WAYNE STATE UNIVERSITY
DATA GOVERNANCE CORE COMMITTEE CHARTER

Last Modified: 5/21/2019

I. GOALS

The goals of the Data Governance Core Committee at Wayne State University are to:

A. Protect the privacy and security of the data and information that is under the stewardship of the University;
B. Create and support a culture of responsible data use for informed and actionable decision making;
C. Establish campus-wide standards and policies that enable holistic understanding and usage of data across University boundaries;
D. Ensure that the University adheres to laws and regulations that governs storing, processing, transmitting, disclosing and disposing of data and information within the university and to third parties;
E. Promote the efficient use of resources to meet the data and information needs of the University community ensuring proper access and control;
F. Ensure that the data comes from a reliable source of truth and users are able to interpret the terms and data in the same manner;
G. Increase the University's transparency and accountability to external stakeholders and the public by promoting access to relevant information;
H. Create and ensure that policies and procedures related to data and data use align with the strategic plan of the university;
I. Research, develop and promote new and innovative ways to access, use and leverage data.
J. Ensure that faculty and staff are educated about data use, privacy and security.

II. DEFINITIONS

A. Institutional Data - data elements which are created, received, maintained and/or transmitted by the Wayne State University in the course of meeting its administrative and academic requirements.
B. Institutional Information - a collection of Institutional Data which can be:
    1. Contained in any form, including but not limited to documents, databases, spreadsheets, email, and websites;
    2. Represented in any form, including but not limited to letters, numbers, words, pictures, sounds, symbols, or any combination thereof;
    3. Communicated in any form, including but not limited to handwriting, printing, photocopying, photographing, and web publishing; and
    4. Recorded upon any form, including but not limited to papers, maps, films, prints, discs, drives, memory sticks, and other information systems.

III. PURPOSE

The objectives of the Data Governance Core Committee are to:

A. Establish fundamental principles or framework governing the management and use of data and information at the University, including, but not limited to, the ***creation*** **or** ***acquisition***; ***quality & consistency; standards; privacy & security***; ***compliance;*** and ***retention & archiving*** of those data and information;

B. Set forth best practices for effective data management with ongoing objectives of increasing efficiencies, managing and mitigating information privacy and security risks, and promoting data quality;

C. Establish clear lines of accountability and decision rights through the definition of roles and responsibilities related to data management;

D. Establish a set of standardized terms and definitions to promote consistent interpretations and implementations of policies, procedures, and practices related to data management.

E. Advocate and champion a culture of collaboration within the University to share information across all departmental units.

IV. SCOPE

A. The governance scope of this committee applies to the following:

1. Everyone employed by the University or any affiliates (such as external agencies such as the University Practice Plan, third party vendors, etc.) who have access to University-related data and information;

2. All Institutional Data created, collected, analyzed, and reported on by WSU units as part of their administrative and academic functions, regardless of where they are located and in what medium they are stored (e.g., physical or electronic), how they are accessed, and how they are transmitted;

3. Sensitive information which is subject to privacy considerations or has been classified as confidential and is therefore subject to protection from public access or inappropriate disclosure. Sensitive information, including personally identifiable information (PII), is defined in University Policy 07-2: Confidential Information Policy

B. The governance scope does not apply to data created, collected, or analyzed for the sole purpose of research that does not require the use of Institutional Data. Although those data are beyond the scope of this committee, they are subject to the requirements of University Policy 07-2: Confidential Information Policy, which applies to all University-related data, as well as restrictions imposed by Federal and State laws governing research on human subjects.

V. PRINCIPLES

The following principles are set forth as minimum standards to govern the appropriate use and management of Institutional Data.

A. Institutional Data is the property of the Wayne State University and shall be managed through defined governance standards, policies, and procedures.

B. Institutional Data shall be safeguarded and protected according to security, privacy, and compliance rules and regulations established by the federal and state government, and Wayne State University policies. This policy is not intended to supersede federal and state rules and regulations, but to promote and reinforce them.

C. Roles and responsibilities involving the management and use of Institutional Data should be clearly defined, and individuals assigned to specific roles will be held accountable for their data management responsibilities.

D. The Data Governance Committee shall coordinate the resolution of issues related to risks, costs, access, management, and use of Institutional Data with the appropriate Data Stewards and with WSU leadership.

VI. ROLES AND RESPONSIBILITIES

The following roles and responsibilities are defined, for both individuals and groups, for the purpose of establishing clear governance and accountability over Institutional Data. The terms and conditions for appointments and assignments are outlined for each.

A. Data Governance Executive Sponsors

1. Associate Provost for Academic Programs/Associate Vice President for Institutional Effectiveness and Chief Information Officer/Associate Vice President for C&IT.

Associate Provost for Academic Programs/Associate Vice President for Institutional Effectiveness and Chief Information Officer/Associate Vice President for C&IT shall lead institutional officers responsible for developing and implementing the University's data governance program.

2. Chief Information Officer and Associate Vice President, Computing and Information Technology

   The Chief Information Officer and Associate Vice President, Computing and Information Technology is responsible for setting and enforcing standards and guidelines for data management technologies and systems related to computing infrastructures, data processing performance, data delivery and integration, data architectures and structures, metadata repositories, and access control mechanisms. The Chief Information Officer and Associate Vice President, Computing and Information Technology has custodial authority over centralized Institutional Data Systems, including the student, financial, and human resources databases.

3. Information Systems Management Committee/Data Governance Steering Committee (ISMC/DGSC)

   ISMC/DGSC are Data Owners and have authority and responsibility over policies and procedures regarding access and usage of data within their delegations of authority, as well as setting work priorities. The Data Governance Core Committee (DGCC) serves in an advisory capacity to ISMC/DGSC on strategic matters and conflict resolution issues.

B. Data Governance Core Committee (DGCC)

The Data Governance Core Committee is a cross-functional, university-wide group dedicated to implementing a data governance program at the University. Committee members are appointed by the Data Governance Steering Committee. The appointed Committee members include representatives from University Counsel, Business Units, Institutional Research and Analysis, C&IT, Enrollment Management, Registrar, Human Resource, Business and Finance, and other senior University personnel. The DGCC may create subcommittees and task forces as needed to carry out its responsibilities.

The DGC's responsibilities include:

I. **Access**: Defining a single set of procedures for requesting permission to access data elements in Institutional Databases and, in cooperation with Stewards, documenting these common data-access request procedures.

II. **Conflict Resolution**: Resolving conflicts in the definition of centrally-used administrative data attributes, data policy, and levels of access. Resolving issues with regard to standard definitions for data elements that cross stewardship boundaries.

III. **Data Administration**: Applying formal guidelines and tools to manage the University's data resources. Overseeing the administration and management of all Institutional Data.

IV. **Data Management**: Establishing policies and procedures that manage Institutional Data as a University resource and communicating them to the University community.

a. Establishing specific goals, objectives, and action plans to implement the policy and monitor progress in its implementation.
b. Identifying data entities and data sources that comprise Institutional Data. As this is an ongoing process, the committee will add data entities and sources to the scope of Institutional Data as circumstances require.

C. WSU Information Security Officer

As a member of the DGCC, the WSU Information Security Officer (or designee) represents the University's Information Security Program. The individual works with campus leadership to improve the security posture of the University & will document best practices around security and privacy.

D. WSU Information Privacy Officer

The WSU Information Privacy Officer works with stakeholders across the university to maintain and establish privacy notices, standards, processes and policies. In conjunction with the Office of General Counsel, the individual ensures that the institution complies with applicable state, federal, and international laws, campus policies and procedures, and industry privacy standards. The individual may advise campus constituents on best practices, privacy complaints, and potential risks.

E. WSU Information Quality Officer

As an authoritative source for WSU official data, the Office of Institutional Research and Analytics (OIRA) Officer will function as the Chief Data Quality Officer, focusing on continuous improvement on data quality and data integrity through regular data audit.

F. Data Owners

Data Owners are University officials accountable for one or more Systems of Record (SOR) and are responsible for ensuring that data is in compliance with policies and standards. Data Owners are accountable for managing, protecting, and ensuring the integrity and usefulness of the University data. They are responsible for identifying the sensitivity and criticality of data.

Data Owners set priorities and provide support for the Data Governance program and delegate data governance responsibilities accordingly to Primary and Associate Data Stewards.

G. Primary and Associate Data Stewards

Data Stewards are subject matter experts (SME's) within business units and ensure **compliance** with applicable federal and state rules and regulations and University policies involving Institutional Data. Data Stewards are responsible for minimizing the use, storage, and exposure of sensitive information, particularly personally identifiable information. They have responsibility to restrict the use and exposure of such information to those specific situations where it is essential and appropriate.

Data Stewards are responsible for the day-to-day use and management of Institutional Data. Data Stewards exist among all levels and across all units within the University. The Registrar, financial aid office, admission office, fiscal managers, human resources specialists, and institutional researchers are among those considered Data Stewards.

Data Stewards engage in the following types of data related activities:

a. Ensure Institutional Data is managed appropriately, according to policies and procedures;

b. Recommend enhancements for their respective program areas to improve data quality, access, security, performance, and reporting;

c. Serve as a conduit between functional and technical personnel to promote communication and a shared understanding of requirements;

d. Fulfill data requests according to administrative procedures on data sharing.

H. Custodians

Data Custodians are the managers and/or administrators of systems or media on which sensitive information resides, including but not limited to personal computers, laptop computers, PDAs, smartphones, departmental servers, enterprise databases, storage systems, magnetic tapes, CDs/DVDs, USB drives, paper files, and any other removable or portable devices or off-site storage technologies such as, but not limited to, cloud storage or cloud services. Information technology personnel are commonly regarded as Data Custodians, however, any authorized individual who downloads or stores sensitive information onto a computer or other storage device becomes a Data Custodian through that act.

Data Custodians are responsible for the technical safeguarding of sensitive information, including implementing and administering controls that ensure the transmission of sensitive information is secure and access controls to prevent inappropriate disclosure are in place.

I. Innovation Leads

Innovation leads advise the Data Governance Core Committee on the advantageous use of new and emerging technologies.

J. Compliance Leads

Compliance Leads ensure compliance with all existing and emerging laws and policies.

K. Strategic Stakeholders

Strategic Stakeholders actively participate in Data Governance and ensure that policies and procedures created by the Data Governance Steering Committee and the Data Governance Core Committee are aligned with the university’s strategic plan, mission and values.