Michigan Technological University
Information Technology

Information Security Roles and Responsibilities

Purpose

Under federal, state, regulatory, and contractual requirements, Michigan Tech is responsible for developing and implementing a comprehensive information security program. The purpose of this document is to clearly define roles and responsibilities that are essential to the implementation and continuation of the University's Information Security Plan (ISP).

Definitions

Information System- Any electronic system that stores, processes, or transmits information.

Information Assets- Definable pieces of information in any form, recorded or stored on any media that is recognized as "valuable" to the University

Principle of Least Privilege- Access privileges for any user should be limited to only what is necessary to complete their assigned duties or functions, and nothing more.

Principle of Separation of Duties- Whenever practical, no one person should be responsible for completing or controlling a task, or set of tasks, from beginning to end when it involves the potential for fraud, abuse, or other harm.

Information Security Board of Review

The Information Security Board of Review (ISBR) is an appointed administrative authority whose role is to provide oversight and direction regarding information systems security and privacy assurance campus-wide. In collaboration with the Chief Information Officer (CIO), the ISBR's specific oversight responsibilities include the following:

- Oversee the development, implementation, and maintenance of a University-wide strategic information systems security plan.
- Oversee the development, implementation, and enforcement of University-wide information systems security policy and related recommended guidelines, operating procedures, and technical standards.
- Oversee the process of handling requested policy exceptions
- Advise the University administration on related risk issues and recommend appropriate actions in support of the University's larger risk management programs.

Security and Information Compliance Officers

The Security and Information Compliance Officers oversee the development and implementation of the University's ISP. Specific responsibilities include:

- Ensure related compliance requirements are addressed, e.g., privacy, security, and administrative regulations associated with federal and state laws.

- Ensure appropriate risk mitigation and control processes for security incidents as required.
- Document and disseminate information security policies, procedures, and guidelines
- Coordinate the development and implementation of a University-wide information security training and awareness program
- Coordinate a response to actual or suspected breaches in the confidentiality, integrity or availability of information assets.

Data Owner

A Data Owner is an individual or group or people who have been officially designated as accountable for specific data that is transmitted, used, and stored on a system or systems within a department, college, school, or administrative unit of the University.

The role of the data custodians is to provide direct authority and control over the management and use of specific information. These individuals might be deans, department heads, managers, supervisors, or designated staff. Responsibilities of a Data Owner include the following:

Ensure compliance with Michigan Tech polices and all regulatory requirements

Data Owners need to understand whether or not any University policies govern their information assets. Data Owners are responsible for having an understanding of legal and contractual obligations surrounding information assets within their functional areas. For example, the Family Educational Rights and Privacy Act ("FERPA") dictates requirements related to the handling of student information. Information Technology Services can assist Data Owners in gaining a better understanding of legal obligations.

Assign an appropriate classification to information assets

All information assets are to be classified based upon its level of sensitivity, value and criticality to the University. Michigan Tech has adopted three primary classifications: Confidential, Internal/Private, and Public. Please see the *Data Classification and Protection Standard* for further reference.

Determine appropriate criteria for obtaining access to sensitive information assets

A Data Owner is accountable for who has access to information assets within their functional areas. This does not imply that a Data Owner is responsible for day-to- day provisioning of access. Provisioning access is the responsibility of a Data Custodian.

A Data Owner may decide to review and authorize each access request individually or may define a set of rules that determine who is eligible for access based on business function, support role, etc. Access must be granted based on the principles of least privilege as well as separation of duties. For example, a simple rule may be that all students are permitted access to their own transcripts or all staff members are

permitted access to their own health benefits information. A Data Custodian should document these rules in a manner that allows little or no room for interpretation.

Approve standards and procedures related to management of information assets

While it is the responsibility of the Data Custodian to develop and implement operational procedures, it is the Data Owner's responsibility to review and approve these standards and procedures. A Data Owner should consider the classification of the data and associated risk tolerance when reviewing and approving these standards and procedures. For example, high risk and/or highly sensitive data may warrant more comprehensive documentation and, similarly, a more formal review and approval process.

Data Custodian

Data Custodians play a critical role in protecting University information technology resources. Data Custodians have administrative and/or operational responsibility over information assets and must follow all appropriate and related security guidelines to ensure the protection of sensitive data and intellectual property residing on systems for which they have accountability. Responsibilities of a Data Custodian include the following:

Understand how information assets are stored, processed, and transmitted

Understanding and documenting how information assets are being stored, processed and transmitted is the first step toward safeguarding that data. Without this knowledge, it is difficult to implement or validate safeguards in an effective manner.

One method of performing this assessment is to create a data flow diagram for a subset of data that illustrates the system(s) storing the data, how the data is being processed and how the data traverses the network. Data flow diagrams can also illustrate security controls as they are implemented. Regardless of approach, documentation should exist and be made available to the appropriate Data Owner.

Implement appropriate physical and technical safeguards to protect the confidentiality, integrity and availability of information assets

Information Technology Services has published guidance on implementing reasonable and appropriate security controls for the three classifications of data: Confidential, Internal/Private, and Public. Contractual obligations, regulatory requirements and industry standards also play in important role in implementing appropriate safeguards.

Data Custodians should work with Data Owners to gain a better understanding of these requirements. Data Custodians should also document what security controls have been implemented and where gaps exist in current controls. This documentation should be made available to the appropriate Data Owner.

Document and disseminate administrative and operational procedures to ensure consistent storage, processing and transmission of information assets

Documenting administrative and operational procedures goes hand in hand with understanding how data is stored, processed and transmitted. Data Custodians should document as many repeatable processes as possible. This will help ensure that information assets are handled in a consistent manner and will also help ensure that safeguards are being effectively leveraged.

Provision and de-provision access as authorized by the Data Owner

Data Custodians are responsible for provisioning and de-provisioning access based on criteria established by the appropriate Data Owner. As specified above, standard procedures for provisioning and de-provisioning access should be documented and made available to the appropriate Data Owner.

Understand and report security risks and how they impact the confidentiality, integrity and availability of information assets

Data Custodians need to have a thorough understanding of security risks impacting their information assets. For example, storing or transmitting sensitive data in an unencrypted form is a security risk. Protecting access to data using a weak password and/or not patching vulnerability's in a system or application are both examples of security risks.

Security risks need to be documented and reviewed with the appropriate Data Owner so that he or she can determine whether greater resources need to be devoted to mitigating these risks. Information Technology Services can assist Data Custodians with gaining a better understanding of their security risks.

Data Users

All users have a critical role in the effort to protect and maintain University information systems and data. For the purpose of information security, a Data User is any employee, contractor or third-party provider of the University who is authorized to access University Information Systems and/or information assets. Responsibilities of data users include the following:

Adhere to policies, guidelines and procedures pertaining to the protection of information assets

Information Technology Services publishes various policies, procedures, and guidelines related to the protection of information assets and systems and can be found on the IT web site.

Users are also required to follow all specific policies, guidelines, and procedures established by departments, schools, colleges, or business units with which they are associated and that have provided them with access privileges.

Report actual or suspected security and/or policy violations or breaches to IT

During the course of day-to-day operations, users may come across a situation where they feel the security of information assets might be at risk. For example, a user comes across sensitive information on a website that he or she feels shouldn't be accessible. If this happens, it is the users responsibly to report the situation.

Please see the *Incidence Response Procedure* for further guidance on what steps to take if you suspect a violation or breach.

END OF DOCUMENT
Rev 9/20/16