Data Governance Standards for Mesa Community College

November 2014
Approved by Shared Governance Council – 1/26/15

Committee Lead:

James Mabry	Vice President of Academic Affairs (has since resigned)

Committee Members:

Matt Ashcraft	Dean of Institutional Effectiveness, Informed Improvement co-lead
Diana Bullen	Business Faculty, Student Outcomes Committee Chair
Brian Dille	Political Science Faculty, Informed Improvement co-lead
Steve Gerlock	Director of Admissions Registration & Records (has since resigned)
Andrew Giddings	Manager of Strategic Systems
Jeremy Kurtz	IT Security
Paul Nunez	Faculty Senate Representative
Dennis Mitchell	Institutional Research Analyst
Roger Yohe	Acting Vice President of Academic Affairs

Committee Rational and Summary

Mesa Community College has for the past few years been working to develop and implement informed improvement in every aspect of the college. The goal of informed improvement is to promote a culture of evidence-based decision making dedicated to advancing student success.

To enable informed improvement, the College is in the process of creating and bolstering systems to enable widespread access to more types of data and more robust data. Some have raised concerns at how this data will be used. Stewards of data currently have practices to ensure that data is used properly, but these practices are not uniform, have not been reviewed, and are little known outside of the offices of those stewards.

In an effort to be proactive, this working group began meeting in early fall 2013 to articulate the core principles of data governance at MCC and the standards of practice by which these principles will be followed at the College. This group consisted of key stakeholders who create, maintain, or secure data at this college. The committee also included representation by the Faculty Senate and the informed improvement team.

The mission of the Institutional Data Governance Committee is to guarantee that Mesa Community College has in place a set of processes that ensures that important data assets are formally managed throughout the enterprise. Data governance should ensure that data can be trusted, that accountability for data quality and protection exists, and that data is both open and secure.

The principles of data governance at MCC are:

Accessibility

Users have role appropriate access to data needed to make informed decisions. Data is available across platforms, on-site and remotely.

Integrity

Data should be collected and maintained with reasonable assurances of its consistency, reliability, timeliness and accuracy. Individuals share responsibility and are accountable for their entry, use and access of the College's data repository, requiring ongoing training on the part of those who enter, use, and care for it.

Security

Sensitive data is protected from unauthorized access and improper disclosure. The integrity of data is protected from malicious or accidental alteration. Data is available with access granted according to the role of the user. Processes are in place to ensure training and awareness.

Ethics

Data is used in accordance with ethical principles, accepted best practices, and legal requirements. Data is used to improve practices and further the College mission.

This document sets forth these principles, articulates the standards of practice that flow from them, and provides a brief description and clarification of the standards for each principle. We have also provided a glossary of terms associated with Data Governance.

We expect them to guide practice throughout the institution and that periodic review of these principles will occur. Having an agreed-upon Data Governance document will enable us to move toward a culture of evidence-based decision making with trust and confidence.

Accessibility

Guideline

Users have role appropriate access to data needed to make informed decisions. Data is available across platforms, on-site and remotely.

Standards

The following accessibility standards apply to MCC's Data Governance process:

1. Data will be available to users at the time and in the manner needed to inform decision-making.
2. All data sources and the avenues for accessing them will be well documented.
3. Access to data sources is granted through a formalized and well-documented process.
   a. Users must complete appropriate training (e.g. Family Educational Rights and Privacy Act (FERPA) training) before gaining access to data.
   b. Access will utilize MEID/password access, when possible.
4. Data access procedures and processes will be reviewed at regular intervals to ensure utility and adherence to these standards.
5. Data will be classified according to access type (e.g. critical data, limited-access data, internal data and public data) as well as by storage, retention, and destruction standards (e.g. Admissions/Records, Human Resources, Purchasing, and Institutional Research). These classifications will be public and justified.

Narrative

Striking a balance between ensuring appropriate protections of security and privacy of records and ensuring users have access to the records they need for informing decisions is at the heart of data accessibility. The standards outlined above provide the framework for striking this balance and will assist us with making data more accessible, useful, and accurate while also ensuring the data security and privacy. Another primary purpose of this component of data governance is to provide a structured and consistent process to obtain necessary data access for conducting MCC operations (including administration, research, and instruction).

Draft mapping of data sources and access

Source	Access Steward	Access Type	Access type Classification	Storage, Retention, and Destruction Classification	Current Governance?	Future Governance	Data Steward
SIS	SIS Security Admin	Functional role based	Critical, limited access, internal	Registrar Records, Financial Aid Records,	FERPA then role determination		
The Datasphere (fed by SIS and eventually other sources)		Role based	Critical, limited access, internal	Registrar Records, Institutional Research Records, Financial Aid Records,			
IRIS (fed by SIS)	District IR	Functional role based (IR staff)		Institutional Research Records			
HRMS	HR	HR Staff		Human Resource Records			
Department Level Databases (data entry)							
Trac System Data (swipe and data entry?) Advisor, Tutor, Fitness, WL							
Canvas (fed by SIS and data entry)		Functional role based					
BOEXI (fed by SIS and HRMS)	BOEXI Security Admin	Role			FERPA then role determination		
R25 (fed by SIS and data entry)							
Qless (swipe and data entry?)							
CRM (data entry?)							

References

"Data Access Standards." The University of Pennsylvania. Accessed from: http://www.upenn.edu/oacp/privacy/policiesguidance/data-access-standards.html

"Standards for Management of Institutional Data." Office of the Vice President for Information Technology. Indiana University. Last Update: 2007. Access from: http://datamgmt.iu.edu/DM01s.shtml

"Data Access." Georgia Tech Policy Library. Last Updated: 2005. Accessed from: http://policies.gatech.edu/data-access

Examples for Data Classification:

Stanford

http://www.stanford.edu/group/security/securecomputing/dataclass_chart.html

University of Michigan

http://www.safecomputing.umich.edu/protect-um-data/examples.php

Portland CC

http://www.pcc.edu/about/policy/electronic/information-classification.html

Integrity

Guideline

Data should be collected and maintained with reasonable assurances of its consistency, reliability, timeliness and accuracy. Individuals share responsibility and are accountable for their entry, use and access of the college's data repository, requiring ongoing training on the part of those who enter, use, and care for it.

Standards

The following data quality standards apply to MCC's data governance process:

1. **Accuracy** - Data values are defined and labeled correctly.
2. **Validity** - Data values are correct and reasonable for the attribute being described. Standardized data validation protocols will be utilized in all data entry interfaces.
3. **Completeness** - All of the data that are intended to be collected are collected.
4. **Integrity** - Data are free from willful or unconscious error.
5. **Uniqueness** - Data elements are unique.
6. **Timeliness** - Data is regularly collected, up-to-date, and available when it is needed.
7. **Relevance** - Data supports and furthers the goals and objectives of users, processes, and the organization.
8. **Accountability** - Individuals are accountable for both entry, use, and dissemination of data.

Narrative

The College community should trust the integrity of institutional data. Data should be collected and maintained with reasonable assurances of its consistency, reliability, timeliness and accuracy. Individuals share responsibility and are accountable for their use and access of the College's data repository, requiring ongoing training on the part of those who use and care for it. Formal procedures and processes need to be in place to resolve reporting frustrations when data results in different reports and database queries that are often contradictory, leading to a data integrity "crisis of confidence." These procedures need to be published and justified.

Data integrity is a business process issue and it requires the College to take responsibility and drive improvements to ensure the following goals:

- To improve consistency and accuracy of data to establish a single version of the truth.

- Improve the quality of the data—greater accuracy, increased timeliness, and reduction in the redundancy of the data.
- Reduce the number of "shadow systems"—separate, unmonitored "silos" of information that can lead to more data inconsistencies and even more versions of the truth.
- Formally assign responsibility for managing data resources to data stewards.

Appointing data stewards is an appropriate approach to help achieve data quality improvement goals for the following reasons:

- Stewardship is most effective when it is positioned closest to the point of capture and maintenance of the data.
- Stewards are in an ideal position to help with an effective governance strategy for data quality, since governance must cascade across the entire organization to ensure that appropriate accountability is enacted and enforced.
- Stewards should be considered subject-matter experts for their departments. They should have specific goals for data quality improvement, but they are responsible just for guiding the effort and do not have to do all the work themselves.

"Data stewardship" is different from "data ownership." Ownership implies control and restriction of access. Stewards are not the owners of the data, but rather are trustees, ensuring that adequate quality is maintained so the data can support business processes. Stewards should assess their respective data systems to ensure data quality. Stewards should also place a priority on open access, since informed decision-making is essential to advancing student success.

In so far as data stewards are responsible to maintain the integrity or accessibility of data, it is necessary to have an appeal procedure for the decisions they make. If there is a potential data consumer who is denied access to data by the data steward, and the potential data consumer feels that denial to be unwarranted, the data consumer can request that the Vice President of Academic Affairs convene the Data Governance Committee to review the situation. Upon review of the merits of the situation as presented by both parties, the Data Governance Committee will either uphold or reverse the position of the data steward.

Security

Guideline

Sensitive data is protected from unauthorized access and improper disclosure. The integrity of data is protected from malicious or accidental alteration. Data is available with access granted according to the role of the user. Processes are in place to ensure training and awareness.

Standards

The following information security standards apply to The College's data governance process:

1. Data has a clear, established steward that ensures these standards are met.
2. Proper controls exist to ensure data confidentiality, integrity, and availability based on classification.
3. Access controls provide the appropriate amount of access required and prohibit unauthorized access.
4. Access is logged, monitored, and audited.
5. Incidents of intentional or accidental misuse of this standard are properly reported.
6. Data is properly destroyed at the end of its lifecycle.

Narrative

The information security principle ensures the confidentiality, integrity, and availability (CIA) of data. As stewards of data, the College must perform its due care and due diligence to remain accountable to Maricopa's Office of Public Stewardship, the Arizona State Library, relevant laws and regulations, and stakeholders of its data. These standards shall provide this assurance.

In order to ensure the data governance body succeeds in its mission, data and systems must be inventoried and have clear, assigned stewardship. These data and system stewards are responsible for formalizing standards such as data classification, data handling, and associated training and awareness. These standards can then be operationalized and delegated to data custodians.

As part of this process, the College is striving to make data more accessible, useful, and accurate. However, sensitive data must not be improperly disclosed. Access controls must be in place to ensure that authenticated users have appropriate authorization to data based on their role. If access to unauthorized data is attempted, these controls must ensure such attempts are not allowed.

Any attempt to access data – authorized or not – must be logged. Data custodians shall be tasked with these duties and are also responsible for routinely monitoring logs for inappropriate access. Finally, any requests for access to logging information must follow an auditing process. This process shall include the entity making the request, the time, and the reason, and will be signed off by the steward.

Availability of data depends on both the real-time systems providing access to the data and the backups of these systems. For example, a system or power failure might cause data to be inaccessible for a short period of time. However, a fire or other disaster could completely destroy the system and its data. Therefore, it is crucial that all data is backed up to a secure, offsite location to ensure its long-term availability.

Data classification and handling standards must exist and apply to data throughout its lifecycle. Data shall be stored and transmitted using means appropriate for its classification and must be retained according to Maricopa's public stewardship policies:

http://www.maricopa.edu/publicstewardship/governance/adminregs/auxiliary/4_15.php

http://www.maricopa.edu/publicstewardship/pr/schedule.php.

Ethics

Guideline

Data is used in accordance with ethical principles, accepted best practices, and legal requirements. Data is used to improve practices and further the college mission.

Standards

The following standards apply to the use of data at the College to ensure that ethics are maintained:

1. Use of data meets legal requirements governing the collection, storage, and dissemination of individualized information.
2. The privacy and confidentiality of individualized information is maintained and safeguarded.
3. The process of gathering data is transparent, including full disclosure when data is being collected.
4. The information gathered is used exclusively for professional, job-related ends, and not for personal purposes.
5. Access to sensitive data for research purposes must be approved by the College Research Review Committee (CRRC).

Narrative:

An informed college is better able to meet its mission, so the College is committed to making data available to employees to inform their decision-making. As data systems increase in complexity and the volume of sensitive data held by the College grows, it is imperative that college administrators and employees access and use data in ways that promote student success, protect the privacy and confidentiality of the personal information of our students and employees, and uphold the professional standards of an institution of higher education.

Those who access individualized information (data that contain personally identifiable information) or sensitive data in the course of their duties need to be aware of the legal requirements and ethical principles that accompany access to that data. These would include requirements from the Family Educational Rights and Privacy Act (FERPA), the Federal General Services Administration (GSA) Requirements for Handling Personally Identifiable Information, Federal and Arizona rules for Freedom of Information requests, and Arizona statutes governing preservation of records, among others. They also need to be careful to follow the standards set forth in the Security Principle as an ethical imperative to protect the individuals whose data is under their care.

If the data is being gathered or used for Human Subjects Research (HSR), as defined by the Maricopa District Institutional Review Board (IRB) Handbook, then those providing the information, or whose information is being provided, have a right to know why, when, and by whom the information is being gathered, and how it will be used. Researchers must gain approval by the CRRC prior to gathering this data. More information on this regard can be obtained at www.maricopa.edu/irb.

Finally, to improve institutional practices and enhance student learning, it is necessary to gather data on personal and organizational effectiveness. The results of such studies are used to improve performance. In all cases, personal evaluation will follow the guidelines set forth in the RFP or employee manuals.

Data Governance Glossary

Data Custodian

Typically IT staff tasked with data protection and maintenance. Maintenance includes responsibility for technical controls that meet the classification requirements set by data stewards.

Data Steward

College leadership in charge of an organizational unit(s). Data stewards are trustees of data, and are ultimately responsible for the data stewardship process. This process includes setting classification levels, defining data custodians, and allocating resources as necessary.

Data Stewardship

The overall process of data governance that ensures standards and policies surrounding data are met.

Encryption

Logical controls that protect the confidentiality and integrity of data using various industry-standard cryptographic algorithms.

FERPA

Family Educational Rights and Privacy Act. Any data that includes student records is protected under FERPA.
http://www.maricopa.edu/publicstewardship/ferpa.php

GSA

The Federal General Services Administration Requirements for handling Personally Identifiable Information. These are located at http://www.gsa.gov/portal/content/104256 and applied to MCCCD Records and Information Management policy at http://www.maricopa.edu/publicstewardship/pr/schedule.php

Personally Identifiable Information (PII)

Identity-based data such as name, address, phone, SSN. This information must be protected to circumvent identity theft.

Role

Job Role or User Role is defined in accordance with Role-Based Access Control (RBAC) as follows:

1 Role assignment: A subject can exercise a permission only if the subject has selected or been assigned a role.

2 Role authorization: A subject's active role must be authorized for the subject. With rule 1 above, this rule ensures that users can take on only roles for which they are authorized.

3 Permission authorization: A subject can exercise a permission only if the permission is authorized for the subject's active role. With rules 1 and 2, this rule ensures that users can exercise only permissions for which they are authorized.

In practice, the supervisor would define #1, the data steward and supervisor would collaborate to define #2, and the data steward in collaboration with IT (and possibly information security) would define and implement #3.

Sensitive Data

Data protected by law, contractual obligation or administrative regulation. Personally identifiable information, personally identifiable education records, individually identifiable health information, personally identifiable financial information and payment card information are examples of Sensitive Information covered under the Arizona Revised Statutes (ARS), Family Educational Rights and Privacy Act (FERPA), Health Insurance Portability and Accountability Act of 1996 (HIPAA), Gramm–Leach–Bliley Act (GLBA aka Financial Services Modernization Act of 1999) and Payment Card Industry Data Security Standard (PCI DSS), respectively.