



MOTLOW STATE

INFORMATION SECURITY PLAN

Motlow State Community College

Information Security Plan



MOTLOW STATE
COMMUNITY COLLEGE



Table of Contents

PURPOSE	3
SCOPE.....	3
DEFINITIONS	3-4
MANAGEMENT COMMITMENT	4-5
DEPARTMENTAL RESPONSIBILITY	6-7
ASSESSING SECURITY RISKS.....	7-8
INFORMATION SYSTEMS UPDATES.....	8
COMPUTER SECURITY PRACTICES.....	8
NETWORK SECURITY	9
SECURITY MONITORING	9-10
INFORMATION CLASSIFICATION	10
TIER 1: CONFIDENTIAL	11
TIER 2: INTERNAL/ PRIVATE	11
TIER 3: PUBLIC	11
INFORMATION SECURITY INCIDENT RESPONSE	11-12
INFORMATION DISSEMINATION.....	12
VENDOR MANAGEMENT	12
COMPLIANCE	12
APPROVAL.....	13



PURPOSE

This plan outlines the College's commitment to protect confidentiality, integrity and availability of information and the reputation of the organization.

This plan reflects Motlow State Community College's (Motlow) 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 Motlow constituents, safeguarding vital business information, and fulfilling TBR policies, guidelines and state laws.

SCOPE

This plan applies to the entire Motlow State community, including students, faculty, staff, alumni, temporary workers, contractors, volunteers and guests who have access to Motlow information and technologies. Such assets include but are not limited to computers, data, images, text, or software, whether stored on hardware, paper or other storage media.

DEFINITIONS

Confidentiality-“Ensuring that information is accessible only to those authorized to have access.”

Integrity-“Safeguarding the accuracy and completeness of information and processing methods.”

Risk-“The likelihood of a threat taking advantage of vulnerability and the resulting business impact.”

Risk Assessment-“The process of risk analysis and risk evaluation by comparing the estimated risk against a given risk criteria to determine the significance of the risk.”

Information Security-“ Refers to the processes and methodologies which are designed and implemented to protect print, electronic, or any other form of confidential, private and sensitive information or data from unauthorized access, use, misuse, disclosure, destruction, modification, or disruption.”

Vulnerability-“A weakness of an asset or group of assets that can be exploited by one or more



Threat-“Potential cause of an unwanted incident, which may result in harm or loss to

Network Security-“Is the process of taking physical and software preventative measures to protect the underlying networking infrastructure from unauthorized access, misuse, malfunction, modification, destruction, or improper disclosure, thereby creating a secure platform for computers, users and programs to perform their permitted critical functions within a secure environment.”

Computer Security-“Is concerned with the risks related to computer use, and ensures the availability, integrity and confidentiality of information managed by the computer system, permitting authorized users to carry out legitimate and useful tasks within a secure computing environment.”

Control-“Means of managing risks, including policies, procedures, guidelines, practices or organizational structures which can be of administrative, technical, management or legal in nature.”

Data Custodians-“Data Custodians are institutional designees who have planning and policy making responsibilities for institutional data and the institutional Data Warehouse. The Data Custodians, as a group, are responsible for overseeing the establishment of data management policies and procedures and for the assignment of data management accountability. Data Custodians are responsible for the oversight of Personally Identifiable Information (PII) in their respective areas of institutional operations.

Personally Identifiable Information (PII)-“Information which can be used to distinguish or trace an individual’s identity, such as their name, Social Security number, or biometric records, alone, or when combined with other personal or identifying information which is linked or linkable to specific individual, such as date and place of birth, mother’s maiden name, etc.”

Access Control- “Refers to the process of controlling access to systems, networks and information based on business and security requirements.”

Dissemination- “The approved and authorized processes where classification information can be shared.”

Timely Manner-“Is subjective and relative to the decisions made by the department heads based on need, time and urgency. *Timely Manner* may not be quantifiable in all instances and is up to each department head to determine the requirements needed to fulfill a timely update.”

Reasonable Amount of Time: “The amount to time that is reasonable under the particular circumstances, but shall not under any circumstances exceed five (5) working days.”

MANAGEMENT COMMITMENT

Motlow College considers information to be a strategic asset that is essential to its core mission and business operations. Furthermore, Motlow values the privacy of individuals and is dedicated to protecting the information with which it is entrusted. Therefore, Motlow is committed to providing the resources



INFORMATION SECURITY PLAN

needed to ensure confidentiality, integrity, and availability of its information as well as reduce the risk of exposure that would damage the reputation of the college. The Information Security Plan shall be established that supports the following core security values:

Support Motlow mission. The Plan is designed to support the missions of Motlow, notably the creation and dissemination of new knowledge, by protecting Motlow resources, reputation, legal position, and ability to conduct its operations. It is intended to facilitate activities that are important to the college.

Consistent with institutional policies, contracts, and laws. The Plan is consistent with and serves to enforce relevant Motlow policies, guidelines, contracts and license agreements governing software, copyrighted files, and other forms of intellectual property; and laws and policies governing student, employee, other sensitive information, and records retention laws and policies. See: [Motlow Policy: Information Technology Resources \(1:08:00:00\)](#)

Appropriate and cost-effective. Not all Motlow resources require the same level of protection. Plan requirements are formulated with the objective that the application of measures be commensurate with the sensitivity and value of resources and the actual threats to those resources. The intent is not to dictate requirements whose implementation would impose unnecessary costs.

Shared responsibility. All members of the Motlow community share in the responsibility for protecting Motlow resources for which they have access or custodianship. The Plan recognizes that people will need adequate information, training, and tools to exercise their responsibilities and that these responsibilities must be made explicit.

Accountability. The Plan intends that members of the Motlow community be accountable for their access to and use of Motlow resources. **See: Information Technology Department Policies and Procedures Manual, and [Motlow Policy: Information Technology Resources \(1:08:00:00\)](#).**

Flexible and adaptable. The goal is that members of the Motlow community be able to exercise their discretion and best judgment when determining how to protect resources for which they have responsibilities, subject to legal and other obligations and policies from TBR and Motlow. Where procedures and practices are required, they are meant to be flexible enough to change as circumstances change.

Emergency preparedness. It is not possible to prevent all incidents affecting information technology. The Plan is designed to outline appropriate measures and prepare for possible incidents, including implementation of business continuity measures to protect critical information, and data.

Reassessment. The Plan recognizes that revisions may be required and that reassessment of the Information Security Plan and the Operations Standards and Procedures Manual may be necessary. At a minimum, this plan will be evaluated annually to determine its effectiveness. **See: Information Technology Department Policies and Procedures Manual**



DEPARTMENTAL RESPONSIBILITY

In order to promote the data security of the college, Motlow will oversee risk management and compliance programs pertaining to information security such as the Health Insurance Portability and Accountability Act, Family Educational Rights and Privacy Act, the Open Records Act of Tennessee, Gramm-Leach-Bliley, Red Flag Rules and PCI. Motlow will:

- Approve and adopt broad information security program principles and approve assignment of key managers responsible for information security.
- Strive to protect the interests of all stakeholders dependent on information security.
- Review information security policies, procedures and guidelines.
- Strive to ensure business continuity.
- Review provisions for internal and external audits of the information security program.

Each department will protect Motlow by adopting and implementing, at a minimum, these security standards and procedures defined by this document. Officials responsible for each of the following areas will be considered data custodians. Departments are encouraged to adopt standards that exceed the minimum requirements for the protection of Motlow resources that are controlled exclusively within the Department.

See: [TBR Policy: Personally Identifiable Information \(PII\)](#)

Individuals within the scope of this guideline are responsible for complying with this plan and the Department's policy, if one exists, to ensure the security of College's resources. Each department is responsible for ensuring all employees are trained on the policies, guidelines and procedures relevant to their department.

ASSESSING SECURITY RISKS

Risk assessments should identify, quantify, and prioritize risk against criteria for risk acceptance and objectives relevant to the organization. The results should guide and determine the appropriate management action and priorities for managing information security risks and for implementing controls selected to protect against, physical security, network security and high-risk areas.

The process of assessing risks and selecting controls may need to be performed a number of times to cover different parts of the organization or individual information systems. Each Motlow department will be responsible for implementing security risk guidelines or procedures. Assessments may include:

- Natural threats: May include, floods, earthquakes, tornadoes.
- Human threats: Are enabled or caused by humans and may be intentional (unauthorized access to data or offices) or unintentional (e.g., inadvertent data entry or inaccurate data.)



- Environmental threats: Power failures, chemicals, pollution, liquid leakage.
- Identification and authentication mechanisms. (e.g., outside guests or vendors.)
- Reviewing government laws and regulations pertaining to minimum security control requirements.
- Reviewing documented or informal policies, procedures and guidelines.

INFORMATION SYSTEMS UPDATES

Motlow is committed to maintaining appropriate and timely updates, patches and maintenance to ensure that systems and data are adequately protected. Critical updates/fixes should be applied as soon as is possible in accordance with institutional approval and sign-off procedures. **See: [TBR Policy: Enterprise Information System Updates](#).**

Enterprise Information Systems Covered By This Policy:

- ERP Quarterly Updates should be installed in their entirety and in a timely manner. The institution should not be more than one version behind the current release.
- Oracle CPU Updates should be installed in a timely manner and the institution should not be more than one version behind the current release.
- External application and system hosting will conform to institutional requirements with written exceptions being made as necessary based on the abilities and contractual obligations between the institution and the hosting vendor.
- Operating System (OS) updates for servers, workstations, and other end user equipment should be installed in a timely manner in accordance to institutional needs and requirements in order to minimize and avoid unduly exposing the institution to risks.
- End-user applications regular and critical updates should be installed in a timely manner in accordance to institutional needs and requirements in order to minimize and avoid unduly exposing the institution to risks.
- Network infrastructure and systems regular and critical updates should be installed in a timely manner in accordance with institutional needs and requirements in order to minimize and avoid unduly exposing the institution to risks.
- All other enterprise information systems and components regular and critical updates should be installed in a timely manner in accordance to institutional needs and requirements, and to minimize and avoid unduly exposing the institution



COMPUTER SECURITY PRACTICES

Following security best practices helps to decrease the risk of an information security breaches. It is the responsibility of each member of the college community to follow the basic computer safety guidelines listed in this document. Motlow's goal is to help maintain a secure computing and network environment. Best practices are a general guideline based on industry standards for information security. All employees should familiarize themselves with the following guidelines:

- Use cryptic passwords that can't be easily guessed and protect the passwords. **See: [TBR Policy: Access Control](#).**
- Beware of scams.
- Protect information when using the internet and email.
- Secure your area before leaving it unattended.
- Secure laptops and mobile devices at all times.
- Secure memory sticks
- Lock or log off computers or other devices before leaving them unattended and make sure they require a passwords to start up or wake-up.
- Make sure there is adequate anti-virus software and that patches and updates are current
- Protect portable and mobile devices.
- Don't install or download unknown or unsolicited programs to Motlow computers.
- File cabinets containing Restricted or Sensitive information must be kept closed and locked when not in use or when not attended.
- Passwords may not be left on sticky notes posted on or under a computer, nor may they be left written down in an accessible location.
- Printouts containing private or confidential information should be immediately removed from the printer.
- Upon disposal Restricted and/or Sensitive documents should be shredded in the official shredder bins or placed in the lock confidential disposal bins.
- Whiteboards containing Restricted and/or Sensitive information should be erased.

NETWORK SECURITY

Network attacks launched from the Internet or from College 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.

Motlow State maintains appropriate configuration standards and network security controls to safeguard information resources from internal and external network threats. Firewalls and Intrusion Prevention Systems (IPS) are deployed at the campus to prevent denial of service attacks, malicious code, or other



traffic that threatens systems within the network.

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 Motlow's network is subject to security vulnerability scans. The goal of the scans is to reduce the vulnerability of Motlow's computers and the network to hacking, denial of service, infection, and other security risks from both inside and outside the college.

Technical Operations scans Motlow servers using a mixture of commercial and open source software to monitor and assess the security of the network.

Technical Operations also coordinates the 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. Suitably strong encryption measures are employed and implemented, whenever deemed appropriate, for information during transmission and in storage.

Security monitoring also includes video surveillance and card key identification systems controlled and monitored by the Network and Security Manager. The Network and Security Manager will oversee the physical security standards, procedures and guidelines for Motlow.

INFORMATION CLASSIFICATION

Information Classification is required to determine the relative sensitivity and criticality of information assets, which provide the basis for protection efforts and access control. Information Classification establishes a baseline derived from federal laws, state laws, regulations, and College policies that govern the privacy and confidentiality of data.

Information Classification applies to all data (e.g., student, financial, academic, and employee data collected in electronic or hard copy form that is generated, maintained, and entrusted to Motlow State) except where a different standard is required by grant, contract, or law.

All institutional data must be classified into one of three sensitivity levels or classifications that Motlow 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 College data is to be reviewed on a periodic basis and classified according to its use, sensitivity and importance to the College and in compliance with federal and/or state laws.



TIER 1: CONFIDENTIAL

Confidential information is information whose unauthorized disclosure, compromise or destruction would result in severe damage to the College, its students, or employees (e.g., social security numbers, dates of birth, medical records, credit card or bank account information). Tier 1 data is intended solely for use within Motlow State and is limited to those with a “business need-to-know.”

TIER 2: 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 Motlow’s reputation, or violate an individual’s privacy rights (e.g., educational student records, employment history, and alumni biographical information). Internal use information is information intended for use by College employees, contractors, and vendors covered by a non-disclosure agreement.

TIER 3: PUBLIC

This is information that is not publicly disseminated, but accessible 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 this information does not expose Motlow to financial or reputational loss, or jeopardize the security of Motlow assets. 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.

INFORMATION SECURITY INCIDENT RESPONSE

A Security Incident is an actual or suspected violation of computer security policies, acceptable use policies, or standard computer security practices. An "IT security incident" could:

- Result in misuse of confidential information (social security number, grades, health records, financial transactions, etc.) of an individual(s).
- Jeopardize the functionality of the college’s IT infrastructure.
- Provide unauthorized access to college resources or information.



INFORMATION SECURITY PLAN

When such an incident occurs, Motlow State has a plan for dealing with (i.e., reporting, investigating, and resolving) the incident. This plan helps ensure the safety, confidentiality, availability, and integrity of Motlow information.

If a user of the Motlow State community suspects that college assets are being misused or are under attack, that user has an obligation to report that incident, in a reasonable amount of time, to the Technical Operations Department. If you suspect an IT security incident, immediate action should be taken to isolate the problem from the campus network.

1. Call the Director of Technical Operations and the Chief Information Officer (CIO).
2. Send an email regarding the incident to the Director of Technical Operations and the CIO.

INFORMATION DISSEMINATION

The dissemination of classified information will go through Vice President of the department in which the breach of confidential information occurs. The Vice President of Finance and Administration or designee will notify the Tennessee Board of Regents, if needed, to determine how breach of classified or private information will be handled.

VENDOR MANAGEMENT

Ensure the existence of a vendor management program that makes certain each vendor delivers its goods and services in a manner where key information to the college remains secured and is not disclosed inappropriately.

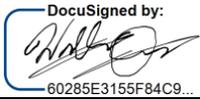
COMPLIANCE

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

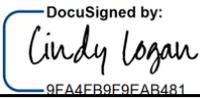


INFORMATION SECURITY PLAN

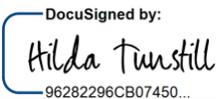
Approval

By:  60285E3155F84C9...
William Quinn, Network Systems and Security Manger

Date: 3/10/2021

By:  9FA4FB9F9FAB481
Cindy Logan, Chief Information Officer

Date: 3/10/2021

By:  96282296CB07450...
Hilda Tunstill, Executive Vice President of Business and Finance

Date: 3/10/2021

By:  CF16EC71E891469...
Dr. Michael Torrence, President

Date: 3/12/2021