Developing an Institution-Wide Data Management Policy

Custom Research Brief

Research Associate
Jon Barnhart

Research Manager
Joe LeMaster
LEGAL CAVEAT
The Advisory Board Company has made efforts to verify the accuracy of the information it provides to members. This report relies on data obtained from many sources; however, and The Advisory Board Company cannot guarantee the accuracy of the information provided or any analysis based thereon. In addition, The Advisory Board Company is not in the business of giving legal, medical, accounting, or other professional advice, and its reports should not be construed as professional advice. In particular, members should not rely on any legal commentary in this report as a basis for action, or assume that any tactics described herein would be permitted by applicable law or appropriate for a given member’s situation. Members are advised to consult with appropriate professionals concerning legal, medical, tax, or accounting issues, before implementing any of these tactics. Neither The Advisory Board Company nor its officers, directors, trustees, employees and agents shall be liable for any claims, liabilities, or expenses relating to (a) any errors or omissions in this report, whether caused by The Advisory Board Company or any of its employees or agents, or sources or other third parties, (b) any recommendation or graded ranking by The Advisory Board Company, or (c) failure of member and its employees and agents to abide by the terms set forth herein.

The Advisory Board is a registered trademark of The Advisory Board Company in the United States and other countries. Members are not permitted to use this trademark, or any other Advisory Board trademark, product name, service name, trade name and logo, without the prior written consent of The Advisory Board Company. All other trademarks, product names, service names, trade names, and logos used within these pages are the property of their respective holders. Use of other company trademarks, product names, service names, trade names and logos or images of the same does not necessarily constitute (c) an endorsement by such company of The Advisory Board Company and its products and services, or (b) an endorsement of the company or its products or services by The Advisory Board Company. The Advisory Board Company is not affiliated with any such company.

IMPORTANT: Please read the following. The Advisory Board Company has prepared this report for the exclusive use of its members. Each member acknowledges and agrees that this report and the information contained therein (collectively, the “Report”) are confidential and proprietary to The Advisory Board Company. By accepting delivery of this Report, each member agrees to abide by the terms as stated herein, including the following:
1. The Advisory Board Company owns all right, title and interest in and to this Report. Except as stated herein, no right, license, permission or interest of any kind in this Report is intended to be given, transferred to or acquired by a member. Each member is authorized to use this Report only to the extent expressly authorized herein.
2. Each member shall not sell, license or republish this Report. Each member shall not disseminate or permit the use of, and shall take reasonable precautions to prevent such dissemination or use of, this Report by (a) any of its employees and agents (except as stated below), or (b) any third party.
3. Each member may make this Report available solely to those of its employees and agents who (a) are registered for the workshop or membership program of which this Report is a part, (b) require access to this Report in order to learn from the information described herein, and (c) agree not to disclose this Report to other employees or agents or any third party. Each member shall use, and shall ensure that its employees and agents use, this Report for its internal use only. Each member may make a limited number of copies, solely as adequate for use by its employees and agents in accordance with the terms herein.
4. Each member shall not remove from this Report any confidential markings, copyright notices and other similar indicia herein.
5. Each member is responsible for any breach of its obligations as stated herein by any of its employees or agents.
6. If a member is unwilling to abide by any of the foregoing obligations, then such member shall promptly return this Report and all copies thereof to The Advisory Board Company.
Table of Contents

I. Research Methodology .............................................................................................................. 4
   Research Challenge ................................................................................................................ 4
   Project Sources ...................................................................................................................... 4
   Definition of Terms .................................................................................................................. 5
   Research Parameters .............................................................................................................. 6

II. Executive Overview ............................................................................................................... 7
    Key Observations .................................................................................................................. 7

III. Data Management Policy Creation and Approval ............................................................... 8
    Data Management Policy Approval Processes ........................................................................ 8
    Policy Development Stakeholders ......................................................................................... 11

IV. Definitions within Data Management Policies ...................................................................... 13
    Defining Data Access Rules and User Responsibilities .......................................................... 13
    Resources for Defining Data Types ......................................................................................... 14

V. Implementing Data Management Policies .......................................................................... 15
    Communicating Policy Changes to Stakeholders .................................................................... 15
    Ensuring Compliance with Policy Changes ........................................................................... 16
I. Research Methodology

**Research Challenge**

*Leadership at a member institution approached the Forum with the following questions:*

**Developing a Data Management Policy Framework**
- What stakeholders are involved in the development of an institution-wide data management policy?
- What departments provide input into the language of the policy?
- What is the approval process for a data management policy?
- What resources (e.g., other colleges and universities, professional organizations, government entities) are consulted when developing a data management policy?
- How do other institutions develop definitions for types of data under the policy?
- What other rules and procedures are outlined in a data management policy?
- What are the responsibilities of non-IT departments and divisions under an institution-wide data management policy?

**Implementing a Data Management Policy**
- How is an institution-wide data management policy communicated to the broader campus community?
- How do other institutions ensure compliance with a new data management policy?
- What implementation barriers did other institutions encounter after the development of a data management policy framework? How were they overcome?

**Project Sources**

- Education Advisory Board’s internal and online research libraries ([www.educationadvisoryboard.com](http://www.educationadvisoryboard.com))
- Institutional websites and data management policies
  - Institution A: Fast Facts
  - Institution A: Information Management Policy
  - System A: Policy Development Process
  - System A: Information Management Policy
  - Institution B: Fast Facts
  - Institution B: Information Management Policy
  - Institution C: Fast Facts
  - Institution C: Information Management Policy
  - Institution D: Information Management Policy
**Definition of Terms**

- **Institutional Data:** Institutional data is defined as such if it meets one or more of the following criteria:
  - Relevant to planning, managing, operating, or auditing a major administrative function of the university
  - Referenced or required for use by more than one organizational unit
  - Derives a data element that meets these criteria

- **Data Access Categories:** These categories label each entry of information in a database with appropriate restrictions. Access categories consist of open data, internal data, and restricted data. More detailed definitions are located on page 13.
  - *Data users* include any individual who has access to institutional data.
  - *Data owners* create and dictate access to information.
  - *Data custodians* maintain information without owning it.

- **Data Types:** Within this report, the term *data types* refers to the format, origin, and content of specific data entries. A few examples may include “course syllabus” which is a Word document (.doc, .pdf), created by Professor A on his or her office computer. Definitions of data types vary by institutional preferences for information access and responsibilities of individuals.

---

1 System A, Information Management Policy
The Forum interviewed policy and privacy officers and directors of institutional research at public institutions.

### A Guide to the Institutions Profiled in this Brief

<table>
<thead>
<tr>
<th>Institution</th>
<th>Region</th>
<th>Type</th>
<th>Approximate Enrollment (Undergraduate/Total)</th>
<th>Carnegie Classification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Institution A</td>
<td>Northeast, Canada</td>
<td>Public</td>
<td>23,000/27,000</td>
<td>N/A</td>
</tr>
<tr>
<td>System A</td>
<td>Midwest</td>
<td>Public</td>
<td>110,000 (Total Enrollment)</td>
<td>N/A</td>
</tr>
<tr>
<td>Institution B</td>
<td>Mountain West, Canada</td>
<td>Public</td>
<td>11,000/14,000</td>
<td>N/A</td>
</tr>
<tr>
<td>Institution C</td>
<td>Northeast, Canada</td>
<td>Public</td>
<td>17,000 (Total Enrollment)</td>
<td>N/A</td>
</tr>
<tr>
<td>Institution D*</td>
<td>South</td>
<td>Public</td>
<td>24,000/31,000</td>
<td>Research Universities (very high research activity)</td>
</tr>
</tbody>
</table>

**Sources:** National Center for Education Statistics (NCES)

Institution A: Fast Facts
Institution B: Fast Facts
Institution C: Fast Facts

* Institution D did not participate in a research interview, but the institution’s data management policy is profiled in this report.
II.  Executive Overview

Key Observations

During the drafting phases, policy developers at all profiled institutions consult stakeholder groups with exposure to the most institutional data, such as the registrar’s office or business affairs personnel. These stakeholder groups develop language that allows each division to comply with policy changes despite different information management practices; the groups simplify language associated with data management processes, such as data input, maintenance, and destruction. Other stakeholder groups that must approve policy changes include faculty committees, student affairs divisions, and institutional research departments.

Data access categories allow institutions to regulate permission to certain data; data access categories include open data, internal data, and restricted data. Within the policy, policy developers define data access categories that detail how certain information types are added to a database, which individuals may access certain information, and what storage maintenance data require.

Data management roles and responsibilities are separated into three categories: data users, data owners, and data custodians. Data users refer to individuals or divisions that engage institutional data, such as students who access library journal archives. Data owners create content and submit materials to institutional databases, such as professors that post lecture notes online for students. Data custodians maintain data without owning the information, such as Oracle, who maintains all Banner product data but does not own or use the information.

Policy developers leverage technological professional organizations, government associations, and other higher education institutions to create data management definitions for data access, data types, and related roles and responsibilities. Contacts at all profiled institutions consult definitions from other higher education institutions in the same province or state to ensure policies comply with regional privacy and information laws. Technological professional organizations provide industry-specific data type definitions to ensure policy language is broad enough as not to require constant updates. Government associations provide sample data definitions as guidelines for institutions to customize and dictate legal standards.

Stakeholder education is a significant barrier to policy implementation; contacts explain compliance is easier to achieve when policies receive input from a variety of stakeholder groups. Communication strategies include individual meetings with division leaders throughout the drafting process and campus-wide emails with specific policy change information.
### Data Management Policy Creation and Approval

**University Systems Require Approval from Multiple Stakeholder Groups from Each Campus**

System A relies on the Association of College and University Policy Administrator’s process for policy approval. The process consists of multiple drafting periods and steps to engage different stakeholder groups.

**Association of Colleges and University Policy Administrators Approval Process**

<table>
<thead>
<tr>
<th>Predevelopment Phase</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>1.</strong> Identify Issues: The policy office proactively identifies areas of concern, such as inconsistent data management policies and practices across institutions within the system.</td>
</tr>
<tr>
<td><strong>2.</strong> Conduct Analysis: A policy committee, which consists of data stewards, data managers from impacted divisions (e.g., registrar’s office, budget office), and policy officers, identifies which offices will be impacted by policy changes and which committees will need to approve policy amendments.</td>
</tr>
<tr>
<td><strong>3.</strong> Decision: The committee determines if current policies address concerns identified in previous steps; if they do not, the committee begins to construct an institution-wide policy framework, which includes scope, policy statement, reason for policy development, procedures, definitions, and sanctions.</td>
</tr>
</tbody>
</table>

*Contacts at System A report policy approval can take up to six months to complete.*
Development Phase

### Development

4 **Draft Language:** Data managers from impacted divisions develop policy language that allows divisions to comply with policy changes despite different information management practices. The committee also crafts definitions for data types, access categories, and staff roles and responsibilities during this step.

5 **Review and Approve Drafts:** Policy developers present initial drafts to several stakeholder groups for approval, beginning with impacted divisions on the policy development committee. Each committee reviews drafts and makes suggestions about processes and definitions specific to their division, such as student affairs administrators defining which data types student workers can and cannot access. After each meeting, policy language is adjusted to reflect recommendations from each group.

6 **Policy Distribution and Education:** After several group approvals, the committee establishes a functional version of the policy—one that could be operational but requires further approvals—and posts it to university policy websites. Policy developers then continue to discuss changes with impacted divisions that still must approve amendments. Unlike previous meetings, these discussions examine how divisions will comply with policy changes, and policy developers help impacted divisions develop practices before policy changes go into effect.

### Approval from 28 Stakeholder Groups at System A

**System A** requires 28 separate stakeholder groups and committees with representatives from each campus to approve institution-wide policy changes. These committees include faculty councils from each campus, IT-specific committees, business office representatives, and central IT staff. Contacts report this process generates input from all impacted divisions about how new procedures will alter common operations, such as data destruction. This proactive approach also decreases procedural concerns once policies are in place as divisions leaders develop steps for staff to follow to ensure compliance.
Maintenance Phase

7 Review Language: As the policy continues through approval committees, the policy office ensures processes and definitions will remain current and not require amendment for three to five years. This requires broad, flexible policy language that can be adapted to new technologies without revision; policy developers create separate procedural practices to accommodate new processes as technology evolves.

8 Measure Outcomes: Data managers from impacted divisions plan procedural tests to ensure divisions can comply with policy changes. These tests require division staff to identify appropriate data types and label information in databases with correct data access categories. Data managers report results to policy developers and compliance officers.

Shorter Policy Approval Processes only Include Senior Management

The policy approval process at Institution A requires significantly less approval from various stakeholder groups but still engages affected divisions in the drafting process. Additionally, a single individual—the Assistant Director of Information Security and Operating Platforms—authors the data management policy, rather than a drafting committee.

Data Management Policy Approval Process at Institution A

Identify Problems and Consult Best Practices

Policy Drafting and Approval

1 Identify Problems and Consult Best Practices: The Assistant Director of Information Security and Operating Platforms authored the current data management policy at Institution A and amends policy language and procedures. Upon identification of an outdated definition or procedure, the assistant director consults corporate resources, such as Gartner’s research on data management, to identify current trends in data type definitions. The assistant director also reviews new regulations from provincial or national laws on data management and privacy during this phase.
2 **Draft Proposal with Assistance from Affected Divisions:** The assistant director consults division leaders from several divisions that will be impacted by changes to the data management policy, such as the Director of Libraries, the Registrar, the Director of Human Resources, and the Budget and Finance Director. After a review of best practices in information definitions and procedures, the committee determines potential amendments and the assistant director drafts a proposal for senior management to review.

3 **Review Proposal with Senior Management and all Other Affected Divisions:** Senior management, which includes members of the chancellor’s cabinet and several IT directors, reviews the initial proposal and determines if additional divisions will be impacted. The assistant director then meets division leaders one-on-one to discuss policy amendments and any foreseeable compliance concerns with new procedures.

4 **Edit Proposal and Submit to Senior Management for Approval:** The assistant director edits the proposal to reflect division leaders’ suggestions. Senior management reviews the amended proposal and votes to approve the final amendments; the policy is in effect immediately following the vote and the assistant director communicates policy changes to all division leaders. This communication includes a university-wide email, updates to policy websites, and an article on the university’s news site.

---

**Policy Development Stakeholders**

**Policymakers Consult with Divisions that Frequently Input and Access Information**

Contacts note that feedback from these stakeholders is critical because each division’s day-to-day responsibilities require access to large amounts of data and frequent input of information.

**Stakeholders to Involve when Drafting Data Management Policy Changes**

<table>
<thead>
<tr>
<th><strong>Human Resources:</strong> Compiles and maintains sensitive information</th>
<th>Policy developers at <strong>System A</strong> partner with human resources division leaders to understand how changes to data management policies alter access to sensitive data. Human resources staff leverage experience educating individuals about job responsibilities and help to reinforce compliance practices among impacted divisions.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Registrar’s Office:</strong> Oversees input of large amounts of information</td>
<td>Contacts at <strong>Institution C</strong> report the registrar’s office inputs more data than most divisions, and the Registrar offers insights for secure data transfer practices and efficient input processes. The registrar also provides suggestions on how procedures can improve under the new policy.</td>
</tr>
<tr>
<td><strong>Budget and Finance:</strong> Leverages data for strategic planning</td>
<td>Budget and finance personnel at <strong>Institution B</strong> help develop access rules and storage protocols in data management policies; contacts explain these personnel maintain different access requirements and frequently pull data for strategic planning purposes. Their perspectives help policy developers define access categories early in the policy development process.</td>
</tr>
<tr>
<td><strong>Student Affairs:</strong> Manages access for students, the largest population of data users</td>
<td>Student affairs personnel at <strong>Institution C</strong> identify considerations for student data users, such as access to university and third-party research databases and restrictions on downloaded materials, such as pirated music or videos.</td>
</tr>
<tr>
<td><strong>Faculty Relations:</strong> Expresses concerns regarding access and privacy</td>
<td>The privacy officer at <strong>Institution A</strong> meets faculty one-on-one during the drafting phase to discuss access to restricted content for research purposes. While policies detail strict guidelines for what are and are not acceptable uses of university resources, policies must also include procedural exceptions, such as when a professor conducts research on anti-government groups that requires the university to unblock certain web-based content.</td>
</tr>
</tbody>
</table>
IV. Definitions within Data Management Policies

Defining Data Access Rules and User Responsibilities

Open Data, Internal Data, and Restricted Data are the Most Common Data Access Categories across Profiled Institutions

Most contacts identify the creation of policy definitions as the starting point for development of new data management policies.

Categories of Data Access from Institution D and System A

- **Open Data** are available for public access. Often referred to as “public data,” this data type requires no institution-specific login or hardware to access. Examples of open data include enrollment data, press releases, or staff contact information.

- **Internal Data** are accessible to university employees without restriction but are not intended for the general public. Often referred to as “university-internal data,” internal data is the default classification for all data in institutional databases at time of entry. Examples of internal data include department budget information, alumni contact information, or student transcript information.

- **Restricted Data** require specific authorization for any employee to access; access is generally not granted to nonemployees or the public. Often referred to as “limited-access data,” restricted data are constrained by legal, ethical, or other limitations, and policies often detail procedures for granting access to this type of data. Examples of restrictive data include institutional subpoenas, some institutional financial information, or student medical records.

Data Management Policies Assign Responsibilities to All Data Users regarding Data Input, Maintenance, and Destruction

Role and responsibility definitions illustrate a baseline for policy compliance; they assign specific labels with an individual’s responsibilities as it pertains to his or her role in data input, maintenance, and destruction.

Data Management Roles and Responsibilities at Institution A*

<table>
<thead>
<tr>
<th>Data Users</th>
<th>Data Owners</th>
<th>Data Custodians</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Users are individuals who have access to institutional data as defined by policy; users do not create or control access to or application of data. Examples include students who can access course syllabi for their classes but not other students’ classes.</td>
<td>Data Owners typically create records and are therefore responsible for the access and application of those records. For example, institutional research offices own responses to a survey on dining services and dictate how responses can and cannot be distributed.</td>
<td>Data Custodians preserve and maintain information but do not own data. An example of a data custodian is Google, who oversees the infrastructure for all Gmail accounts but does not own the rights to the content within each account.</td>
</tr>
</tbody>
</table>

1. Institution D, Information Management Policy
2. System A, Information Management Policy
3. Institution D, Information Management Policy
4. Institution A, Information Management Policy
Resources for Defining Data Types

Profiled Institutions Consult Definitions from Government Resources, Private Sector Entities, and Higher Education Peers to Develop Data Type Definitions

Contacts at all profiled institutions rely on sources outside the university to construct definitions for institutional data types; contacts explain these definitions serve as guidelines and require adjustments to match institution-specific access and application policies.

**Defining Types of Data through Third-Party Resources**

<table>
<thead>
<tr>
<th><strong>Peer Institutions:</strong> Review institutions with similar data types</th>
<th>Policy developers at <strong>Institution C</strong> benchmark current data type definitions with peer institutions to ensure terms are broad enough to encompass all university information. Contacts explain peer institutions located in the same province are particularly notable because they also account for regional laws governing data type definitions.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Technological Professional Organizations:</strong> Private sector groups provide best practices</td>
<td><strong>System A</strong> subscribes to the Unified Compliance Framework (UCF), a professional organization, to stay current on technology industry definitions for categorizing data. Contacts explain UCF also provides “compliance tasks” that can be assigned to data types to integrate procedure with policy changes; an example is scheduled tasks, such as restricting input of restricted data after 5pm to avoid unauthorized access.</td>
</tr>
<tr>
<td><strong>Institutional Auditors:</strong> Auditors ensure definitions meet compliance</td>
<td>Policy authors at <strong>Institution A</strong> review university auditors’ recommendations for other institutions to establish a framework for data type definitions. Auditors establish a minimum standard for how definitions should meet compliance; policymakers then customize data type definitions to reflect privacy and procedures for certain data types.</td>
</tr>
<tr>
<td><strong>Government Resources:</strong> Regional and national government entities set guidelines and laws for data types</td>
<td>Contacts at <strong>Institution B</strong> cite province-specific freedom of information legislation as a starting point for data type definitions. Contacts report two regional government organizations maintain guidelines for defining data types as definitions relate to regional legislation.</td>
</tr>
</tbody>
</table>
V. Implementing Data Management Policies

Communicating Policy Changes to Stakeholders

Begin Policy Education during the Drafting Phase

Contacts at most profiled institutions report policy education and communication as a barrier to implementation; contacts explain communication to stakeholder groups is essential because daily operations are likely to change as a result of policy amendments.

Policy and Compliance Communication Strategies across Profiled Institutions

System A requires policy approval from approximately 28 separate groups and committees. During each meeting, policy officers explain impacts of policy changes on operational tasks of specific divisions, such as how student affairs catalogs counseling center visits; policy adjustments are made to accommodate concerns of division leaders. Although not yet finalized, policy developers institute a functional policy so each division can examine new compliance procedures and make suggestions before final approvals.

Policy authors at Institution C discuss proposed policy changes with division leaders one-on-one; this practice provides division leaders with context for policy changes specific to departments and allows communication of changes to division staff. Contacts explain this empowers division leaders to embrace policy changes and provide input from their staff to policy developers before final approval.

Consult More Divisions and Test New Compliance Standards

Discuss Policy Changes One-on-One with Division Managers

Send a Campus-Wide Email

Publish Policy Changes on the Campus Newsfeed

Contacts at all institutions cite campus-wide email as a quick and efficient tool to alert all data users and owners of policy changes. This email includes details on how policy changes impact specific users, such as faculty that can now access research databases from other departments on campus.

Communications staff at Institution A publish policy changes in the university’s daily news briefing; articles describe specific impacts on all data users and owners and provide contact information to direct questions or concerns.
Some Contacts View Compliance as a Separate Process from Policy Development; Some Policies do not Include Procedural Actions

Contacts at some profiled institutions intentionally develop policies that require separate procedural addendums, such as a separate acceptable use procedure for students, faculty, and staff. This process allows policy authors to make compliance easier through policy amendments.

Addressing Compliance Concerns across Profiled Institutions

Policy developers at **Institution C** distribute compliance notices and strategies to each division leader consulted during the policy drafting phase. These memos address specific compliance requirements for each division, such as requirements that residential directors enter data about student health concerns rather than residential advisors.

Institutional auditors at **Institution A** review recent policy changes for potential compliance concerns; auditors then analyze compliance practices of specific divisions and make recommendations to policy developers to ensure each division’s practices are in compliance with university policies. For example, auditors may identify divisions that allow students to input restricted data and recommend that the assistant director define access rules for student workers in a separate compliance policy.

Policy developers at **Institution A** and **Institution C** develop separate procedural policies after data management policies are implemented; these compliance policies detail responsibilities and practices for management of specific data or divisions. Examples of these policies include information security policies, acceptable use policies, data management infrastructure policies, and telecommunications policies.

Established Data Management Policies Facilitate Compliance at **System A**

Contacts at **System A** view compliance as a perceived barrier to policy implementation; faculty and staff believe if compliance will be difficult, the policy must be incomplete. Policy developers, however, find that working with an established data management policy simplifies development of compliance practices. For example, a mobile data security policy received negative feedback from staff about compliance concerns; contacts report that once the data management policy was in place, IT staff could solicit funds from senior management for a new database that automatically archives all mobile information, which mitigates staff compliance.