

Information Security Plan

The Information Security Plan establishes and states the policies governing Michigan Technological University's IT standards and practices. These policies define the University's objectives for managing operations and controlling activities. These top-level policies represent the plans or protocols for achieving and maintaining internal control over information systems as well as compliance with the requirements imposed on the University.

INFORMATION SECURITY PLAN

Approval by Information Security Board of Review Members

Information Security Plan

Table of Contents

1	EXECUTIVE SUMMARY	4
2	PURPOSE.....	4
3	SCOPE.....	5
4	DEFINITIONS.....	5
5	IT GOVERNANCE COMMITMENTS & RESPONSIBILITIES.....	6
6	UNIVERSITY POLICY STATEMENT	6
7	ENFORCEMENT.....	6
8	INFORMATION SECURITY PROGRAM.....	6
8.1	RISK ASSESSMENT.....	7
8.2	CONTROL ACTIVITIES.....	7
8.2.1	<i>Internal controls.....</i>	<i>8</i>
8.2.2	<i>Preventative Controls.....</i>	<i>8</i>
8.2.3	<i>Detective Controls.....</i>	<i>8</i>
8.2.4	<i>Corrective Controls.....</i>	<i>8</i>
8.3	CONTROL ENVIRONMENT	8
8.3.1	<i>Michigan Tech's Security policy</i>	<i>9</i>
8.4	ORGANIZATION OF INFORMATION SECURITY.....	10
8.5	ACCOUNTABILITY FOR ASSETS.....	10
8.6	INFORMATION CLASSIFICATION.....	11
8.6.1	<i>Tier I: Confidential.....</i>	<i>11</i>
8.6.2	<i>Tier II: Internal/ private</i>	<i>11</i>
8.6.3	<i>Tier III: Public.....</i>	<i>12</i>
8.7	INFORMATION HANDLING.....	12
8.8	IDENTITY & ACCESS MANAGEMENT.....	12
8.8.1	<i>Identification</i>	<i>13</i>
8.8.1	<i>Authentication</i>	<i>13</i>
8.8.2	<i>Authorization.....</i>	<i>13</i>
8.8.3	<i>Remote Access.....</i>	<i>14</i>
8.8.4	<i>Privileged Access.....</i>	<i>14</i>
8.8.5	<i>Segregation of Duties.....</i>	<i>15</i>
8.9	COMMUNICATION AND OPERATIONS MANAGEMENT.....	15
8.9.1	<i>Network Security</i>	<i>16</i>
8.9.2	<i>Security Monitoring.....</i>	<i>16</i>
8.9.3	<i>Encryption</i>	<i>16</i>
8.9.4	<i>Virus Protection.....</i>	<i>17</i>
8.9.5	<i>Backup and recovery.....</i>	<i>17</i>
8.10	SYSTEMS & APPLICATION SECURITY	18
8.10.1	<i>Systems development and maintenance</i>	<i>18</i>
8.10.2	<i>Change control.....</i>	<i>19</i>
8.11	PHYSICAL SECURITY MEASURES	20
8.11.1	<i>Physical entry controls</i>	<i>20</i>
8.11.2	<i>Provisioning Process.....</i>	<i>21</i>
8.11.3	<i>Visitors.....</i>	<i>21</i>
8.11.4	<i>Alarms & Surveillance.....</i>	<i>21</i>

8.11.5	<i>Equipment Control</i>	21
8.11.6	<i>Computer data and media disposal policy</i>	21
8.12	BUSINESS CONTINUITY	22
8.12.1	<i>Business Impact Analysis</i>	22
8.12.2	<i>Disaster Recovery</i>	23
8.13	INFORMATION SECURITY INCIDENT RESPONSE.....	24
9	REGULATIONS	24
9.1	FAMILY EDUCATION RIGHTS AND PRIVACY ACT.....	24
9.2	HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT	24
9.3	HEALTH INFORMATION TECHNOLOGY FOR ECONOMIC AND CLINICAL HEALTH ACT	25
9.4	INTERNATIONAL TRAFFIC IN ARMS REGULATIONS/EXPORT ADMINISTRATION REGULATIONS.....	25
9.5	GRAMM-LEACH-BLILEY ACT FOR DISCLOSURE OF NONPUBLIC PERSONAL INFORMATION	25
9.6	RED FLAG RULES.....	25
9.7	PAYMENT CARD INDUSTRY DATA SECURITY STANDARDS	25
10	COMPLIANCE	26
11	RELATED POLICIES & PROCEDURES	26
12	ISP - REVISION HISTORY	27

1 EXECUTIVE SUMMARY

An Information Security Plan (ISP) is designed to protect information and critical resources from a wide range of threats in order to ensure business continuity, minimize business risk, and maximize return on investments and business opportunities.

Information Technology (IT) security is achieved by implementing a suitable set of controls, including policies, processes, procedures, organizational structures, and software and hardware functions. These controls need to be established, implemented, monitored, reviewed and improved, where necessary, to ensure that the specific security and business objectives of Michigan Technological University are met.

This plan governs the privacy, security, and confidentiality of University data, especially highly sensitive data, and the responsibilities of departments and individuals for such data. IT security measures are intended to protect information assets and preserve the privacy of Michigan Tech employees, students, sponsors, suppliers, and other associated entities. Inappropriate use exposes Michigan Tech to risks including virus attacks, compromise of network systems and services, and legal issues.

All users of Michigan Tech's information technology resources are required to follow [2.1009 Information Security Compliance Policy](#) and are bound by this plan as well as other University policies and procedures as terms of their employment. All employees share responsibility for the security of the information and resources in their respective departments.

2 PURPOSE

The purpose of this plan is to ensure the confidentiality, integrity, and availability of data, define, develop, and document the information policies and procedures that support University goals and objectives, and to allow the University to satisfy its legal and ethical responsibilities with regard to its IT resources.

Information security policies and procedures represent the foundation for the University's ISP. Information security policies serve as overarching guidelines for the use, management, and implementation of information security throughout Michigan Tech.

Internal controls provide a system of checks and balances intended to identify irregularities, prevent waste, fraud and abuse from occurring, and assist in resolving discrepancies that are accidentally introduced in the operations of the business. When consistently applied throughout the University, these policies and procedures assure that information technology resources are protected from a range of threats in order to ensure business continuity and maximize the return on investments of business interests.

This plan reflects Michigan Tech's commitment to stewardship of sensitive personal information and critical business information, in acknowledgement of the many threats to information security and the importance of protecting the privacy of University constituents, safeguarding vital business information, and fulfilling legal obligations. This plan will be reviewed and updated at least once a year or when the environment changes.

3 SCOPE

This plan applies to the entire Michigan Tech community, including the President, Vice Presidents, Deans, Directors, and Department Heads, students, faculty, staff, alumni, trustees, temporary employees, contractors, volunteers and guests who have access to Michigan Tech information technology resources. Such assets include data, images, text, or software, stored on hardware, paper or other storage media.

4 DEFINITIONS

Confidentiality- “Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information...”

A loss of *confidentiality* is the unauthorized disclosure of information.

Integrity-“Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity...”

A loss of *integrity* is the unauthorized modification or destruction of information.

Availability- “Ensuring timely and reliable access to and use of information...”

A loss of *availability* is the disruption of access to or use of information or an information system.

Risk Assessment is a process which determines what information technology resources exist that require protection, and to understand and document potential risks from IT security failures that may cause loss of information confidentiality, integrity, or availability.

Control Activities are the policies, procedures, techniques, and mechanisms that help ensure that management's response to reduce risks identified during the risk assessment process is carried out.

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

Access Control refers to the process of controlling access to systems, networks, and information based on business and security requirements.

ISO (International Organization for Standardization) - An international-standard-setting body composed of representatives from various national standards organizations.

NIST (National Institute of Standards and Technology) - A non-regulatory federal agency within the U.S. Department of Commerce whose mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life.

VPN (Virtual Private Network) - A network that uses a public telecommunication infrastructure, such as the Internet, to provide remote offices or individual users with secure access to the University's network. VPN's use encryption and other security mechanisms to ensure that only authorized users can access the network and that the data cannot be intercepted.

IDS (Intrusion Detection System) - A device (or application) that monitors network and/or system activities for malicious activities or policy violations.

IPS (Intrusion Prevention System) - A device (or application) that identifies malicious activity, logs information about said activity, attempts to block/stop activity, and reports activity.

Encryption- Process of converting information so that it is humanly unreadable except by someone who knows how to decrypt it.

5 IT GOVERNANCE COMMITMENTS & RESPONSIBILITIES

IT governance is the responsibility of Executive Management and consists of the leadership, organizational structures, and processes to ensure that the University's information technology sustains and extends Michigan Tech's strategies and objectives.

Executive Management has established the overall approach to governance and control by forming the Information Security Board of Review (ISBR) to provide strategic direction, ensure objectives are achieved, ascertain risks are managed appropriately, and verify that the University's resources are used responsibly.

The Office of Information Technology (OIT) shows its commitment by developing and implementing good internal controls as well as ensuring the promotion and awareness of IT requirements and plans throughout the University. Michigan Tech's strategic vision is linked with the IT departments' goals and objectives, ultimately assuring that the University meets customer and legal requirements while undergoing continual improvement.

6 UNIVERSITY POLICY STATEMENT

Each department will protect University resources by adopting and implementing, at a minimum, the security standards and procedures developed and approved by the Information Security Board of Review that are included within this ISP. All departments must meet the minimum standards. Departments are encouraged to adopt standards that exceed the minimum requirements for the protection of University resources that are controlled exclusively within the Department.

Individuals within the scope of this policy are responsible for complying with this policy and the Department's policy, if one exists, to ensure the security of University resources.

7 ENFORCEMENT

All individuals accessing University data at Michigan Tech are required to comply with federal and state laws, University policies and procedures regarding security of highly sensitive data. Any University employee, student or non-university individual with access to University data who engages in unauthorized use, disclosure, alteration, or destruction of data is in violation of this plan and will be subject to appropriate disciplinary action, including possible dismissal and/or legal action.

8 INFORMATION SECURITY PROGRAM

Through this document and associated policies, Michigan Tech has established, documented, and implemented an Information Security Program. The system is designed to result in improving the effectiveness of IT operations and ability to satisfy regulatory requirements. This program has been implemented to ensure the confidentiality and integrity of University information while maintaining appropriate levels of accessibility.

In order to ensure the security and confidentiality of sensitive information and to protect against any anticipated threats or hazards to the security or integrity of data, the University has put in place all reasonable technological means, (i.e., security software, hardware) to keep information and facilities secure. The University has defined its own security controls, which are to be equal to or greater than security requirements and controls prescribed by law and/or standards bodies (ISO, NIST, etc.).

8.1 RISK ASSESSMENT

A risk assessment is a process which determines what information resources exist that require protection, and to understand and document potential risks from IT security failures that may cause loss of information confidentiality, integrity, or availability. The purpose of a risk assessment is to help management create appropriate strategies and controls for stewardship of information assets. Because economics, regulatory and operating conditions will continue to change, mechanisms are needed to identify and deal with the special risks associated with change.

Objectives must be established before administrators can identify and take necessary steps to manage risks. Operations objectives relate to effectiveness and efficiency of the operations, including performance and financial goals and safeguarding resources against loss. Financial reporting objectives pertain to the preparation of reliable published financial statements, including prevention of fraudulent financial reporting. Compliance objectives pertain to laws and regulations which establish minimum standards of behavior.

Information Technology Services (ITS), with the aid of other departments, will conduct an annual risk assessment and/or business impact analysis in order to:

- Inventory and determine the nature of campus information resources
- Understand and document the risks in the event of failures that may cause loss of confidentiality, integrity, or availability of information resources
- Identify the level of security necessary for the protection of the resources.

8.2 CONTROL ACTIVITIES

Control activities are the policies, procedures, techniques, and mechanisms that help ensure that management's response to reduce risks identified during the risk assessment process is carried out. In other words, control activities are actions taken to minimize risk. When the assessment identifies a significant risk to the achievement of an objective, a corresponding control activity or activities is determined and implemented.

Control activities occur throughout the University, at all levels, and in all functions. They include a range of activities as diverse as approvals, authorizations, verifications, reconciliations, reviews of operating performance, security of assets and segregation of duties.

Control activities usually involve two elements: a policy establishing what should be done and procedures to affect the policy. All policies must be implemented thoughtfully, conscientiously and consistently.

8.2.1 INTERNAL CONTROLS

Internal controls are designed to provide a reasonable assurance that goals and objectives for the University and administrative areas are met. Effective controls provide reasonable assurance regarding the accomplishment of established objectives.

Internal controls, procedures, and practices also ensure that:

- Risks are reduced to an acceptable level
- All assets are safeguarded against waste, fraud, loss, unauthorized use or disclosure, and misappropriation
- Programs are efficiently and effectively carried out in accordance with applicable laws and University policy

Controls are selected based on the cost of implementation relative to the reduction of risk and potential for loss, if and when a security breach occurs. Non-monetary factors, such as loss of reputation, are also taken into account.

The administrative processes within Michigan Tech rely on internal controls to remain in compliance with internal and external requirements. Without adequate internal controls, functions within the University may become non-compliant, inefficient, and too costly to operate, which in turn will ultimately fail. Adequate controls to mitigate risks need to exist in everyday business procedures and can be preventative, detective, or corrective in nature.

8.2.2 PREVENTATIVE CONTROLS

Preventive controls are designed to discourage or pre-empt errors or irregularities from occurring. They are more cost effective than detective controls. Credit checks, job descriptions, required authorization signatures, data entry checks and physical control over assets to prevent their improper use are all examples of preventive controls.

8.2.3 DETECTIVE CONTROLS

Detective controls are designed to search for and identify errors after they have occurred. They are more expensive than preventive controls, but still essential since they measure the effectiveness of preventive controls and are the only way to effectively control certain types of errors. Account reviews and reconciliations, observations of payroll distribution, periodic physical inventory counts, passwords, transaction edits and internal auditors are all examples of detective controls.

8.2.4 CORRECTIVE CONTROLS

Corrective controls are designed to prevent the recurrence of errors. They begin when improper outcomes occur and are detected and keep the "spotlight" on the problem until management can solve the problem or correct the defect. Quality teams and budget variance reports are examples of corrective controls.

8.3 CONTROL ENVIRONMENT

The control environment, as established by the University's administration, sets the tone of the University and influences the control consciousness of its people. Leaders of each

department, area, or activity establish a local control environment. This is the foundation for all other components of internal control, providing discipline and structure.

Managers and employees are to have personal and professional integrity and are to maintain a level of competence that allows them to accomplish their assigned duties, as well as understand the importance of developing and implementing good internal controls.

This requires managers and their staff to maintain and demonstrate at all times:

- Personal and professional integrity and ethical values
- A level of skill necessary to help ensure effective performance
- An understanding of information security and internal controls sufficient to effectively discharge their responsibilities

Managers and supervisors are also responsible for ensuring their employees are aware of the relevance and importance of their activities and how they contribute to the achievement of the control environment.

8.3.1 MICHIGAN TECH'S SECURITY POLICY

The information technology resources at Michigan Tech support the educational, instructional, research, and administrative activities of the University and the use of these resources is a privilege that is extended to members of the University community. Any employee using University information technology resources for any reason must adhere to strict guidelines regarding its use. Employees are being entrusted with the safety and security of University information resources. A sound security policy for information technology resources includes the participation of every employee, at all times. Sound policy promotes information security.

Any person or organization within the University community who uses or provides information technology resources has a responsibility to maintain and safeguard these assets. Each individual student, staff, and faculty member in the Michigan Tech community is expected to use these shared resources with consideration for others.

Individuals are also expected to be informed and be responsible for protecting their own information resources in any environment, shared or stand alone. It is unacceptable for anyone to use information resources to violate any law or University policy or perform unethical academic or business acts.

Michigan Tech's [Acceptable Use of Information Technology Resources](#) contains the governing philosophy for effective and efficient use of the University's computing, communications, and information resources by all members of the University community.

While chairs/directors and supervisors are ultimately responsible for ensuring compliance with information security practices, ITS in cooperation with various departments will develop annual security awareness and compliance training to achieve technical proficiency and appropriate use for all employees who have access to information technology resources.

8.4 ORGANIZATION OF INFORMATION SECURITY

The University assumes a coordinated approach to the protection of information technology resources and depositories of protected information that are under its custody by establishing appropriate and reasonable administrative, technical and physical safeguards that include all departments, individuals, or others that administer, install, maintain, or make use of Michigan Tech's information technology resources.

The Information Security Board of Review's (ISBR) role is to provide oversight and direction regarding information systems security and privacy assurance University-wide.

Chief Technology Officer (CTO) is responsible for the University's IT planning, budgeting, and performance including its information security components. Decisions made in these areas should be based on an effective risk management program.

Security and Information Compliance Officers are responsible for the University's security programs, including risk management. They play a leading role in introducing an appropriate, structured methodology to help identify, evaluate, and minimize risks to the information technology resources that support the University's mission and compliance needs.

Data Owners are responsible for ensuring that proper controls are in place to address integrity, confidentiality, and availability of information technology resources and data they own.

IT security practitioners (e.g., network, system, application, and database administrators; computer specialists; security analysts) are responsible for proper implementation of security requirements within the information technology resources when change occurs.

Data Custodians have a responsibility to the University to ensure they grant access to data to only those who require that access to perform their job responsibilities.

Data User is a person who has been granted explicit authorization to access the data by the owner. The user must use the data only for purposes specified by the owner, comply with security measures specified by the owner or custodian (i.e., securing login-ID and password), and not disclose information or control over the data unless specifically authorized in writing by the owner of the data.

Information Security Roles & Responsibilities describes the overall organization at Michigan Tech. All Information Technology personnel and users with access to sensitive data are required to sign and date the Confidentiality Agreement at time of hire, and annually thereafter.

8.5 ACCOUNTABILITY FOR ASSETS

Information Technology Services, working in cooperation with other campus departments will develop and maintain a Data Owner Matrix defining those persons responsible for each covered data field in relevant software systems (financial, student administration, development, etc.). ITS will conduct ongoing audits, and will report any significant questionable activities, which may compromise security of protected information.

Proper internal control is to be maintained over all information technology resources, at all times. Proper IT asset management – from requisition to disposal – ensures a much greater likelihood that the University will continue to meet customer requirements into the indefinite future by planning in an orderly fashion and mandating consistency throughout the University.

ITS will conduct an annual survey to develop and maintain a registry of those members of the University community who have access to protected information and maintain an inventory of information assets on all campus systems that are considered in-scope. Individuals who are authorized to access institutional data shall adhere to the appropriate roles and responsibilities, as defined within University policy.

8.6 INFORMATION CLASSIFICATION

Information classification is required to determine the relative sensitivity and criticality of information technology resources, which provide the basis for protection efforts and access control. The [*Data Classification and Protection Standard*](#) establishes a baseline derived from federal laws, state laws, regulations, and University policies that govern the privacy and confidentiality of data.

The [*Data Classification and Protection Standard*](#) apply to all data (e.g., student, research, financial, employee data collected in electronic or hard copy form that is generated, maintained, and entrusted to Michigan Tech) except where a different standard is required by grant, contract, or law.

All institutional data must be classified into one of three sensitivity tiers, or classifications that Michigan Tech has identified, which are referred to as Confidential, Internal/Private, and Public. Although all the enumerated data values require some level of protection, particular data values are considered more sensitive and correspondingly tighter controls are required for these values.

All University data is to be reviewed on a periodic basis and classified according to its use, sensitivity and importance to the University and in compliance with federal and/or state laws.

ITS has pre-defined several types of sensitive data. The level of security required depends in part on the effect that unauthorized access or disclosure of those data values would have on University operations, functions, image or reputation, assets, or the privacy of individual members of the University community.

8.6.1 TIER I: CONFIDENTIAL

Confidential information is information whose unauthorized disclosure, compromise or destruction would result in severe damage to the University, its students, or employees (e.g., social security numbers, dates of birth, medical records, credit card or bank account information). Tier I data is intended solely for use within Michigan Tech and is limited to those with a “business need-to-know.”

8.6.2 TIER II: INTERNAL/ PRIVATE

Internal use information must be guarded due to proprietary, ethical or privacy considerations. Although not specifically protected by statute, regulations, or other legal obligations or mandates, unauthorized use, access, disclosure, acquisition, modification,

loss or deletion of information at this level could cause financial loss, damage to Michigan Tech's reputation, or violate an individual's privacy rights (e.g., educational student records, employment history, and alumni biographical information). Tier II information is intended for use by University employees, contractors, and vendors covered by a non-disclosure agreement.

8.6.3 TIER III: PUBLIC

Public information is information that is not publicly disseminated, but assessable to the general public. These data values are either explicitly defined as public information (e.g., state employee salary ranges), intended to be readily available to individuals both on and off campus (e.g., an employee's work email addresses or student directory information), or not specifically classified elsewhere in the protected data classification standard. Knowledge of Tier III information does not expose Michigan Tech to financial or reputational loss, or jeopardize the security of University data. Publicly available data may be subject to appropriate review or disclosure procedures to mitigate potential risks of inappropriate disclosure data in order to organize it according to its risk of loss or harm from disclosure.

8.7 INFORMATION HANDLING

University employees create records as part of the normal course of conducting the business of the University. Records containing highly sensitive information should exist only in areas where there is a legitimate and justifiable business need and maintained under strict controls as outlined in this document

Mishandling of sensitive information is a significant risk to the University, and may cause considerable financial or reputational harm. It is the responsibility of all Michigan Tech employees, regardless of position, to protect sensitive information by being aware of any sensitive information they may store, process, or transmit.

The [Data Classification and Protection Standard](#) outlines the minimum standards for protection of highly sensitive University information. Additional controls required under applicable laws, regulations, or standards governing specific forms of data (e.g., health or financial information, credit card data), may also apply.

8.8 IDENTITY & ACCESS MANAGEMENT

Identity and access management ensures accurate identification of authorized University community members and provides secure authenticated access to and use of network-based services. Identity and access management is based on a set of principles and control objectives to:

- Ensure unique identification of members of the University community and assignment of access privileges
- Allow access to information resources only by authorized individuals
- Ensure periodic review of membership in the community and review of their authorized access rights
- Maintain effective access mechanisms through evolving technologies

Access Control refers to the process of controlling access to systems, networks, and information based on business and security requirements. The objective is to prevent unauthorized disclosure of Michigan Tech's information assets. University access control measures include secure and accountable means of identification, authentication, and authorization. Please see the [Identity and Access Management Policy](#) for further reference.

8.8.1 IDENTIFICATION

Identification is the process of uniquely naming or assigning an identifier to every individual or system to enable decisions about the levels of access that should be given. The key feature of an identity process is that each user of the University community, and any other entity about which access decisions need to be made, is uniquely identifiable from all other users.

8.8.1 AUTHENTICATION

The authentication process determines whether someone or something is, in fact, who or what it is declared to be. Authentication validates the identity of the person. Authentication factors can be something you know (password), something you have (token), or something you are (biometric). Two-factor authentication consists of two of the three factors (e.g., password and token) in these distinct categories. For the purpose of access control, authentication verifies one's identity through IT.

Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may result in the compromise of Michigan Tech's entire network. Adhering to secure password procedures will help reduce the compromise of user accounts on the University's systems. As such, all community users (including students, faculty, staff, guests, contractors and vendors) are responsible for selecting and securing their passwords. Please see [Password Standards](#) for further reference on passwords.

8.8.2 AUTHORIZATION

Authorization is the process used to grant permissions to authenticated users. Authorization grants the user, through technology or process, the right to use the information assets and determines what type of access is allowed (read-only, create, delete, and/or modify).

The access rights to the information must then be entered into the security system via an access list, directory entry, or view tables, for example, so the authorization rules can be enforced. The level of control will depend on the classification of the data and the level of risk associated with loss or compromise of the information.

In addition,

- Criteria must be established by the Data Owner for account eligibility, creation, maintenance, and expiration.
- Highly sensitive data must be individually authorized by the Data Owner and an annual confidentiality agreement must be acknowledged or signed by all authorized users.

-
- Depending on the relative sensitivity of the data, staff may be subject to a security clearance check before they are hired, transferred, or promoted. Any employee who was not subjected to such a clearance check when first hired should not be placed in a sensitive position until security clearance has been obtained.
 - Data Owners must periodically review user privileges and modify, remove, or inactivate accounts when access is no longer required.
 - Procedures must be documented for the timely revocation of access privileges and return of institutionally owned materials (e.g., keys) for terminated employees and contractors.
 - Inactivity time-outs must be implemented, where technically feasible, for terminals and workstations that access highly sensitive data. The period of inactivity shall be no longer than 10 minutes in publicly accessible areas.
 - Audit trails exist for detective and reactive response to system penetration, infection of systems and data due to malicious code, catastrophic system loss or a compromise of data integrity.

8.8.3 REMOTE ACCESS

Remote access to information technology resources (switches, routers, computers, etc.) and to sensitive or confidential information (social security numbers, credit card numbers, bank account numbers, etc.) are only permitted through secure, authenticated and centrally-managed access methods. Systems that contain sensitive student, personnel and financial data will be available for off-site remote access through a centrally managed VPN that provides encryption and secure authentication.

It should also be understood that when accessing sensitive data remotely, it is prohibited to store cardholder or other sensitive data onto local hard drives, floppy disks, or other external media (including laptops and Smartphones).

External computers that are used to administer University resources or access sensitive information must be secured. This includes patching (operating systems and applications), possessing updated anti-virus software, operating a firewall and being configured in accordance with all relevant University policies and procedures.

8.8.4 PRIVILEGED ACCESS

System administrators routinely require access to information resources to perform essential system administration functions critical to the continued operation of the University. Such privileged access is often termed “superuser,” “root,” or “administrator” access. Privileged accounts enable vital system administration functions to be performed and are only to be used for authorized purposes.

The number of privileged accounts is to be kept to a minimum, and only provided to those personnel whose job duties require it. Administrators or users who require privileged accounts should also have non-privileged accounts to use when performing daily routine tasks and should not use their privileged accounts for non-authorized purposes. Activities performed using a privileged account is to be logged and the logs will be reviewed on a regular basis by an independent and knowledgeable person.

Personnel who manage, operate, and support University information systems, including individuals who manage their own systems, are expected to use appropriate professional practices in providing for the security of the systems they manage. Responsibility for systems and application security must be assigned to an individual knowledgeable about the information technology used in the system and in providing security for such technology.

8.8.5 SEGREGATION OF DUTIES

Tasks involved in critical business processes must be performed by separate individuals. Responsibilities of programmers, system administrators and database administrators must not overlap, unless authorized by the Data Owner. Duties and responsibilities shall be assigned systematically to a number of individuals to ensure that effective checks and balances exist. Such controls keep a single individual from subverting a critical process. Key duties include authorizing, approving, and recording transactions; issuing and receiving assets; and reviewing or auditing transactions.

Segregation of duties should be maintained between the following functions:

- Data entry
- Computer operation
- Network management
- System administration
- Systems development and maintenance
- Change management
- Security administration
- Security audit

Qualified and continuous supervision is to be provided to ensure that internal control objectives are achieved. This standard requires supervisors to continuously review and approve the assigned work of their staff as well as provide the necessary guidance and training to ensure that errors, waste, and wrongful acts are minimized and that specific management directives are followed.

8.9 COMMUNICATION AND OPERATIONS MANAGEMENT

System communications protection refers to the key elements used to assure data and systems are available, and exhibit the confidentiality and integrity expected by owners and users to conduct their business. The appropriate level of security applied to the information and systems is based on the classification and criticality of the information and the business processes that use it. The System's integrity controls must protect data against improper alteration or destruction during storage, during processing, and during transmission over electronic communication networks.

The key elements of system and communications protection are backup protection, denial of service protection, boundary protection, use of validated cryptography (encryption), public access protection, and protection from malicious code.

Operations management refers to implementing appropriate controls and protections on hardware, software, and resources; maintaining appropriate auditing and monitoring; and evaluating system threats and vulnerabilities.

Proper operations management safeguards all of the University's computing resources from loss or compromise, including main storage, storage media (e.g., tape, disk, and optical devices), communications software and hardware, processing equipment, standalone computers, and printers.

8.9.1 NETWORK SECURITY

Network attacks launched from the Internet or from University networks can cause significant damage and harm to information resources including the unauthorized disclosure of confidential information. In order to provide defensive measures against these attacks, firewall and network filtering technology must be used in a structured and consistent manner.

Michigan Tech maintains appropriate configuration standards and network security controls to safeguard information resources from internal and external network mediated threats. Firewalls and Intrusion Detection Systems (IDS) are deployed at the campus border and Intrusion Prevention Systems (IPS) are deployed on core services to augment normal system security measures to prevent denial of service attacks, malicious code, or other traffic that threatens systems within the network or that violates University information security policies. Firewalls and or IDS/IPS are also deployed as appropriate to limit access to systems that host restricted or essential information.

8.9.2 SECURITY MONITORING

Security Monitoring provides a means by which to confirm that information resource security controls are in place, are effective and are not being bypassed. One of the benefits of security monitoring is the early identification of wrongdoing or new security vulnerabilities. Early detection and monitoring can prevent possible attacks or minimize their impact on computer systems.

Any equipment attached to Michigan Tech's network is subject to security vulnerability scans. The goal of the scans is to reduce the vulnerability of University computers and the network to hacking, denial of service, infection, and other security risks from both inside and outside the University. ITS scans University servers using a mixture of commercial and open source software to monitor and assess the security of the University's network. Critical servers that store legally protected or other important non-public data are given priority, but others may be scanned.

ITS also coordinates the external vulnerability scans for departments that are required to use this service to meet the Payment Card Industry Data Security Standards (PCI DSS) for credit card processing. The external scans use a PCI approved external scan vendor.

8.9.3 ENCRYPTION

Michigan Tech has developed standards for encryption to ensure that sensitive data is protected from disclosure. Suitably strong encryption measures are employed and implemented, whenever deemed appropriate, for information during transmission and in storage.

Transmission

In order to protect the confidentiality and integrity of the University's sensitive data; any data classified as *Tier I* data, and having a required need for confidentiality and/or integrity, shall be transmitted via encrypted communication to ensure that it does not traverse the network in clear text. It is further recommended that data classified as *Tier II* be transmitted via encrypted communications when possible.

Storage

Encryption of information in storage presents risks to the availability of that information, due to the possibility of encryption key loss. In order to protect the confidentiality and integrity of the University's sensitive data; any data classified as *Tier I* data, and having a required need for confidentiality and/or integrity, shall be stored encrypted in systems and/or databases and/or portable media. *Tier II* or *Tier III* data classifications do not require such encrypted storage however is recommended. See the [Data Classification and Protection Policy](#) for further clarification on data classification and handling.

8.9.4 VIRUS PROTECTION

Viruses are a threat to the University as infected computers may transmit confidential information to unauthorized third parties, provide a platform for unauthorized access or use of the internal network, contaminate or infect other network connected devices, or interfere with University information technology resources. Antivirus software is provided to the University community to protect against the damage caused by virus attacks. Network administrators are responsible for creating procedures to ensure anti-virus software has the latest updates and virus signatures installed and also to verify that computers are virus-free.

The University reserves the right to review any device attached to the network (public or non-public) for adequate virus protection. The University reserves the right to deny access to the network to any device found to be inadequately protected. Additionally, the University reserves the right to disable network access to any device that is insufficiently protected, or currently infected with a virus. Network access may be restored when the device has been cleaned and current antivirus software and applicable operating system and application patches have been installed.

8.9.5 BACKUP AND RECOVERY

All electronic information is to be copied onto secure storage media on a regular basis (i.e., backed up), for the purpose of disaster recovery and business resumption. The [Backup and Recovery Standard](#) outlines the minimum requirements for the creation and retention of backups. Special backup needs which exceed these minimum requirements, may be accommodated on an individual basis.

All backups must conform to the following best practice procedures:

- All data and utility files must be adequately and systematically backed up. (Ensure this includes all patches, fixes and updates)
- Records of what is backed up and to where must be maintained
- Records of software licensing should be backed up

-
- The backup media must be precisely labeled and must have, at a minimum, the following identifying markers that can be readily displayed by labels and/or a bar-coding system:
 - System name
 - Creation date
 - Sensitivity Classification (Based on applicable electronic record retention regulations)
 - Copies of the back-up media, together with the back-up record, should be stored safely in a remote location, at a sufficient distance away to escape any damage from a disaster at the main site
 - Regular tests of restoring data/software from the backup copies should be undertaken, to ensure that they can be relied upon for use in an emergency. Note: For most important and time-critical data, a mirror system, or at least a mirror disk may be needed for a quick recovering.

8.10 SYSTEMS & APPLICATION SECURITY

Application development procedures are vital to the integrity of systems. If applications are not developed properly, data may be processed in such a way that the integrity of the data is corrupted. In addition, the integrity of the application software itself should be maintained, both in term of change control and terms of attack from malicious software.

8.10.1 SYSTEMS DEVELOPMENT AND MAINTENANCE

Security has to be considered at all stages of the life cycle of an information system in order to: a) ensure conformance with all appropriate security requirements, b) protect sensitive information throughout its life cycle, c) facilitate efficient implementation of security controls, d) prevent the introduction of new risks when the system is modified, and e) ensure proper removal of data when the system is retired.

In order to ensure that systems security is considered during the development and maintenance stages Michigan Tech has defined a [*Systems Development Lifecycle*](#) (SDLC) and the following minimum requirements during each phase:

- Feasibility Phase – high level review to ensure security requirements can support the business case
- Requirements Phase – define any initial security requirements or controls to support the business requirements
- Design Phase – verify appropriate security controls for the baseline have been identified and ensure change control is established and used for the remainder of the life cycle. Repeat verification with each design change or as warranted
- Development Phase – to verify and validate all security controls identified from design phase. Repeated throughout as changes are made or as warranted
- Implementation Phase – final verification of existing controls and the appropriate levels of risk mitigation

8.10.2 CHANGE CONTROL

Change Control is the process that management uses to identify, document and authorize changes to an IT environment. It minimizes the likelihood of disruptions, unauthorized alterations and errors.

The change control procedures are designed with the size and complexity of the environment in mind. For example, applications that are complex, maintained by a large IT staff or represent high risks require more formalized and more extensive processes than simple applications maintained by a single IT person. In all cases there should be clear identification of who is responsible for the change control process.

Michigan Tech is currently in the process of developing a University-wide change management process however the following elements will be included:

- Change Request Initiation and Control - Requests for changes are to be standardized and subject to management review. Changes are categorized and prioritized and specific procedures are in place to handle urgent matters. Change requestors should be kept informed about the status of their request.
- Impact Assessment - A procedure is in place to ensure that all requests for change are assessed in a structured way for all possible impacts on the operational system and its functionality.
- Control and Documentation of Changes - Changes to production systems are made only by authorized individuals in a controlled manner. Where possible a process for rolling back to the previous version should be identified. It is also important to document what changes have been made. At a minimum a change log should be maintained that includes:
 - A brief functional description of the change
 - Date the change was implemented
 - Who made the change
 - Who authorized the change (if multiple people can authorize changes)
 - What technical elements were affected by the change e.g., program modules, database tables or fields, screens and forms
- Documentation and Procedures - The change process includes provisions that whenever system changes are implemented, the associated documentation and procedures are updated accordingly.
- Authorized Maintenance - Staff maintaining systems are to have specific assignments and their work monitored as required. In addition, their system access rights should be controlled to avoid risks of unauthorized access to production environments.
- Testing and User Signoff - Software is thoroughly tested, not only for the change itself but also for impact on elements not modified. A standard suite of tests should be developed as well as a separate test environment. The standard test suite will help identify if core elements of an application were inadvertently

affected. Data owners of the systems should be responsible for signing off and approving changes being made.

- Testing Environment - Ideally systems should have at least three separate environments for development, testing and production. The test and production environments should be as similar as possible, with the possible exception of size. If cost prohibits having three environments, testing and development may take place in the same environment; but development activity needs to be closely managed (stopped) during acceptance testing. In no case should untested code or development be in a production environment.
- Version Control - Control is placed on production source code to ensure that only the latest version is being updated. If not, previous changes may be inadvertently lost when a new change is moved into production. Version control may also help in being able to effectively back out of a change that has unintended side effects.
- Emergency Changes - Emergency situations may occur that requires some of the program change controls to be overridden such as granting programmers access to production. However, at least a verbal authorization should be obtained and the change should be documented as soon as possible.
- Distribution of Software - As a change is implemented, it is important that all components of the change are installed in the correct locations and in a timely manner.
- Hardware and System Software Changes - Changes to hardware and system software should also be tested and authorized before being applied to the production environment. They should also be documented in the change log.

If a vendor supplies patches, they should be reviewed and assessed for applicability and potential impact to determine whether their fixes are required by the system.

8.11 PHYSICAL SECURITY MEASURES

Physical security controls and secure areas are used to minimize unauthorized access, damage, and interference to information and information systems. Physical Security means providing environmental safeguards for controlling physical access to equipment and data on the University network in order to protect information technology resources from unauthorized use, in terms of both physical hardware and data perspectives.

8.11.1 PHYSICAL ENTRY CONTROLS

Access to areas containing sensitive information must be physically restricted. Access to all entry points into and within the data center is protected by electronic access control mechanisms to validate access and ensure only authorized individuals enter the facility. An audit trail of all access is securely maintained for auditing purposes.

All individuals with access to these areas must wear an identification badge on their outer garments so that both the picture and information on the badge are clearly visible. Individuals are also encouraged to challenge unescorted strangers and anyone not wearing visible identification. Access rights to secure areas are regularly reviewed and updated.

8.11.2 PROVISIONING PROCESS

Individuals requesting access to the data center are to be enrolled in a structured and documented provisioning process for ensuring the integrity of the person entering the facility.

Personnel working within the data center or clients utilizing the facility services must be immediately removed from systems that have allowed access to the facility itself when no longer employed by the University. This includes all electronic access control mechanism along with removal of all systems, databases, Web portals, or any other type of sign-in mechanism that requires authentication and authorization activities.

8.11.3 VISITORS

Visitors must be properly identified with a current, valid form of identification and must be given a temporary facility badge allowing access to certain areas within the data center. A log of this activity is retained for audit and security purposes.

8.11.4 ALARMS & SURVEILLANCE

All exterior doors and sensitive areas within the facility are hard wired with alarms and have a mixture of security cameras in place throughout all critical areas, both inside and out, of the data center.

8.11.5 EQUIPMENT CONTROL

The assigned user of information technology resources is considered the custodian for the resource. If the item has been damaged, lost, stolen, borrowed, or is otherwise unavailable for normal business activities, the custodian must promptly inform the involved department manager. Sensitive information technology resources located in unsecured areas should be secured to prevent physical tampering, damage, theft, or unauthorized physical access.

An inventory of all computer equipment and media is maintained to account for restricted and confidential information. When feasible, IT equipment is to be marked with some form of identification that clearly indicates it is the property of Michigan Tech.

8.11.6 COMPUTER DATA AND MEDIA DISPOSAL POLICY

Proper data disposal is essential to controlling sensitive data including student records, personnel records, financial data, and protected health and credit card information. If the information on those systems is not properly removed before the equipment is disposed of, or transferred within the University, that information could be accessed and viewed by unauthorized individuals.

Media or devices containing sensitive information transferred between departments or removed from service must be properly sanitized, as outlined within the [Data Sanitization Standard](#) to ensure that all computers and electronic media are properly sanitized before disposal. Michigan Tech is committed to compliance with federal statutes associated with the protection of confidential information as well as ensuring compliance with software licensing agreements.

8.12 BUSINESS CONTINUITY

Michigan Tech provides a safe, secure IT environment to serve its customers' requirements, ensure stability and continuity of the business, and promote confidence in its ability to not only continuously provide goods and/or services, but also to recover quickly from disaster and minimize disruption.

8.12.1 BUSINESS IMPACT ANALYSIS

A Business Impact Analysis should correlate specific system components with the critical services that they provide, and based on that information, to characterize the consequences of a disruption to the system components. It is the responsibility of both the Data Owner and Data Custodian to perform appropriate business impact analysis tasks as outlined below.

Identify Critical IT Resources

Data owners and custodians are to evaluate his/her system to determine the critical functions performed and to identify the specific system resources required to perform them. Two activities usually are needed to complete this step:

1. Identify and coordinate with internal and external users associated with the system to characterize the ways that they depend on or support the system. When identifying contacts, it is important to include departments that provide or receive data from the system as well as contacts supporting any interconnected systems. This coordination should enable the data owner and custodian to characterize the full range of support provided by the system, including security, managerial, technical, and operational requirements.
2. Evaluate the system to link these critical services to system resources. This analysis usually will identify infrastructure requirements such as electric power, telecommunications connections, and environmental controls. Specific IT equipment, such as application servers, and authentication servers, are usually considered to be critical. However, the analysis may determine that certain IT components, such as a printer or print server, are not needed to support critical services.

Identify Outage Impacts and Allowable Outage Times

Data owners and custodians should analyze the critical resources identified in the previous step and determine the impact(s) on IT operations if a given resource were disrupted or damaged. The analysis should evaluate the impact of the outage in the following three ways:

1. The effects of the outage may be tracked over time. This will enable the University to identify the maximum allowable time that a resource may be unavailable before it prevents or inhibits the performance of an essential function.
2. The effects of the outage may be tracked across related resources and dependent systems, identifying any cascading effects that may occur as a disrupted system affects other processes that rely on it.
3. The effects of the outage may be tracked using revenue streams and cost expenditures, identifying any areas of monetary need or concern that could cause a delay in the recovery effort.

Data owners and custodians will determine the optimum point to recover the IT system by balancing the cost of system inoperability against the cost of resources required for restoring the system.

Develop Recovery Priorities

Data owners and custodians should develop recovery priorities for the system resources. A scale of high-, medium-, low should be used to prioritize the resources. High priorities are based on the need to restore critical resources within their allowable outage times; medium and low priorities reflect the requirement to restore full operational capabilities over a longer recovery period.

The outage impact(s) and allowable outage times characterized in the previous step enable the University to develop and prioritize recovery strategies that personnel will implement during contingency plan activation. For example, if the outage impacts step determines that the system must be recovered within 4 hours, Michigan Tech needs to adopt measures to meet that requirement. Similarly, if most system components could tolerate a 24-hour outage but a critical component could be unavailable for only 8 hours, the necessary resources for the critical component would be prioritized. By prioritizing these recovery strategies, the University may make more informed, tailored decisions regarding contingency resource allocations and expenditures, saving time, and effort .

Business Impact Analysis Documentation Requirements

Data owners and custodians are responsible for maintaining the Business Impact Analysis document(s). A periodic review of the Business Impact Analysis should be performed by the data owner to ensure accuracy and completeness.

8.12.2 DISASTER RECOVERY

A disaster recovery plan can be defined as the ongoing process of planning, developing and implementing disaster recovery management procedures and processes to ensure the efficient and effective resumption of critical functions in the event of an unscheduled interruption.

There are five main components of the disaster recovery plan. The Supporting Information and Plan Appendices provide essential information to ensure a comprehensive plan. The Notification/Activation, Recovery, and Reconstitution Phases address specific actions that University should take following a system disruption or emergency. IT contingency plans should be clear, concise, and easy to implement in an emergency. Where possible, checklists and step-by-step procedures should be used.

The Disaster Recovery Plan must contain detailed information on how to continue business operations and perform all tasks required to do so while the computer hardware, network and data are being recovered. Technical capabilities need to be documented and designed to support operations and should be tailored to the University requirements. The order in which systems are to be recovered and at what level of functionality based upon the BIA need to be fully documented. Not all systems may need to be recovered simultaneously or to 100% for the system to begin functioning.

Michigan Tech is in the process of developing a comprehensive contingency planning program. Each campus department will develop IT contingency plans that contain

detailed roles, responsibilities, teams, and procedures associated with restoring an IT system following a disruption.

8.13 INFORMATION SECURITY INCIDENT RESPONSE

An IT security incident is defined as an event that impacts or has the potential to impact the confidentiality, availability, or integrity of University information technology resources. Having an effective incident response is essential in mitigating damage and loss due to an information security incident. Proper handling of such incidents protects the University's information technology resources from future unauthorized access, use or damage.

If you suspect an IT security incident, immediate action should be taken to isolate the problem from the campus network. Be ready to provide specifics such as date/time of loss, type of device(s), contact information, and any specific information that you believe indicates that a device was breached, a computer security incident occurred or a device was lost or stolen. Please see the [IT Incident Response Procedure](#) for further reference.

9 REGULATIONS

The University must be proactively aware of and prepared to comply with a wide variety of federal and state laws, regulations, and University policies with respect to information protection and privacy. While this is not an exhausted list,

9.1 FAMILY EDUCATION RIGHTS AND PRIVACY ACT

FERPA deals with student "education records," defined to mean (with a few exceptions) records containing information directly related to a student that are maintained by the University. "Education records" is broadly defined and includes electronic records. FERPA prohibits schools from disclosing education records, or personally identifiable information in those records other than certain basic "directory information," without the student's prior written consent unless an exception applies.

9.2 HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT

HIPAA and its regulations (the "Privacy Rule" and the "Security Rule") protect the privacy of an individual's health information as well as govern the way Michigan Tech collects, maintains, uses and discloses protected health information ("PHI").

Michigan Tech must ensure the confidentiality, integrity and availability of confidential information; and detect and prevent reasonably anticipated errors and threats due to malicious or criminal actions, system failure, natural disasters and employee or user error. Such events could result in damage to or loss of personal information, corruption or loss of data integrity, interruption of University activities, or compromise to the privacy of the University employees and its records.

9.3 HEALTH INFORMATION TECHNOLOGY FOR ECONOMIC AND CLINICAL HEALTH ACT

HITECH imposes federal security breach notification requirements for unauthorized uses and disclosures of “unsecured PHI” and adds numerous privacy and data security restrictions to HIPAA.

9.4 INTERNATIONAL TRAFFIC IN ARMS REGULATIONS/EXPORT ADMINISTRATION REGULATIONS

ITAR and EAR are federal regulations that prohibit the unlicensed export of specific technologies for reasons of national security or protection of trade. If University research involves such specified technologies, regulations may require the University to obtain prior approval before allowing foreign nationals to participate in the research, partnering with a foreign company and/or sharing research—verbally or in writing—with persons who are not United States citizens or permanent resident aliens.

9.5 GRAMM-LEACH-BLILEY ACT FOR DISCLOSURE OF NONPUBLIC PERSONAL INFORMATION

GLBA mandates that the University safeguard nonpublic personally identifiable financial information (PIFI); limit disclosures of such data, and notify customers of their information sharing practices and privacy policies. The act states, among other things, that the University must develop, implement and maintain a written comprehensive information security program that contains administrative, technical, and physical safeguards appropriate to its size and complexity, the nature and scope of its activities, and the sensitivity of the relevant customer data. The plan must be “reasonably designed” to achieve the security and confidentiality of customer data, to protect against anticipated threats or hazards, and to protect against unauthorized access or use that could result in substantial harm.

9.6 RED FLAG RULES

The RFR requires that the University implement a written Identity Theft Prevention Program designed to detect the warning signs — or “red flags” — of identity theft in their day-to-day operations. By identifying red flags in advance, businesses will be better equipped to spot suspicious patterns that may arise -- and take steps to prevent a red flag from escalating into a costly episode of identity theft.

9.7 PAYMENT CARD INDUSTRY DATA SECURITY STANDARDS

PCI DSS provides a single approach to safeguarding confidential credit card account data and establishes security best practice standards that the University must follow when storing, processing, or transmitting credit card data. While not a law, the University must comply in order to be approved and continue to accept payment cards.

10 COMPLIANCE

Upon implementation of this plan, ITS will ensure that the plan is being effectively carried out in accordance with regulatory and University requirements and meets or exceeds industry standards for information security.

11 RELATED POLICIES & PROCEDURES

[Information Security Compliance Policy](#)

[Acceptable Use of Information Technology Resources](#)

[Confidentiality Agreement](#)

[Information Security Roles & Responsibilities](#)

[Data Classification & Protection Standard](#)

[Identity and Access Management](#)

[Password Standards](#)

[Backup & Recovery Standard](#)

[Data Sanitization Standard](#)

[Retention Policy](#)

[System Development Life Cycle](#)

[IT Incident Response Procedure](#)

Change Management Policy - Under Development

Disaster Recovery & Business Continuity - Under Development

12 ISP - REVISION HISTORY

Revision	Date	Description of changes	Requested By
Rev 2	2/7/11	Final Version	AS
Rev 3	10/13/11	Updated to reflect new Acceptable Use of Information Technology Resources	AS
Rev 4	9/12	Updated to reflect new policies and procedures	AS

END OF DOCUMENT