Overview

Description: In advancement of the Chief Information Officer’s operational responsibilities and in accordance with federal, state, local and international laws relevant to information privacy and security, this administrative regulation outlines the role-based responsibilities and procedures of Maricopa County Community College District’s (“MCCCD”) collective body, known as the Information Security Incident Response Team, which is charged with responding to actual or suspected situations involving unauthorized access to and/or misappropriation of Sensitive Information.

Applicability: Information Security is everyone’s responsibility. All MCCCD Personnel and Persons of Interest (“POIs”) with access to MCCCD Sensitive Information, whether through use of online technology resources or otherwise, 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.

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 Sensitive Information are continuously evolving. In this context, to the extent that applicable data privacy laws or regulations conflict with the procedures outlined in the Information Security Incident Response Plan, the applicable laws or regulations govern and override the Information Security Incident Response Plan.

1 A Security Incident is the unauthorized access to and/or misappropriation of Sensitive Information. Sensitive 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 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.

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 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.

4 See, for example, MCCCD Administrative Regulations 2.1 General Regulation, 2.5.1 Disciplinary Standards, and 2.5.2 Student Conduct Code.
Information Security Incident Response Team Responsibilities and Procedures

The Incident Response Team ("IRT") is co-chaired by the Chief Information Security Officer and Chief Privacy Officer, who are assigned primary responsibility for providing a thorough and orderly response to an actual or suspected Security Incident. While Information Security 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 (and appropriate external authorities, as necessary) in a timely, cost-efficient manner. The IRT aims to minimize financial loss and protect Sensitive Information by ensuring evidence gathering, chain of custody tracking, and preservation of data, as appropriate. The IRT prepares a written summary of each actual or suspected Security Incident, as necessary.

The IRT includes representatives of several operating units within MCCCD. The IRT provides a coordinated response to actual or suspected Security Incidents. Each represented operating unit has designated one IRT member. The Chief Information Security Officer and Chief Privacy Officer are in charge of the incident response, along with alternates who are designated by the Chief Information Security Officer and Chief Privacy Officer, respectively, to assume authority in all capacities including IRT responsibilities, if the Chief Information Security Officer and Chief Privacy Officer are absent or otherwise unavailable. Listed below are the roles and responsibilities of each operational unit represented on the IRT:

<table>
<thead>
<tr>
<th>Role</th>
<th>IRT Responsibilities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Business Services Division</td>
<td>- When notified that the IRT is activated, provide assistance as determined by the details of the potential incident.</td>
</tr>
</tbody>
</table>
| Chief Information Security Officer| - Serve as co-chairperson of the IRT and, in conjunction with the Chief Privacy Officer, take charge of the incident response.  
- Coordinate activities with Chief Privacy Officer.  
- Provide guidance throughout the investigation.  
- Communicate, in collaboration with the Chief Privacy Officer and Legal, at the executive level the status of any ongoing investigative process and/or Security Incident, as necessary.  
- Make business-related decisions after receiving input from members of the IRT. |
<table>
<thead>
<tr>
<th>Role</th>
<th>Responsibilities</th>
</tr>
</thead>
</table>
| Chief Privacy Officer       | • Serve as co-chairperson of the IRT and, in conjunction with the Chief Information Security Officer, take charge of the incident response.  
• In coordination with Legal, provide legal advice in connection with any actual or suspected Security Incidents.  
• Contact the individual who reported the actual or suspected Security Incidents.  
• Determine the nature and scope of the actual or suspected Security Incidents.  
• Inform Legal and the Chief Information Security Officer if an actual or suspected Security Incident has been reported and provide them with an overview of the situation.  
• Contact appropriate members of the IRT, as necessary.  
• Determine which IRT members will play an active role in the investigation.  
• Contact auxiliary departments, as appropriate.  
• Monitor progress of the investigation.  
• Escalate actual and suspected Security Incidents to the Chief Information Security Officer or executive management, as necessary.  
• Communicate, in collaboration with the Chief Information Security Officer, at the executive level the status of any ongoing investigative process and/or Security Incident, as necessary.  
• In coordination with the Legal, prepare a written summary of actual and suspected Security Incidents, in conjunction with IRT and others, as necessary. |
| Division of Academic and Student Affairs | • When notified that the IRT is activated, provide assistance as determined by the details of the potential incident. |
| Human Resources Division    | • In coordination with Legal, carry out any necessary investigations and disciplinary actions, up to and including dismissal from employment and volunteer service at MCCCD, with respect to those involved in an actual or suspected Security Incident.  
• Prepare a written summary of any corrective action taken, in coordination with Legal. |
Incident Response Procedures

The MCCCD IRT will use the following components in responding to incidents. Notably, after the initial assessment commences, it is anticipated that some components will proceed simultaneously:

1. **Report and Assess Situation:**
The Chief Privacy Officer reports all actual and suspected Security Incidents to the Chief Information Security Officer as soon as practicable.

2. **Strategize to Formulate Response:**
The Chief Privacy Officer conducts a preliminary assessment of the situation to determine the nature and scope of the incident, and notifies appropriate IRT members, Legal, and Outside Counsel. Contacted individuals meet or discuss the situation over the telephone and determine a response strategy.

3. **Contain and Limit Exposure:**
Once the actual or suspected Security Incident has been reported by the Chief Privacy Officer to the Chief Information Security Officer, the Chief Information Security Officer, at the direction of and in coordination with Legal and consistent with any legal advice provided, ensures that the following immediate steps are taken, if applicable, to contain or limit the exposure:
   - Secure the physical area where the actual or suspected Security Incident occurred, if applicable.
   - Interview departments responsible for the Sensitive Information, examine records to identify the relevant data population, and analyze that data population to determine which data contains Sensitive Information that may have been compromised.
   - If the actual or suspected Security Incident is related to electronic data, do not alter or reboot the system(s) containing Sensitive Information that may have been compromised, unless the GC has provided written approval to take such action.
   - Ensure compromised system(s) and media are isolated on and/or from the wireless and all other relevant networks.
   - Gather, review, and analyze all available system, web, database, firewall, file integrity and intrusion detection system event logs.
   - Continue actively monitoring traffic on all systems.
   - Engage external forensic analysts, at direction of Legal, as needed.
   - Perform other procedures mandated by payment card brands, if the actual or suspected Security Incident involves payment card data.
4. **Notify and Engage Authorities:**

- Legal, in coordination with other members of the IRT, determines whether notification must be provided to individuals, entities, regulatory agencies, law enforcement, and/or other external organizations pursuant to applicable federal, state, and/or international law. In some cases, the law may not require notice, but MCCCD may decide, based on the facts and circumstances of a particular incident, to provide notification.
- Legal and Outside Counsel, if applicable, interface with regulators to report Security Incidents in consultation with IRT.
- Unless otherwise permitted by law, no individual or department is to communicate with any internal or external parties without consultation with Legal and obtaining the consent of Legal and the IRT members involved in the particular investigation. In the event that an individual or department receives an inquiry about an actual or potential Security Incident, the inquiring party should immediately be referred to the Chief Privacy Officer.
- If the incident relates to payment card data, the IRT collaborates with Legal and the Business Services Division to contact the applicable acquiring banks, payment card brands and law enforcement offices as required.

5. **Remediate and Resolve Vulnerabilities:**

The IRT helps implement remediation, for example, by working with applicable departments to resolve vulnerabilities, and with the Chief Privacy Officer and Chief Information Security Officer to revise administrative regulations and improve training programs.

6. **Document Investigation and Communicate:**

- Once the investigation is complete, the Chief Privacy Officer, with assistance from IRT and as directed by Legal, creates an Incident Report, in consultation with the investigating unit and Legal, to summarize Security Incidents for review and approval by IRT.

Since a breach or potential breach could result in a regulatory investigation or litigation, it is important that MCCCD receive advice of counsel whenever an actual or suspected Security Incident is investigated and analyzed. Accordingly, all communications concerning actual and suspected Security Incidents are expressly made at the direction of Legal and Outside Counsel (when Outside Counsel is involved) in anticipation of regulatory investigation and litigation that may result from a breach or potential breach. Where practicable, all such written communication should be marked with the following notice: “Privileged and Confidential: Attorney-Client Privileged Communication. This document was prepared at the direction of counsel for the purpose of obtaining legal advice.”

**Annual Review and Simulation**

Annually, members of the IRT receive a copy of the Information Security Incident Response Plan and will review it. The IRT also will annually engage in, at the direction of Legal, an incident response simulation using and testing the Information Security Incident Response Plan. As needed, the Information Security Incident Response Plan will be modified and approved by the IRT based upon the results of the annual incident response simulation, the occurrence of Security Incidents, and notable relevant developments in the higher education and information security industries.

**AMENDED by Direct Chancellor Approval: November 12, 2014**

**DIRECT APPROVAL by the Chancellor, June 19, 2014**