Policy IT013
Volume 10, Information Technology
Responsible Administrator(s): Vice President and CIO, Information Technology and Assistant Dean, Institutional Research and Effectiveness
Responsible Office(s): Information Technology and Institutional Research and Effectiveness
Issued: March 2015

DATA CUSTODIANSHIP AND ACCESS

POLICY STATEMENT

This policy defines the guidelines for the security, confidentiality and use of data maintained by the Fashion Institute of Technology ("the College" or "FIT"), both in paper and electronic form. This policy also informs each person who is entrusted to access student, employee and/or institutional data of their responsibilities with regard to confidentiality, privacy of eligible student records, safeguarding and use of FIT data.

The purpose of this policy is to provide users with data governance guidance in order to protect institutional data from unauthorized use, including but not limited to acquisition, access, disclosure, retention, and disposal. This policy puts forth best practices in data management custodianship and access and clarifies the roles and responsibilities of various stakeholders in the College. The goal is to streamline the efforts of the entire community as they seek to access and utilize institutional data.

REASON FOR THE POLICY

The College maintains data essential and valuable to the performance of its business. These data resources are regulated by internal policies and local, state and federal laws that identify types of data and restrictions placed on data. This policy incorporates local, federal and state standards, regulations and legislation and establishes responsibilities for all forms of college data for confidentiality, integrity, and availability.

While data are critical to FIT operations and must be shared, it must also be used with care. The benefit of sharing data is greatly diminished through misuse, abuse, misinterpretation or unnecessary restrictions on access. Although some portion of FIT's data is public information, some data are restricted by college policies and local, state or federal legislation. FIT has the right and obligation to protect, manage, secure, and control data under its purview in order to comply with legislation, protect its community and to generate benefits from data use.

Data use governed by this policy include observation and distribution of personal information, the use of data in internal and external reports, and the use of data in information technology applications and projects.

WHO SHOULD READ THIS POLICY

- All members of the FIT community – faculty, administrators and staff
- Anyone at the College who is granted access to data

WHO IS RESPONSIBLE FOR THIS POLICY

- Data Owners
- Data Custodians
- Data Administrators

POLICY TEXT

I. Definitions:

Data Owners - senior college officials or their designees who have planning and policy-level responsibility for data within their functional areas and management responsibility for defined segments of institutional data.

Data Custodians - college officials having direct operational-level responsibility for the management of one or more types of institutional data.

Data Administrators - central or distributed college departments or computer system administrators responsible for the operation and management of systems and servers which collect, manage, and provide access to institutional data.

II. Responsibilities:

A. General

Access to FIT data is provided to college employees to conduct college business. Internal use only and confidential/sensitive data, as defined by this policy, will be made available to employees who have legitimate interest. This may include data collected from students, faculty, staff, contractors, members of the community, or those who have no affiliation with the College. Employees accessing such data must observe the requirements for privacy and confidentiality, comply with the protection and control procedures, and accurately present the data used in any type of reporting. Individuals that have custodianship responsibilities for data access must establish internal controls to ensure that college policies are enforced. All data users (including data owners, data custodians, data administrators and data processors) are responsible for the security and privacy of the data they access as prescribed by this policy and other regulatory policies.

B. Compliance

1. The College forbids the disclosure of internal-use-only data or confidential/sensitive data in any medium, including electronic information, information on paper, and information shared verbally or visually (e.g., telephone or video), except as approved by the data custodians. **The use of any internal-use-only or confidential/sensitive college data for one's own personal gain or profit, for the personal gain or profit of others, or to satisfy personal curiosity is strictly prohibited.** Data users are responsible for the consequences resulting from their misuse or abuse of college data.

2. All individuals accessing college data are required to comply with applicable local, federal and state laws (e.g. FERPA, HIPPA, Gramm-Leach-Bliley), E-Discovery, research data and college policies and procedures regarding security of confidential/sensitive data and to exercise discretion with regard to such data. Any college employee, student, or non-college individual with access to college data who engages in, or allows other individuals to engage in, unauthorized use, disclosure, alteration, or destruction of such data in violation of this policy will be subject to appropriate disciplinary action, including and not limited to dismissal or expulsion, criminal and/or legal action.

C. Functional Responsibilities

Authorization for access to and the maintenance and protection of all college data, particularly confidential/sensitive data are delegated to specific individuals within their respective areas of responsibility.

1. **Data Owners** (also see Appendix A- identifying data owners):

a. Establish policies and direction for the security, privacy and use of all college data and particularly confidential/sensitive data within their respective areas of responsibilities.

b. Identify and appoint data custodians for departments within their areas of responsibility.

2. **Data Custodians** (also see Appendix A- identifying data custodians and areas of responsibility):

a. Grant access to data for legitimate interest and necessary to perform task as defined in this policy. Partner with data users and IT in the creation of reports, workflows, system implementations (any product that uses data under their purview) to ensure that data and information is utilized correctly.

b. Ensure accuracy of all data within their area of responsibility.

c. Annually review access to all data within their area of responsibility with the appropriate data administrator, and update access of users if necessary.

d. Ensure that authorized data users understand their responsibilities with regard to their approved access.

e. Review appeals resulting from decisions to deny access.

3. **Data Administrators**:

a. Assign or configure access to college data as prescribed and approved by the data custodian.
b. Maintain documentation of data users who have been authorized access to confidential/sensitive data. Where an abuse of privileges is discovered, make access removal recommendations to the appropriate data custodian.
c. Ensure the usability, reliability, availability, and integrity of information systems and the associated data.

4. **Data Processor**:

a. Accurately input and present data. Data processors will be held responsible for their intentional misrepresentation of data.
b. Maintain data integrity. Upon recognizing that any data elements are in error, the data processor will notify the appropriate data custodian.

5. **Data User:** (includes computer programmers and data analysts):

a. Use internal use only and confidential/sensitive data only as required to perform the employee's job responsibilities and as authorized by the appropriate data custodian.
b. Respect and protect the confidentiality and privacy of individuals whose records to which they have access.
c. Abide by federal, state and local laws and college policies and procedures with respect to access, use, and disclosure of confidential/sensitive data.
d. Report any suspected breach in computer security, misuse or abuse of confidential/sensitive or internal use only data to the data owner or data custodian.

PROCEDURES

While the requirements for complying with confidentiality regulations and ensuring data accuracy are straightforward, additional description of how this policy will be carried out in data reporting and information technology application development projects is in order. These guidelines are included below. Approval and routing forms used for reports and IT applications should be modified to reflect these guidelines.

1. Reporting

In their roles as analysts and programmers, many employees at FIT have the access to data and the technical skills to produce a wide variety of reports. Care must be taken in reporting projects to work with the data owners and custodians to ensure that data is accurately used and that reporting efforts are coordinated.

Problems may include inaccuracy of data and inconsistencies in results of reports that use the same or similar data.

This policy requires that requests for reports that are produced by analysts and programmers be routed through the offices of the appropriate data owners and custodians.

2. Information technology application development

Information technology projects often involve the input or export of data across systems, distribution of information, and event-triggering based on data outcomes. It is essential that, in the planning of these projects and throughout their development, that the appropriate data owners and custodians be informed and involved.

For example, no project involving the use of student course or enrollment data shall take place without the knowledge of the Vice President for Enrollment Management and Student Success and the involvement of the Registrar's office.

RELATED POLICIES

- Acceptable Use and Data Security For Cloud Systems
- Computer and Network Use
- FERPA
- Identity Theft
- Password Change
- Privacy and Confidentiality

RELATED DOCUMENTS

- Banner/Hyperion/BDM/Nolij Access Form
- Data Classification Owner Table (Appendix A)

CONTACT(S)

- **Vice President and CIO**
  Information Technology
  236 W. 27th St., 2nd Floor
  212.217.3400

- **Assistant Dean**
  Institutional Research and Effectiveness
  Feldman Center, Room C110
  212.217.3070