university ultimately owns all **institutional data**. However, individual units will have oversight of those **data elements** that fall within their custodial responsibilities. As such, those custodial units are responsible for establishing and maintaining the quality of those **elements** with input from the **Data Oversight Committee**.

To establish and maintain a highly functional reporting environment, those units assigned responsibility by the **Data Oversight Committee** will complete all agreed upon reports. Those reports must be created and maintained based upon the best practices established by the **Data Oversight Committee** for the institution.

6. AVAILABILITY OF OFFICIAL DATA - **Data elements** for reporting needs must be placed in **institutionally approved data management environments**. Business processes will be modified, as required, to allow for the capture and validation of **institutional data**. The data will be integrated as needed.

The **institutionally approved data management environments** will be the area for reporting utilized by the university, thus it is of highest priority that all necessary **data elements** are placed in that environment. Where business processes must be modified to allow for the placement of the highest-quality data in the reporting environment, the units with custodial responsibility for the data will do so.

For the institution to achieve maximum benefit from the use of its data it is necessary for those **data elements** that arise from disparate **systems of record** to be integrated into the reporting environment. As such, the institution, through the efforts of the **Data Oversight Committee**, will actively create those integrations.

7. OFFICIAL REPORTING – There will be an institutional dialogue and review around how and when official reports are generated and released. Official reporting will be done from **institutionally approved data management environments**.

For UNLV to maximize the benefit of its data environment it is essential that it establishes procedures around its official reports. The **Data Oversight Committee** is tasked with the responsibility for ensuring that appropriate dialogue occurs and for establishing the process for official reports.

It is essential for consistency and replicability that all **official reporting** be conducted from the **institutionally approved data environments.** Where a unit within the institution chooses to utilize an **external system** for operational needs, any reports done from that system will not be accepted as official. When it is necessary to use

reports generated by **external systems** for **official reporting,** every effort should be made to gain approval from the **Data Oversight Committee**. It is the unit's responsibility to work with the **Data Oversight Committee** to integrate the data from their **external system** with **official systems of record.**

8. DATA ACCESSIBILITY - The institution will provide access to all data necessary for individuals to perform the functions of their positions at the university. For public reports, the underlying data details are accessible to those who have a need to know based on job function.

For optimal use of the university's environment, all **data elements** necessary for the performance of an individual's position must be accessible to that position. This includes access to data at the level of granularity necessary for the performance of the essential functions of the position.

UNLV will provide public reports, as necessary, to meet the goals of its underlying mission and to meet all federal and state compliance requirements. While those public reports will be accessible to anyone, the underlying data details will only be accessible to those positions where it is necessary for the performance of their job functions.

9. DATA PRIVACY / SECURITY / COMPLIANCE - To provide high availability and prevent data from being used for unauthorized purposes, **data custodians** of **institutional data** must:

- ensure the privacy, security, and availability of the data
- maintain compliance with federal, state, Nevada System of Higher Education (NSHE), Board of Regents, and campus statutes, regulations, and/or policies.

Data privacy procedures must be approved by the **Data Oversight Committee**.

UNLV will always conduct itself and operate within compliance of federal, state, system, and campus statutes, regulations, and/or policies.

RELATED DOCUMENTS

Data Governance and Management Procedures
https://docs.google.com/document/d/19Zm8736lX_jRTOXoDiywlaZ8j8aDT5Tn2uQQ3CPUPrU/edit

Family Educational Rights and Privacy Act (FERPA):
https://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html

Health Insurance Information Portability and Accountability Act (HIPAA):
https://www.hhs.gov/hipaa/index.html

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):
https://www.leg.state.nv.us/Division/Legal/LawLibrary/NRS/NRS-239.html

Nevada Revised Statute – NV Rev Stat 396.405 (2013) (Nondisclosure of Contributors)
https://law.justia.com/codes/nevada/2013/chapter-396/statute-396.405/

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

NSHE Board of Regents Handbook, Title 4 Chapter 21, NSHE Data Administration
https://nshe.nevada.edu/wp-content/uploads/file/BoardOfRegents/Handbook/title4/T4-CH21%20NSHE%20Data%20Administration.pdf

UNLV Acceptable Use of Computing and Information Technology Resources Policy:
https://www.unlv.edu/sites/default/files/page_files/27/AboutUNLV-AcceptUseComputingTechResources-Policy.pdf

UNLV Computer Security Policy:
https://oit.unlv.edu/about-oit/policies/computer-security-policy

UNLV Policy on Research Involving Human Subjects:
https://www.unlv.edu/sites/default/files/assets/research/policies/HumanSubjectsResearchPolicy-June13.pdf

CONTACTS

Data Oversight Committee, EDOC-group@unlv.edu

Office of Decision Support, http://ir.unlv.edu/iap/, 702-895-3771

Office of Information Technology, ithelp@unlv.edu, 702-895-0777

DEFINITIONS

To ensure a common understanding of key terms used in the management of institutional data, the definition list includes terms not specifically referenced in the policy.

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 dictionary values, etc.) about a data element that facilitate the interpretation and use of the element.

Data Custodian - A manager of a functional area within the university who is charged with the operational responsibility for the quality, content, retention, metadata management, security, privacy, and availability of institutional data. They work with applicable units to develop definitions and standards for the data under their stewardship.

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 maintenance, use, and accessibility of institutional data.

Data Oversight Committee – A committee of senior administrative officials who are responsible for the maintenance of the data governance policies and practices for the institution.

Data Warehouse - A large central repository of integrated data obtained from different campus source systems to support institutional research and business intelligence. Warehouse data is typically captured and retained to allow for further analysis.

Executive Data Oversight Committee – The committee facilitates the work of the Data Oversight Committee (DOC) and its affiliated committees. The committee ensures DOC direction and priorities guide the work of those committees. The EDOC also serves as the conduit for bringing forth any data issues that require DOC attention.

External System - Any system or operational process that exists outside of the university's recognized systems of records or official reporting environment. An external system includes any external sources of data such as an operational system, web service, cloud computing, SQL server database, or spreadsheets maintained directly within a department for operational procedures or departmental reporting.

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.

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:

1. relevant to the management, oversight, or planning function of an administrative or academic unit within the university
2. included in an official university-, college-, department-, or program-level administrative report or
3. 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
- be comprised of a variety of electronic, printed, or other formats
- be maintained under shared or individual control
- 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 the 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. Additionally, donor information is owned by the UNLV Foundation and is governed by Nevada Revised Statute NRS 396.405 which states a university foundation is not required to disclose donor names, the amount of contribution, or any information that could reveal or lead to the discovery of donor identity. The UNLV Foundation can share information with university staff that have a legitimate business need if \
there is a fully executed confidentiality agreement on file.

Institutionally Approved Data Environments - data environments (e.g., **operational data store, data warehouse, etc.)** that are approved by the **Data Oversight Committee.**

Internal Data - Data that may be released to individuals outside the university community only with approval from the data custodian, designated executive sponsor, or when required by law. Some data in this category may be a matter of public record in the State of Nevada.

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

Operational Data Store - A large central repository of integrated data obtained from different campus source systems to support the operations of the university. Access to the operational data store is restricted based on the essential functions of a position. The operational data store is refreshed periodically, most commonly on a daily basis to provide current-state information.

Official Reporting - A formal accounting by the university of its activities. Official reports are those that follow university policy and guidelines and are derived from data that originate from an official system of record and must be able to be replicated by any member of the institution with access to the data.

Public Data - Institutional data that 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 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 access should be limited to only university employees with a demonstrated business need.

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.