POLICY PURPOSE
This policy has three purposes: (1) To establish FMS as the first data system that all Plant units will attempt to use before setting up or purchasing a separate data system; (2) to require that all data systems have documentation describing the data access and management practices; and (3) to require that new data system requests outside of FMS be reviewed by the Information Strategy Committee before acquisition.

Plant personnel shall make a reasonable effort to use FMS as the primary data and reporting repository for all Plant Operations data. The use of Microsoft SQL, Access, Excel, or other third party applications shall be avoided and used only as exceptions. Legacy or existing data repositories such as Microsoft Access databases shall be reviewed for transition to FMS or other enterprise capable systems by the Information Strategy Committee (ISC).

SCOPE: DATA SYSTEMS NOT USING FMS
Applies to data systems not using FMS, are not shadow systems, and include primary data not found elsewhere at the U-M.

For exceptions, where FMS cannot be used, a written statement must be documented, vetted and approved by the ISC as to why FMS cannot be used. The ISC has created the Data Systems Request Form to facilitate the processing of FMS exceptions. This form is to be used by units requesting to set up a new data system not presently in existence at Plant Operations. The form is located on the Plant Operations website on the web page titled, “Forms for Plant Operations Employees”. See: http://www.plantops.umich.edu/director/guides/forms/employee_forms.php

A. DATA ACCESS PRACTICES MUST BE DOCUMENTED
For existing data systems:
• Define the business purpose of this data
• If mission critical, the data must be clearly classified as being mission critical
• Instructions for access including screenshots as appropriate
• Who has access to the data, and the type of access they have
• Who approves/initiates access requests?
• Who is the primary owner(s) of the data
• Who has “administrative rights” to the data
• How is the data backed up?
• How to access data in the event that the primary person is absent
• How is the data maintained and updated
• Procedures for accessing data must be defined when staff turnover occurs
1) **Disaster Recovery**
   - Define how the data is protected
   - Define the recovery process if the primary data is destroyed
   - Define where the data is stored
   - Describe the data backup method and frequency
   - Does a manual (paper-based) method exist if the electronic data were inaccessible
   - Is there a backup person to the primary owner

2) **Data Requirements**
   - The data must be stored on a storage system approved by Plant IT that is regularly backed up.
   - The data cannot be stored on local drives (e.g. C Drive)

3) **Shared Accounts**
   - Shared accounts shall not be used for access to data. Unique individual Kerberos accounts must be used to access Plant data. Using individual accounts provides an audit of precisely who accessed the data, and what they did.

**B. DATA ACCESS AND COMPLIANCE FORM**
In addition to any local documentation that Plant Operations units maintain for their data systems, all units running data systems shall be required to fill out the **Data Access and Compliance Form**, and then update this form annually if/as changes occur. This form is located on the Plant Operations website in the web page titled, “Forms for Plant Operations Employees”. See: [http://www.plantops.umich.edu/director/guides/forms/employee_forms.php](http://www.plantops.umich.edu/director/guides/forms/employee_forms.php)

**C. ANNUAL REVIEW OF DATA MANAGEMENT PRACTICES**
At the beginning of each calendar year, Plant IT or the ISC will alert owners/units of data systems that they should validate documentation of their data access procedures. Units with existing documentation stored within the Data Access and Compliance Form will be asked to validate or update the existing documentation on an annual basis.
   - During January of each calendar year, units will review their data access procedures and update or modify them if there are changes.
   - All updates will be completed and confirmed by the Plant Operations Information Strategy Committee by March 31st of each calendar year.

**FAILURE TO COMPLY**
All Plant Unit personnel are expected to comply with this policy. Exceptions shall only be granted in response to a specific limited written request to and by the Manager of Plant IT.

Compliance with this policy is mandated for all Plant Operations employees.