Data Request Policy

Institutional Analysis Mission Statement
The Office of Institutional Analysis office serves as a reliable source for comprehensive and authoritative information about the University of Michigan-Flint.

Institutional Analysis is responsible for collecting, analyzing, and distributing data and information related to the general operations of the institution. The office works with data from various areas related to students, faculty, programs, personnel, facilities and finance. It serves as the primary contact with state and federal agencies, guidebooks, and higher education organizations for information reporting.

Data Request Directions
Follow the steps below to request access to Institutional Analysis Tableau dashboards:

1. Fill out the Data Request Form
2. If the request is able to be fulfilled, you will be contacted within 3 business days by a member of Institutional Analysis.

Proper Use of Student Data
Any and all data requests require a legitimate educational interest. This means that “the need to review an education record in order for a University official to carry out his or her responsibilities in regard to performing an administrative task outlined in the official’s duties, or performing a supervisory or instructional task directly related to the student’s education (Academic Policies of the University).” Students’ educational records are protected under the Family Educational Rights and Privacy Act (FERPA). “FERPA applies to all educational records in whatever medium which are: 1. maintained by the University of Michigan-Flint or by a party acting for the university, and 2. directly related to a student (Understanding Privacy Rights).”

How to identify Sensitive Data
“The University of Michigan follows a three tiered definition of different kinds of data:

Public Data:
This is data that, when disclosed to the general public, poses virtually no risk to the university's reputation, resources, services, or individuals. This information can be readily found on many University of Michigan - Flint websites without login. Examples include information found in the University of Michigan Directory or on the University of Michigan - Flint Homepage.

Private or Confidential Data:
If Private or Confidential data is disclosed without authorization, moderate adverse effects on the University’s reputation, resources, services, or individuals could occur. It is safe to assume that all data, unless indicated that it fits into another category, fits into this category.

Sensitive Data:
Unauthorized disclosure of this data could have serious adverse effects on the University's reputation, resources, services, or individuals. This data needs to have the utmost level of protection to ensure its safety. There are two kinds of sensitive data:

Regulated Sensitive Data:
Data Request Policy

This data is sensitive data that is regulated and protected under federal or state law. Depending on the type of regulated sensitive data and the restrictions already in place, additional measures to protect this data may be needed. Examples of this include Social Security numbers or Protected Health Information (HIPAA).

**Unregulated Sensitive Data:**
This data is sensitive data that is NOT regulated and protected under federal or state law. However, this data is still extremely delicate due to proprietary, ethical, or privacy concerns. This includes things like your current UMFlint password (Identifying Sensitive Data).

**How to store sensitive data**
You are responsible for the data you download. If you are not sure about the sensitivity level of the data you have; keep it on your personal network drive (H). Do not save it to a local or removable storage device. In the case that it must be transported on an external hard drive. Be sure that the data is on an encrypted hard drive. Please contact ITS for assistance if you are not sure how to properly encrypt and protect the data in your possession.

**How to share data between co-workers with a legitimate educational interest**
It is required that any sensitive student data be transmitted via encrypted channels. There are a couple options to achieve this. The first and easiest option is to use file locker located at https://files.umflint.edu. The second option is to enable email encryption on all devices sending or receiving. Please see the “What is Email Encryption” and contact ITS (66804) for instruction on how to configure your email and devices.
References