Information Security Plan

This Information Security Plan ("Plan") describes MCAD's safeguards to protect *covered data and information.*[1] These safeguards are provided to:

- Ensure the security and confidentiality of covered data and information;
- Protect against anticipated threats or hazards to the security or integrity of such information; and
- Protect against unauthorized access to or use of covered data and information that could result in substantial harm or inconvenience to any customer.

This Information Security Plan also provides for mechanisms to:

- Identify and assess the risks that may threaten covered data and information maintained by MCAD;
- Develop written policies and procedures to manage and control those risks;
- Implement and review the plan; and
- Adjust the plan to reflect changes in technology, the sensitivity of covered data and information, and internal or external threats to information security.

Identification and Assessment of Risks to Customer Information

MCAD recognizes that it has both internal and external risks. These risks include, but are not limited to:

- Unauthorized access of covered data and information by someone other than the owner of the covered data and information
- Compromised system security as a result of system access by an unauthorized person
- Interception of data during transmission
- Loss of data integrity
- Physical loss of data in a disaster
- Errors introduced into the system
- Corruption of data or systems
- Unauthorized access of covered data and information by employees
- Unauthorized requests for covered data and information
- Unauthorized access through hard copy files or reports
- Unauthorized transfer of covered data and information through third parties

[1] *Covered data and information* for the purpose of this policy includes *student financial information* (defined below) required to be protected under the Gramm Leach Bliley Act (GLBA). In addition to this coverage, which is required under federal law, MCAD chooses, as a matter of policy, to also include in this definition any credit card information received in the course of business by MCAD, whether or not such credit card information is covered by the GLBA. Covered data and information includes both paper and electronic records.
Student financial information is that information that MCAD has obtained from a customer in the process of offering a financial product or service, or such information provided to MCAD by another financial institution. Offering a financial product or service includes offering student loans to students, receiving income tax information from a student's parent when offering a financial aid package, and other miscellaneous financial services. Examples of student financial information include addresses, phone numbers, and credit card account numbers, income and credit histories and Social Security Numbers, in both paper and electronic format.

MCAD recognizes that this may not be a complete list of the risks associated with the protection of covered data and information. Since technology growth is not static, new risks are created regularly. Accordingly, the Technology Department ("IT") will actively participate and monitor advisory groups, such as Educause Security Institute, the Internet2 Security Working Group, and SANS for identification of new electronic risks.

MCAD believes its current safeguards are reasonable and, in light of IT's current risk assessments, are sufficient to provide security and confidentiality to covered data and information maintained by MCAD. Additionally, these safeguards protect against currently anticipated threats or hazards to the integrity of such information.

Information Security Plan Coordinators

The Vice President of Administration and Associate Vice President of Technology have been appointed as the Coordinators of this Plan. They are responsible for assessing the risks associated with unauthorized transfers of covered data and information and implementing procedures to minimize those risks to MCAD. MCAD personnel will also conduct reviews of areas that have access to covered data and information to assess the internal control structure put in place by the administration and to verify that MCAD departments comply with the requirements of this Plan.

Design and Implementation of Safeguards Program

Employee Management and Training

References of new employees working in areas who regularly work with covered data and information (i.e., Business Office, Continuing Education, Human Resources, IT, Registrar, Institutional Advancement, and Financial Aid) are checked. During employee orientation, each new employee in these departments will receive proper training on the importance of confidentiality of student records, student financial information, and other types of covered data and information. Each new employee is also trained in the proper use of computer information and passwords. Training also includes controls and procedures to prevent employees from providing confidential information to an unauthorized individual, including "pretext calling"[2] and how to properly dispose of documents that contain covered data and information. Each department responsible for maintaining covered data and information is instructed to take steps to protect the information from destruction; loss or damage due to environmental hazards, such as fire and water damage; or technical failures. The Associate Vice President of Technology and the Vice President of Administration will review and develop training for all employees who have access to covered data. These training efforts should help minimize risk and safeguard covered data and information security.

Physical Security

MCAD has addressed the physical security of covered data and information by limiting access to only those employees who have a business reason to know such information. For example, personal

[2] "Pretext calling" occurs when an individual improperly obtains personal information of college customers so as to be able to commit identity theft. It is accomplished by contacting MCAD, posing as a customer or someone authorized to have the customer's information and, through the use of trickery and deceit, convincing an employee of MCAD to release customer identifying information.

customer information, accounts, balances, and transactional information are available only to MCAD employees with an appropriate business need for such information.

Loan files, account information, and other paper documents are kept in file cabinets or rooms that are locked each night. Only authorized employees know combinations and the location of keys. Paper documents that contain covered data and information are shredded at the time of disposal.

"Procedures for Information Security" contains documented procedures for maintaining physical security of customer financial information.

Access to covered data and information via MCAD's computer information system is limited to those employees who have a business reason to know such information. Each employee is assigned a user name and password. Databases containing personal covered data and information, including, but not limited to, accounts, balances, and transactional information, are available only to MCAD employees in appropriate departments and positions.

MCAD will take reasonable and appropriate steps consistent with current technological developments to make sure that all covered data and information is secure and to safeguard the integrity of records in storage and transmission. MCAD maintains a secure procedure for creation and maintenance of passwords. User and system passwords are also required to comply with the MCAD Password Policy.

A variety of intrusion detection systems are being implemented and tested to detect and stop certain external threats. An Incident Response Policy for occasions where intrusions or breaches occur is also being developed.

When commercially reasonable, encryption technology will be utilized for both storage and transmission. All covered data and information are maintained on servers that are behind MCAD's firewall. All firewall software and hardware maintained by IT will be kept current. IT has a number of policies and procedures in place to provide security to MCAD's information systems. These policies are available upon request from MCAD's Director of IT.

MCAD does not use Social Security Numbers as an identifier for students or employees. However, Social Security Numbers are provided to MCAD in connection with payroll reporting and financial aid, so, out of necessity, MCAD retains some Social Security Numbers.

<u>Management of System Failures</u>
IT is in the process of developing written plans and procedures to detect any actual or attempted attacks on MCAD systems and will prepare an Incident Response Policy that outlines procedures for responding to actual or attempted unauthorized access to covered data and information.

Selection of Appropriate Service Providers

Due to the specialized expertise needed to design, implement, and service new technologies, vendors may be needed to provide resources that MCAD determines not to provide on its own. In the process of choosing a service provider that will maintain or regularly access covered data and information, the evaluation process shall include the ability of the service provider to safeguard confidential financial information. MCAD will review its relationships with such service providers and confirm that such service providers have initiated privacy and security safeguards.

Continuing Evaluation and Adjustment

This Information Security Plan will be subject to periodic review and adjustment. Technology reviews will occur within IT, where constantly changing technology and evolving risks mandate increased vigilance. Continued administration of the development, implementation, and maintenance of the program will be the responsibility of the designated Information Security Plan Coordinators. The Coordinators will review the standards set forth in this policy and recommend updates and revisions as necessary. It may be necessary to adjust the plan to reflect changes in technology, the sensitivity of student/customer data, and internal or external threats to information security.

Procedures for Information Security

General College Compliance Procedures

The College instructs employees to take basic steps to maintain the security, confidentiality, and integrity of student financial information, such as:

- Locking rooms and file cabinets where paper records are kept;
- Using password-activated screensavers;
- Using individual passwords for computer access;
- Referring calls or other requests for customer information to designated individuals who have authority to release such information;
- Regularly reminding employees of MCAD's policy and the legal requirement to keep customer information secure and confidential;
- Recognizing any fraudulent attempt to obtain customer information and reporting it to the proper administrator, who will, in turn, report it to the proper authorities as necessary.

The following departments have considerable access to student and/or employee information. Safeguards to ensure the security and confidentiality of customer information within these departments are outlined below.

Business Office

The Business Office is protected by a security alarm. The door to the Business Office is locked at all times and entry is gained through card access. The front door and payment window of the Business Office are monitored at all times by Public Safety staff by way of security cameras. All monies entrusted to the Business Office are maintained in a locked fireproof safe whenever Business Office staff is away from the office. Obsolete materials are shredded by an outside shredding company.

<u>Accounts Receivable</u>
Student payments are made online and electronically transferred directly to the College's bank account. They are entered into the student information system by the Accounts Receivable Accounting Associate and posted to the students' accounts by the Director of Student Accounts. All postings and related supporting documentation is maintained in a secure filing cabinet and older records are stored in a storage closet that is locked at all times.

Donor payments are brought to the Business Office from the Institutional Advancement Office. These payments are deposited and entered into the general ledger by the Accounts Receivable Accounting Associate. Donor credit card payments are made online and electronically transferred directly to the College's bank account. These payments are also entered into the general ledger by the Accounts Receivable Accounting Associate. All postings and related supporting documentation is maintained in a secured filing cabinet.

Perkins loans are processed by the Director of Student Accounts after a directive is received from the Financial Aid Office. All student information is maintained in a secure filing cabinet in the Business Office.

Accounts Payable

Accounts Payable maintains files that have paid invoice records. These records include a copy of the check, invoice, and supporting documentation. Within this file are payments to independent contractors that include their personal address and Social Security Numbers. These records are stored in a secure filing cabinet in the Business Office and in the locked storage cabinet.

Payroll

Student and staff payroll information is collected by the Payroll Accounting Associate prior to each payroll for submission to Ceridian, the outside payroll processor for MCAD. The Human Resource Office provides all faculty and staff information to the Payroll Accounting Associate. After payroll is processed, the Payroll Accounting Associate maintains all relevant data. Employee checks are kept in the Business Office safe until distributed. The Financial Aid Office monitors all student workers' pay for each payroll period.

On payday, staff and student paychecks are distributed to their respective departments. Faculty paychecks are mailed, as are unclaimed paychecks.

All payroll records are maintained by the Payroll Accounting Associate and kept in a locked filing cabinet in the Business Office.

Financial Aid

Third parties with whom Financial Aid interacts include lending agencies, as well as federal and state governments. These agencies follow federal guidelines resulting from the Privacy Act and the Higher Education Act.

Student information located in the Financial Aid Office is stored in locked filing cabinets. Office doors are always locked when a staff member is not present. Any obsolete materials are shredded in the office or through an outside shredding company.

Records Office

All student information is archived under the direction of the Registrar. A student may receive a transcript upon written request that is dated and signed by the student. To ensure the information is provided to the proper student, the birth date and Social Security Number must be included on all requests.

Student identification numbers are assigned by the Records Office or by the Admissions Office. To ensure confidentiality of students' personal information, these numbers are different than the students' Social Security Numbers.

The Records Office is charged with the compliance of all FERPA regulations as they relate to MCAD.

Continuing Education

The Continuing Education Office receives tuition payments online, which are electronically transferred directly to the College's bank account.

Student information is kept in secure filing cabinets that are constantly monitored during business hours. The office door is locked after hours or when no one is present in the office. Redundant materials are shredded in the office or by an outside shredding company. The Continuing Education Office strictly adheres to all FERPA regulations as they relate to MCAD.

Admissions Office

The Admissions Office receives application fees and tuition deposits online, which are electronically transferred directly to the College's bank account.

Student information is kept in secure filing cabinets that are constantly monitored during business hours. The office door is locked after hours. When files are completed before orientation, they are securely moved to the Records Office. Redundant materials are shredded in the office or by an outside shredding company. The Admissions Office strictly adheres to all FERPA regulations as they relate to MCAD.

Career Services Office

The Career Services Office manages the registration of for-credit student internships. Students complete a Learning Contract that includes their name, address, phone number, major, year in school, and the logistics of the internship. The completed contract is signed by the student, internship site supervisor, the MCAD faculty sponsor, and the MCAD Division Chair. A copy of the completed form is sent to the internship site, the MCAD faculty sponsor, and the MCAD Records Office. Original copies are filed in the Career Services Director's office that is either locked or staffed at all times. Career Services staff will discuss a student's internship activity with the internship site and/or the faculty who are grading the student.

The Career Services Office does not distribute any information about students unless requested by the student. With the student's permission, resumes may be used to provide strong samples for students developing their own resume. Students working in the Career Services Office sign an MCAD Career Services Agreement, stating they understand and will adhere to the professional conduct standards of the Career Services Office and that no student information is to be copied, distributed, or discussed outside of the office.

Housing Office

Student information located in the Housing Office is stored in filing cabinets and online. The Housing Office door is always locked when no staff members are present. All Housing staff members are trained to keep all birth dates, addresses, and phone numbers confidential. Student staff members sign a statement that they understand and will adhere to FERPA guidelines.

Employee Management and Training

Realizing that employees are the ones who ensure the success of any information security, the Human Resource Department will perform background checks prior to hiring regular employees who will have access to customer information. In addition, the Employee Handbook, Faculty Administrative Handbook, and Adjunct Faculty Handbook all contain a section on confidentiality that expressly prohibits the disclosure of confidential information.

Information Security and Processing

Network and Software Design

MCAD uses financial, payroll, student, and institutional advancement software (produced by Great Plains, Ceridian, Jenzabar, and Blackbaud, respectively) that is designed for password and "permitted" access only. This limits access to those users who have a need to use particular sections of the software and prevents unauthorized actions.

Each employee chooses a password with which to gain access to computer terminals and software. These passwords are maintained by the Information Technology Department.

Information Processing, Storage, Transmission, and Disposal

Information is processed daily and backed up seven days a week in the early evening hours. The server room is kept locked and can only be accessed with the permission of the Public Safety or the Information Technology Department.

Information contained on the server is accessible only by the Information Technology Department and is protected by passwords.

Software Backup Plan

All data residing on the Great Plains, Ceridian, Jenzabar, and Blackbaud software is backed up using a rotating schedule. The backup tapes are rotated off-site to Iron Mountain bi-weekly on Tuesdays.

Managing System Security

The Information Technology Department manages system security. This ensures that staff on the technology team implement and carry out required responsibilities relating to the academic, student, and financial software and hardware needs of the campus.

The "backbone" of the system is outfitted with security filters that include access lists to help ensure the integrity of the system and the information residing therein.

Third Party Service Providers

MCAD continually strives to control the risks associated with third party service providers that receive, maintain, process, or otherwise are permitted access to student and/or employee information through their services to the institution. The following third parties have been identified as providing services to the College whereby access to student and/or employee information is provided, either directly or indirectly, through access to MCAD's records so the service providers can fulfill their contractual obligation to the institution. MCAD has requested individual safeguard rules from the following third party service providers:

- Credit Bureau Enterprises (collection agency)
- Williams and Fudge (collection agency)

- Northland Credit Control (collection agency)
- Outsourcing Solutions, Inc. (collection agency)
- IPEDS (government reporting agency)
- TIAA-CREF (employee pension investments)
- Lincoln National Life (employee pension investments)
- Sheffield Olson McQueen (employee benefit administrator)
- Great Plains Dynamics (software provider)
- Ceridian Employer Services (payroll service)
- National Student Loan Clearing House (NSLC)
- Sallie Mae (online service and payment plan provider)
- Veterans Administration
- Sales Force (Admissions' CMS system)
- Blackbaud (software provider)
- Jenzabar
- HigherOne