administrative regulation

auxiliary services section IV

AR

4.24 Information Security and Privacy Incident Response Plan

Overview

Description: To advance MCCCD's operational responsibilities and to comply with federal, state, local and international laws relevant to information privacy and security, this administrative regulation outlines the responsibilities and procedures of Maricopa County Community College District's ("MCCCD") collective body, known as the Information Security and Privacy Incident Response Team ("IRT"). The IRT is defined in Appendix AS-14 and is charged with responding to actual or suspected situations involving unauthorized access to and/or misappropriation of Confidential Information.[1][2]

Applicability: Information security and privacy is everyone's responsibility. All MCCCD Personnel and Persons of Interest ("POIs") are covered by this administrative regulation. MCCCD students are expected to know and comply with all current published policies, rules and regulations as stated in the college catalog, class schedule, and/or student handbook.[3]

Failure to Comply: Failure to comply with this administrative regulation may result in disciplinary actions up to and including dismissal from employment and termination of service at MCCCD. Regulators may commence legal actions, including, but not limited to, the application of civil and criminal penalties for violations of applicable regulations and/or laws. MCCCD recognizes that laws and regulations involving security of Confidential Information are continuously evolving. In this context, to the extent that applicable data privacy and security laws or regulations conflict with the procedures outlined in the Information Security and Privacy Incident Response Plan, the applicable laws or regulations govern and override the Information Security and Privacy Incident Response Plan.

Information Security and Privacy Incident Response Team Responsibilities

The IRT is chaired by the Chief Information Security Officer, the Chief Privacy Officer, and the Director of Enterprise Risk Management ("Risk Manager") (collectively, "Core IRT"), who are assigned primary responsibility for providing a thorough and orderly response to an actual or suspected Security Incident. While Information security and privacy is everyone's responsibility, the IRT's specific mission is to provide an effective and skillful response to actual or suspected Security Incidents by taking appropriate steps to investigate, contain, and mitigate each incident while reporting findings to management in a timely, efficient manner. The IRT aims to protect Confidential Information and minimize financial loss by ensuring evidence gathering, chain of custody tracking, and preservation of data, as appropriate.

The IRT provides a coordinated response to actual or suspected Security Incidents. The IRT includes, as needed, representatives from operating units within MCCCD along with their alternates. Each represented operating unit has designated one IRT member. The Core IRT is in charge of leading the incident response. Where a Core IRT member is absent during a Security Incident, the Core IRT alternate has the same level of responsibility and expectations under this administrative regulation as does the member of the Core IRT for which he or she serves as an alternate.

If, as a result of an actual or suspected Security Incident, the Chief Information Security Officer and the Chief Information Officer/Vice Chancellor for Information Technology determine that it is necessary to take immediate action involving MCCCD's information technology systems, the Chief Information Security Officer and the Chief Information Officer will determine the appropriate action to take and take that action, consulting with legal counsel if needed, and informing the Chancellor promptly of the determination made and the need for the actions to be taken or already taken. Any subsequent changes to the action taken require the approval of the Chief Information Security Officer and the Chief Information Officer.

AR **4.24 Information Security and Privacy Incident Response Plan (cont'd)**

Appendix AS-14 - Standing Information Security and Privacy Incident Response Team Members is a supplement to Administrative Regulation 4.22 through 4.24, which are known as the *Privacy Statement, The Written Information Security Program* and *Privacy Incident Response Plan*, respectively. Appendix AS-14 contains the job titles that constitute the members of the IRT.

The Core IRT will determine, based on the type of Security Incident involved, which members of the IRT will be called to provide assistance. On a quarterly basis, the IRT will review and, if needed, recommend an update to the job titles listed in the Appendix to ensure that they include the appropriate personnel with District-wide oversight over Confidential Information, employment matters, student matters, and MCCCD's security and privacy. The Core IRT will report the results of its review to the Chancellor for review, revision and approval. The Core IRT will also promptly update the Appendix when the names of the persons in those job titles changes.

With the agreement of the Core IRT, other MCCCD employees or critical contractors may be asked to assist with, for instance, the investigation of an actual or alleged Security Incident ("Auxiliary Personnel"). The IRT will limit the scope of work performed by Auxiliary Personnel at the request of the IRT, along with the time period that the Auxiliary Personnel is involved, to that necessary to investigate facts or to implement mitigation/remediation procedures. Additionally, the Core IRT along with other IRT members will use their best efforts to avoid methods of communication among themselves that may increase the potential for sensitive or confidential information being shared inappropriately outside of the IRT.

General Responsibilities of the Core IRT (Chief Information Security Officer, Chief Privacy Officer and Director of Enterprise Risk Managementr)

- Take charge of the incident response.
- Inform the Chancellor, General Counsel, and the Chief Information Officer if an actual or suspected Security Incident has been reported and provide them with an overview of the situation.
- Lead the investigation and the remediation and mitigation efforts.
- Determine with the General Counsel whether the Core IRT and other members of the IRT and selected MCCCD contractors should operate as agents of the General Counsel.
- Triage each actual or suspected Security Incident.
- Contact the individual who reported the actual or suspected Security Incident.
- Determine the nature and scope of the actual or suspected Security Incident.
- Take steps to ensure that communications among IRT members and with the Chancellor and any other MCCCD executives are confidential and, where appropriate, subject to the attorney-client privilege.
- Determine and engage other members of the IRT in the investigation of and response to an actual or suspected Security Incident as needs dictate.
- For the Risk Manager:
  - Determine whether or when it is appropriate to notify MCCCD's network security and privacy coverage insurance carrier.
  - Be solely responsible for communicating and coordinating with MCCCD's network security and privacy coverage insurance carrier.
- Determine whether there are possible criminal aspects to the actual or suspected Security Incident and, if so, contact MCCCD Public Safety.
- Coordinate responsibilities among themselves and other IRT members.
- Develop a communication plan appropriate for the circumstances including formulating as needed public or internal messages about an actual or suspected Security Incident with

AR **4.24 Information Security and Privacy Incident Response Plan (cont'd)**

Incident Response Steps

The MCCCD IRT will generally follow the steps identified below in responding to incidents. Notably, after the initial assessment commences, some components will proceed simultaneously.

Additionally, these steps in practice may change if MCCCD network security and privacy insurance carrier is involved in the matter. For instance, MCCCD insurance carrier may direct that MCCCD hire outside legal counsel to assist with the legal issues surrounding the actual or suspected Security Incident in which case the Legal Services Department and the Risk Manager will jointly supervise the work of that counsel.

The steps may also change in instances where the Legal Services Department hires outside counsel without consulting with MCCCD's insurance carrier because the matter is not covered by MCCCD's insurance. The steps below are intended to be guidelines, and not set standards, for how MCCCD's response to an actual or suspected Security Incident is conducted.

1. Report and Assess Situation
2. Investigate and Conduct Fact Finding
3. Strategize to Formulate Response
4. Contain and Limit Exposure.
5. Remediate and Resolve Vulnerabilities
6. Document Investigation and Communicate
7. Conduct an Annual Review and Simulation

[1] A Security Incident is the unauthorized access to and/or misappropriation of Confidential Information, or threats to the security and privacy of MCCCD's information technology systems, such as malware or ransomware. Confidential Information is 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 Confidential 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.
[2] This Administrative Regulation supersedes and expressly replaces Administrative Regulation 2.5.6 and Appendix S-11 such that Administrative Regulation 2.5.6 and Appendix S-11 are hereby repealed and no longer effective.
[3] See, for example, MCCCD Administrative Regulations 2.1 General Regulation, 2.5.1 Disciplinary Standards, and 2.5.2 Student Conduct Code.

AMENDED by Direct Chancellor Approval, July 11, 2017
AMENDED by Direct Chancellor Approval: August 24, 2016
AMENDED by Direct Chancellor approval: January 5, 2016
AMENDED by Direct Chancellor Approval: November 12, 2014
DIRECT APPROVAL by the Chancellor, June 19, 2014