INFORMATION SECURITY PROGRAM

The Board authorizes the Chancellor to develop, implement, and maintain a comprehensive Information Security Program designed to address the security of the College District's information resources against unauthorized or accidental modification, destruction, or disclosure. The Information Security Program shall include appropriate administrative, technical, and physical safeguards to protect the confidentiality of Personal Information that we access, collect, distribute, process, protect, store, use, transmit, dispose, or otherwise handle. This program shall also address accessibility, privacy, and security of the College District's Web site, information resources, associated processes, systems and networks. To protect confidential information and to comply with applicable federal and state privacy and data security laws and regulations, the Chancellor shall implement policies, regulations, plans, and documents that make up the comprehensive written Information Security Program.

PURPOSE

To protect the integrity, availability, and confidentiality of information used by the College District to run its day to day operations by implementing information safeguards to minimize or control identified internal, operational, and external risks that are potential threats to sensitive personal information and information resources.

APPLICABILITY

This Information Security Program applies to all MCC employees, whether full-time or part-time, including faculty, administrative staff, contract or temporary workers, consultants, interns, and student employees. The Information Security Program also applies to certain contracted third-party vendors. The Information Security Program applies to any Personal Information, whether in paper, electronic, or other form, that is accessed, collected, distributed, processed, protected, stored, used, transmitted, disposed, or otherwise handled by or on behalf of MCC or its affiliates. This Information Security Program is not intended to supersede any existing MCC policy that provides more specific requirements for safeguarding certain types of data, including the definition of directory information under the Family Educational Rights and Privacy Act (FERPA).

DEFINITIONS

"***Personal Information"*** includes nonpublic personally identifiable financial information and other personally identifiable information.

"***Nonpublic Personally Identifiable Financial Information***" means any information that is not publicly available and:

(i) An individual provides to obtain a financial product or service from MCC;
(ii) About an individual resulting from a transaction with MCC involving a financial product or service; or
(iii) MCC otherwise obtains about an individual in connection with providing a financial product or service.

Examples of nonpublic personally identifiable financial information include (but are not limited to):

1. Information an individual provides to MCC on an application to obtain a student loan, credit card, or other financial product or service;

2. Account balance information, payment history, loan or deposit balances, debts, overdraft history, and credit or debit card purchase information;

3. The fact that an individual has obtained federal student aid or a financial product or service from MCC;

4. Any information an individual provides to MCC or that MCC otherwise obtains in connection with collecting on, or servicing, a credit account;

5. Any information MCC collects through an Internet “cookie;”

6. Information from a consumer report; and

7. Any list, description, or other group that is derived using any nonpublic personally identifiable financial information (as described in 1-6 above) that is not publicly available.

“***Personally identifiable information”*** generally means information that can be used to distinguish or trace an individual’s identity and any other information that is linked or linkable to an individual.

Examples of Personally Identifiable Information include (but are not limited to):

- First name and last name or first initial and last name
- Maiden name
- Alias
- Name of student’s parents or other family members
- Mother’s maiden name
- Address
- Telephone number
- Fax number
- Email address
- Social media address
- Social security number
- Driver’s license number, state-issued identification card number
- Federal or state government issued identification card or tribal identification card
- Passport number
- Date of birth
- Place of birth
- Financial account number
- Bank account number
- Credit or debit card number
- Password, PIN, or other access code or security code that would permit access to the person’s financial account

- Tax return information, including taxpayer identification number
- Medical (mental or physical) history information
- Medical (mental or physical) condition information
- Medical (mental or physical) treatment or diagnosis information
- Health account numbers
- Health account payment information
- Health insurance information, subscriber identification number, any unique identifier used by a health insurer to identify the individual, or any medical information in an individual's health insurance application and claims history
- Medical records or medical record numbers
- Other insurance account number
- License plate number
- Device identifiers and serial numbers
- Fingerprints
- Digital signature
- Handwriting
- Biometric data – retina or iris scan, voice, facial geometry
- DNA profile
- Photos, especially of face or other identifying characteristics
- Educational information, including performance evaluations
- Any unique identifying number, characteristic, or code, including electronic identification number or routing code

"Personal Information" does not include:

1. Publicly available information, which means information that MCC has a reasonable basis to believe is lawfully made available to the general public from federal, state, or local government records; widely distributed media; or disclosures to the general public that are required to be made by federal, state, or local law;

2. Any list, description, or other grouping of consumers (and publicly available information pertaining to them) that is derived without using any Personal Information that is not publicly available; or

3. Information that does not identify an individual, such as aggregate information or blind data that does not contain personal identifiers such as account numbers, names, or addresses.

"Service Provider" means any person or entity that receives, maintains, processes, or otherwise is permitted access to customer information through its provisions of services directly to a qualifying entity.

OBJECTIVE

The objectives of this policy are to (1) ensure the security and confidentiality of Personal Information; (2) protect against any anticipated threats or hazards to the security or integrity of Personal Information; and (3) protect against unauthorized access to or use of Personal Information that could result in substantial harm or inconvenience to any individual.

To develop, implement, and maintain the information security program, MCC shall:

1. Designate an employee or employees to coordinate the program;

2. Identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that could result in the unauthorized disclosure, misuse, alteration, destruction or other compromise of such information, and assess the sufficiency of any safeguards in place to control these risks. At a minimum, such a risk assessment should include consideration of risks in each relevant area of the institution's operations, including:
    a. Employee training and management;
    b. Information systems, including network and software design, as well as information processing, storage, transmission and disposal; and
    c. Detecting, preventing and responding to attacks, intrusions, or other systems failures.

3. Design and implement information safeguards to control the risks the institution identifies through risk assessment, and regularly test or otherwise monitor the effectiveness of the safeguard's key controls, systems, and regulations.

4. Oversee service providers by:
    a. Taking reasonable steps to select and retain service providers that are capable of maintaining appropriate safeguards for the customer information at issue; and
    b. Requiring the institution's service providers by contract to implement and maintain such safeguards.

5. Evaluate and adjust the information security program in light of the results of testing and monitoring, any material changes to the institution's operations or business arrangements, or any other circumstances that the college district knows or has reason to know may have a material impact on the information security program.

CHIEF INFORMATION SECURITY OFFICER

MCC designates the Chief Information Security Officer ("CISO") to coordinate our information security program. The CISO may designate other MCC representatives to oversee and coordinate particular elements of the Information Security Program.

NOTICES

Notices informing individuals of their rights to limit the disclosure of personal information and describing the safeguards taken by MCC to protect covered data are provided in a variety of media. Employee specific notices are provided internally through publications such as newsletters, employee handbooks, internal postings, and email messages. Other individuals may receive the information via mailings, campus postings, publications such as the catalog, schedule, student and employee handbooks, and the Student Right to Know Report.

Opt-Out: Individuals have the right to restrict access to publicly available personal information and limit access to covered data and information in some instances (i.e., parental access to attendance records).

Permission to Release Information: Individuals have the right to authorize access to non-public personal information or “covered data and information” to particular individuals, agencies or organizations.

Both “Opt-Out” and “Permission to Release Information” requests must be made on official MCC forms available on the MCC website or campus registrar’s office.

ENFORCEMENT OF POLICY

Compliance with the Information Security Program, this policy and applicable regulations shall be strictly enforced. Violations may result in disciplinary action, up to and including termination.