PROTECT MSU DATA

The MSU Institutional Data Policy was released on January 1, 2011, establishing minimum requirements for the appropriate stewardship of the University’s institutional data. The policy applies to all business and academic units and all MSU employees. Michigan State University needs to protect the security and integrity of its institutional data without hindering the effective and efficient use of those data.

WHAT ARE INSTITUTIONAL DATA?

Institutional data are all of the data held by MSU, in any form or medium, for normal business operations.

WHAT ARE CONFIDENTIAL DATA?

• Data that can be used for identity theft or related crimes.
  *(Includes, but not limited to: Social Security numbers, account numbers, date of birth, and mother’s maiden name.)*

• Data whose public disclosure is restricted by law, contract, University policy, professional practice.
  *(Includes but not limited to: student records, medical records, and donor records.)*

• Information concerning MSU’s plans, procedures, and methods for securing data.
  *(Includes but not limited to: passwords, decryption keys, data access controls, and threat assessments.)*

• Data whose value would be lost or reduced by unauthorized disclosure or whose unauthorized disclosure would otherwise adversely affect the University financially.
  *(Includes but not limited to: research data, technical information, and property appraisals.)*

Protecting the university’s information assets and reducing the risk of unauthorized exposure is the RESPONSIBILITY of EVERY member of the MSU community.

KNOW YOUR ROLE

MSU employees need to protect the security of MSU’s institutional data, as well as the associated computer systems and networks that handle the data.

Employees also need to comply with state and federal legislation, funded research program requirements, and associated University policies and guidelines that address protecting the security and confidentiality of institutional data.

eis.msu.edu/idp