PURPOSE

The purpose of this policy is to outline the duties and responsibilities of all individuals tasked with reporting, investigating, and resolving information security incidents.

APPLICABILITY

This policy applies to all MCC employees, whether full-time or part-time, including faculty, administrative staff, contract or temporary workers, consultants, interns, and student employees. This policy also applies to certain contracted third-party vendors.

DEFINITIONS

“Information Security Incident” is defined as an event which results in accidental or deliberate unauthorized access, loss, disclosure, modification, disruption, or destruction of technology resources.

"Information Security Breach" means unauthorized access to and unauthorized acquisition of personal information maintained in computerized form by a person that compromises the security, confidentiality, or integrity of the personal information. Good faith acquisition of personal information by a person or that person's employee or agent for a legitimate purpose of that person is not a breach of security, provided that the personal information is not used in violation of applicable law or in a manner that harms or poses an actual threat to the security, confidentiality, or integrity of the personal information. Security breaches are a type of information security incident.

“Data Owner” is the manager or agent responsible for the business function supported by the information resource or the individual upon whom responsibility rests for carrying out the program using the information resource.

“Data Custodian” is an employee who is responsible for the day to day maintenance of information resources. In certain instances, the responsibility may be assigned to a third party vendor.

“Information Resource” are the procedures, equipment, facilities, software, and data that are designed, built, operated, and maintained to create, collect, record, process, store, retrieve, display, and transmit information.

"Person" means any individual, corporation, business trust, estate, trust, partnership, limited liability company, association, joint venture, government, governmental subdivision, governmental agency, govern-mental instrumentality, public corporation, or any other legal or commercial entity.

"Owns or licenses" includes, but is not limited to, personal information that a business retains as part of the internal customer account of the business or for the purpose of using the information in transactions with the person to whom the information relates.

"Consumer" means an individual who is a resident of this state.

CYBERSECURITY INCIDENT RESPONSE PLAN

MCC will develop, maintain, and update a Cybersecurity Incident Response Plan ("CIRP"). The responsible party for the CIRP is Chief Information Security Officer (CISO) or designee. The CIRP shall include the requirements listed within this policy. To the extent that the CIRP conflicts with this policy, this policy shall control.

The CIRP is intended to provide organizational structure, operational structure, processes, and procedures to MCC personnel, responding to incidents that may affect the function and security of IT assets, information resources, and business operations.

INFORMATION SECURITY INCIDENT REPORTING

Data Owners and Data Custodians who believe any possible or actual unauthorized access to or disclosure, misuse, alteration, destruction, or other compromise of Personal Information, or a violation or attempted violation of information safeguards has occurred, shall immediately report the relevant information to the CISO.

Any attempt to interfere with, prevent, obstruct, retaliate for or dissuade the reporting of an information security incident, critical security concern, policy violation or information resource vulnerability is strictly prohibited and may be cause for disciplinary action.

MCCPD will be notified for information security incidents involving criminal activity.

INVESTIGATION

Upon notification of information regarding a potential security incident, the CISO shall promptly conduct an investigation to determine the impacted data, systems, and business processes. Data Owners and Data Custodians are expected to cooperate fully with the investigation and provide access to all relevant records. The CISO shall confirm whether a security incident occurred, assess the risks involved, and determine a mitigation strategy.

In the event of a breach of Personal Information, MCC will take immediate action to secure any Personal Information that has or may have been compromised; preserve and review files or programs that may indicate how the breach occurred; and if appropriate, retain professionals to assess the breach.

RESPONSE TEAM

The CISO will notify an incidence response team of the findings.

The incidence response team shall: 1) Take action to limit the magnitude and scope of the information security incident; 2) Conduct post security incident review and make recommendations to mitigate or eliminate risks resulting from incident; and 3) Draft a report summarizing the information security incident and recommended actions. The Data Owner is responsible for ensuring that new risk mitigation measures are implemented and monitored.

INFORMATION SECURITY INCIDENT NOTIFICATION

Any person that owns or licenses personal information of residents of Missouri or any person that conducts business in Missouri that owns or licenses personal information in any form of a resident of Missouri shall provide notice to the affected consumer that there has been a breach of security following discovery or notification of the breach. The disclosure notification shall be:

TO MISSOURI RESIDENTS

1. Made without unreasonable delay;

2. Consistent with the legitimate needs of law enforcement; and

3. Consistent with any measures necessary to determine sufficient contact information and to determine the scope of the breach and restore the reasonable integrity, security, and confidentiality of the data system.

TO OWNER OR LICENSE HOLDER-MISSOURI RESIDENTS

Any person that maintains or possesses records or data containing personal information of residents of Missouri that the person does not own or license, or any person that conducts business in Missouri that maintains or possesses records or data containing personal information of a resident of Missouri that the person does not own or license, shall notify the owner or licensee of the information of any breach of security immediately following discovery of the breach, consistent with the legitimate needs of law enforcement.

DISCLOSURE NOTIFICATION-MISSOURI RESIDENTS

The notice shall at minimum include a description of the following:

1. The incident in general terms;

2. The type of personal information that was obtained as a result of the breach of security;

3. A telephone number that the affected consumer may call for further information and assistance, if one exists;

4. Contact information for consumer reporting agencies;

5. Advice that directs the affected consumer to remain vigilant by reviewing account statements and monitoring free credit reports.

DISCLOSURE NOTIFICATION-ALL OTHERS

MCC shall provide notifications in accordance with applicable state and federal laws, methods, and timelines. The notification will include a brief description of the information security incident, a contact for inquiries, and helpful reference regarding identity theft and fraud. Notice shall be delivered by one of the following methods:

1. Written notice;

2. Electronic mail;

3. Conspicuous posting on MCC's website; or

4. Publication through broadcast media.

CRIMINAL INVESTIGATION EXCEPTION	The notice required may be delayed if a law enforcement agency informs the person that notification may impede a criminal investigation or jeopardize national or homeland security, provided that such request by law enforcement is made in writing or the person documents such request contemporaneously in writing, including the name of the law enforcement officer making the request and the officer's law enforcement agency engaged in the investigation. The notice shall be provided without unreasonable delay after the law enforcement agency communicates to the person its determination that notice will no longer impede the investigation or jeopardize national or homeland security.
CONSUMER REPORTING AGENCY	In the event a person provides notice to more than one thousand consumers at one time, the person shall notify, without unreasonable delay, the attorney general's office and all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, of the timing, distribution, and content of the notice.
COMMUNICATION	External inquiries from members of the public or media shall be routed through the College and Community Relations Department. Only authorized personnel are permitted to speak on behalf of MCC regarding security incidents.
ENFORCEMENT	Compliance with this policy shall be strictly enforced. Violations may result in disciplinary action, up to and including termination.