Appendix AS-14 Standing Information Security Incident Response Team Members

The Maricopa County Community College District is committed to ensuring the protection of private information. This language serves as a supplement to MCCCD administrative regulations 4.22 through 4.24, which are known as the Privacy Statement, the Written Information Security Program and the Information Security Incident Response Plan, respectively. Individuals in the following roles shall serve to facilitate the implementation of the respective regulations. Likewise, the Chancellor may name or appoint additional designees as appropriate:

District Emergency Manager
Director of Enterprise Risk Management
District Director of Business Applications and Compliance
Associate Vice Chancellor of Student Affairs
District Director Center for Human Resource Innovation, Strategy, and Planning
General Counsel
Chief Privacy Officer and Co-Chair of IRT
Chief Information Security Officer and Co-Chair of IRT
Chief Information Officer
Deputy Chief Information Officer
District Director of Marketing and Communications

Definitions: As used in this administrative regulation, the following terms have the respective meanings set forth below:

ARS: Arizona Revised Statutes; the statutory laws that govern the state of Arizona as formally enacted in writing by the Arizona State Legislature, such as the Arizona law that requires businesses, including, but not limited to, colleges and universities, to provide consumer notification of data breaches involving personally identifiable information. Pursuant to ARS § 44-7501, “personally identifiable information (PII) (a) Means an individual’s first name or first initial and last name in combination with any one or more of the following data elements, when the data element is not encrypted, redacted or secured by any other method rendering the element unreadable or unusable: (1) The individual’s social security number; (2) The individual’s number on a driver license issued pursuant to ARS § 28-3166 or number on a nonoperating identification license issued pursuant to ARS § 28-3165; or (3) The individual’s financial account number or credit or debit card number in combination with any required security code, access code or password that would permit access to the individual’s financial account.” PII does not include publicly available information that is lawfully made available to the general public from federal, state or local government records or widely distributed media.

FERPA: Family Educational Rights and Privacy Act; a federal law that protects the privacy of student education records. “Education records” are “those records, files documents, and other materials which 1) contain information directly related to a student; and 2) are maintained by an educational institution.” (20 U.S.C. § 1232g(a)(4)(A); 34 CFR § 99.3). FERPA applies to all schools that receive funds under an applicable program of the U.S. Department of Education.
GLBA aka Financial Services Modernization Act of 1999: Gramm–Leach–Bliley Act; an Act that requires “financial institutions,” including, but not limited to, colleges and universities, to protect the privacy of their customers, including information that customers provide to a financial institution that would not be available publicly (“personally identifiable financial information (PIFI)”). MCCCD, therefore, has a responsibility to secure the personal records of its students and employees. To ensure this protection, GLBA mandates that all financial institutions establish appropriate administrative, technical and physical safeguards. GLBA also requires financial institutions to provide notice to customers about their privacy policies and practices, but institutions of higher education are generally exempt from this requirement, because they already do so under FERPA. Colleges and universities complying with FERPA are considered to be in compliance with GLBA.

HIPAA: Health Insurance Portability and Accountability Act of 1996; an Act to amend the Internal Revenue Code of 1986 to improve portability and continuity of health insurance coverage in the group and individual markets, to combat waste, fraud, and abuse in health insurance and health care delivery, to promote the use of medical savings accounts, to improve access to long-term care services and coverage, to simplify the administration of health insurance, and for other purposes.

HIPAA Privacy Rule aka Privacy Rule: A statute that (1) establishes national standards to protect individuals’ medical records and other personal health information and applies to health plans, health care clearinghouses, and those health care providers that conduct certain health care transactions electronically, (2) requires appropriate safeguards to protect the privacy of personal health information, and sets limits and conditions on the uses and disclosures that may be made of such information without patient authorization, and (3) gives patients rights over their health information, including rights to examine and obtain a copy of their health records, and to request corrections. The Privacy Rule protects all “individually identifiable health information” held or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper, or oral. The Privacy Rule calls this information “protected health information (PHI)” (45 CFR § 160.103). Individually identifiable health information” is information, including demographic data, that relates to:

- the individual’s past, present or future physical or mental health or condition,
- the provision of health care to the individual, or
- the past, present, or future payment for the provision of health care to the individual, and that identifies the individual or for which there is a reasonable basis to believe it can be used to identify the individual. Ibid. Individually identifiable health information includes many common identifiers (e.g., name, address, birth date, social security number).

The Privacy Rule excludes from protected health information employment records that a covered entity maintains in its capacity as an employer and education and certain other records subject to, or defined in, the Family Educational Rights and Privacy Act, 20 U.S.C. §1232g.

Also, See, 17 CFR 160.3 [Title 17 Commodity and Securities Exchanges; Chapter I Commodity Futures Trading Commission; Part 160 Privacy of Consumer Financial Information], for a related definition of PIFI and whereby some GLBA requirements with respect to futures commission merchants, commodity trading advisors, commodity pool operators and introducing brokers.
HIPAA Privacy Rule aka Privacy Rule: A statute that (1) establishes national standards to protect individuals’ medical records and other personal health information and applies to health plans, health care clearinghouses, and those health care providers that conduct certain health care transactions electronically, (2) requires appropriate safeguards to protect the privacy of personal health information, and sets limits and conditions on the uses and disclosures that may be made of such information without patient authorization, and (3) gives patients rights over their health information, including rights to examine and obtain a copy of their health records, and to request corrections. The Privacy Rule protects all “individually identifiable health information” held or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper, or oral. The Privacy Rule calls this information “protected health information (PHI).” (45 CFR § 160.103). Individually identifiable health information is information, including demographic data, that relates to:

- the individual’s past, present or future physical or mental health or condition,
- the provision of health care to the individual, or
- the past, present, or future payment for the provision of health care to the individual, and that identifies the individual or for which there is a reasonable basis to believe it can be used to identify the individual. Ibid. Individually identifiable health information includes many common identifiers (e.g., name, address, birth date, social security number).

The Privacy Rule excludes from protected health information employment records that a covered entity maintains in its capacity as an employer and education and certain other records subject to, or defined in, the Family Educational Rights and Privacy Act, 20 U.S.C. §1232g.

Information Security Incident Response Team (IRT): The internal ad hoc team of professionals that is convened to provide incident handling services to MCCCD during an ongoing information security event and to respond to an information security incident when the need arises.

Payment Card Industry Data Security Standard (PCI DSS): Payment Card Industry Data Security Standard; a proprietary information security standard for organizations that handle cardholder information for the major debit, credit, prepaid, e-purse, automated teller machine (ATM), and point-of-sale (POS/ePOS) cards. “Payment card information” is any personally identifiable information associated with a cardholder, such as the cardholder’s account number, account expiration date, name, address, or social security number. All personally identifiable information associated with the cardholder that is stored, processed, or transmitted is also considered payment card information.

Personnel: All full-time, part-time and temporary employees and faculty who work for the MCCCD organization.

POI: Person(s) of Interest; individuals such as the following who are not considered part of the MCCCD workforce but who are still of interest to the organization:

<table>
<thead>
<tr>
<th>Person of interest category</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dual enrollment instructor</td>
<td>Individuals who teach college-level courses to high school students and are not compensated by MCCCD</td>
</tr>
<tr>
<td>Consultant</td>
<td>Individuals who are hired to do specialized work for MCCCD and are paid by outside sources</td>
</tr>
<tr>
<td>Agency temporary employee</td>
<td>Temporary agency employees who come to work for MCCCD and are paid by the temporary agency</td>
</tr>
</tbody>
</table>
Retired employee | Retired employees who continue a relationship with MCCCD are changed from Employee status to Person of Interest status
Call center or contract employee | Employees who provide support for some of our systems and are paid by the contracted company
Unpaid intern | An individual who is completing an internship at MCCCD for credit in their degree program
Volunteer | An individual who is working at MCCCD on a volunteer basis
Vendor (e.g., Follett bookstores, Chartwells dining services, Aramark facilities services) | Members of organizations that provide services to MCCCD employees and students
ESS Educational Services (e.g., hospitals providing adjuncts for nursing program and/or Fire Science/EMT department) | Members of organizations that have contractual relationships with MCCCD for specialized programs

**Security Incident:** The unauthorized access to and/or misappropriation of Sensitive Information.

**Sensitive Information:** Information that is so deemed under applicable law. Personally identifiable information, personally identifiable education records, individually identifiable health information, personally identifiable financial information and payment card information are examples of Sensitive Information covered under the Arizona Revised Statutes (ARS), Family Educational Rights and Privacy Act (FERPA), Health Insurance Portability and Accountability Act of 1996 (HIPAA), Gramm–Leach–Bliley Act (GLBA aka Financial Services Modernization Act of 1999) and Payment Card Industry Data Security Standard (PCI DSS), respectively.

**Technology Resources:** MCCCD Administrative Regulation 4.4 Technology Resource Standards provides the following examples of technology resources: Websites, applications (such as, but not limited to, MCCCD's Instructure/Canvas-based Course Management System and RioLearn Learning Management System), desktop and laptop systems, printers, central computing facilities, MCCCD-wide or college-wide networks, local-area networks, telephones, facsimile machines, scanners, access to the Internet, electronic mail and similar electronic devices and information.

**Reference(s):**

MCCCD Administrative Regulation 4.4 *Technology Resource Standards*

MCCCD Administrative Regulation 4.23 *Written Information Security Program*

MCCCD Administrative Regulation 6.11 *Identity Theft Red Flag and Security Incident Reporting*

MCCCD Administrative Regulation 6.17 *Requests for Public Information*

MCCCD Appendix AS-14 *Standing Information Security Incident Response Team Members* as attached to this administrative regulation known as MCCCD Administrative Regulation 4.23 *Information Security Incident Response Plan*
Records Retention and Disposition Schedules for Arizona Community Colleges and Districts are located at: https://chancellor.maricopa.edu/public-stewardship/records-information/records-retention-and-disposition-schedules-for

Contact(s):
Pursuant to MCCCD Administrative Regulation 6.11 Identity Theft Red Flag and Security Incident Reporting, anyone who notices that a MCCCD technology resource(s) is currently being or may have been used in an inappropriate fashion should contact the Chief Privacy Officer via email at protectprivacy@maricopa.edu or by phone at 480-784-0PII (x 4-0PII or x 4-0744).

Pursuant to MCCCD Administrative Regulation 6.11 Identity Theft Red Flag and Security Incident Reporting: (1) anyone, including, but not limited to, any MCCCD Personnel and POI, who notices and/or suspects that MCCCD Sensitive Information may currently be or may have been exposed to someone without authorization should immediately contact the Chief Privacy Officer at 480-784-0PII (x 4-0PII or x 4-0744) or protectprivacy@maricopa.edu, and (2) the Chief Privacy Officer is designated as the exclusive recipient of reports of this nature. The Chief Privacy Officer is responsible for obtaining details about the situation from the individual(s) and coordinating with the IRT to take any additional actions that the IRT deems necessary.

MCCCD, in consultation with legal counsel, is responsible for completing the analysis necessary to determine whether a breach has indeed happened. Deciding whether a breach of Sensitive Information has happened is a complex technical and legal determination that involves detailed analysis. Neither MCCCD Personnel, POIs, nor students should postpone notification of the Privacy Officer until they have further investigated or made a breach determination. It is very important that the Privacy Officer be made aware of the situation immediately so that the proper steps can be taken to protect Sensitive Information. MCCCD encourages anyone to report their hunch or suspicion right away, since MCCCD counts on everyone to share the responsibility for keeping information secure.

Please email info@domail.maricopa.edu with any questions and concerns about the MCCCD administrative regulations.

Please email protectprivacy@maricopa.edu with any legal questions and/or to arrange for the evaluation of any vendors, subcontractors and/or third-party products in advance of any work or purchase.

AMENDED by Direct Chancellor Approval: November 12, 2014
DIRECT APPROVAL by the Chancellor, June 19, 2014