ADMINISTRATIVE REGULATION 3732

SOUTH ORANGE COUNTY COMMUNITY COLLEGE DISTRICT

BUSINESS

INFORMATION SECURITY-SECURITY INCIDENT RESPONSE

I. PURPOSE AND SCOPE

The purpose of the Security Incident Response Administrative Regulation is to provide requirements and procedural steps that will enable a quick and effective recovery from unplanned South Orange County Community College District (SOCCCD) security incidents.

This is one of a series of information security Administrative Regulations designed to protect SOCCCD information systems. District Information Technology (IT) department has the primary responsibility to maintain and implement the provisions of the AR with input from the college Technology Services departments. Refer to *AR 3725 – Information Security Program Overview* Applicability of Assets, Application to Staff, and External Policies.

The primary audience for this Administrative Regulation is the Computer Incident Response Team (CIRT), system and network administrators, and those in District and campus or business areas who have been designated to participate in incident response teams.

Depending on the particulars of the incident, steps noted here may be supplemented by additional SOCCCD procedures, such as those that exist in other documentation, business continuity plans, operational procedures, technical standards, or in other processes and procedures fitting the circumstances of the incident.

1. Applicability

   This Administrative Regulation applies to all Board of Trustees authorized/ratified full-time and part-time regular academic and classified employees, substitutes, short-term (temporary) staff, professional experts, College Work Study students, student help and volunteers who are employed in the South Orange County Community College District for the purpose of meeting the needs of students.

2. Applicability to External Parties

   This Administrative Regulation applies to all external parties, including but not limited to SOCCCD business partners, vendors, suppliers, outsource service providers, and other third-party entities with access to SOCCCD networks and system resources.

3. References and Related Documents

   Please refer to the following Administrative Regulations for additional information and references including definitions:

AR 3725: Information Security Program Overview
AR 3726: Data Classification
AR 3729: Logging and Monitoring
AR 3728: Physical Security
AR 3730: Remote Access
AR 3731: Change Control
AR 3733: Secure Operations
AR 3734: Network Security
AR 3735: Disaster Recovery
AR 4000.2: Electronic Communications

II. INFORMATION SECURITY INCIDENT RESPONSE

Incident response is an expedited reaction to an issue or occurrence either electronic or physical. Those responding must react quickly, minimize damage, minimize service interruptions, and restore resources, all the while attempting to guarantee data integrity, and preserve evidence.

1. Incident Response Administrative Regulation

   Unplanned information security events must be reported to the appropriate operational manager and the District-wide IT Service Desk as quickly as possible. A consistent approach to information security incident response can minimize the extent and severity of security exposures.

   All security incidents must be documented. Where appropriate, security incidents will be reviewed with College Technology Services Department. The Security Incident Report template is used for this purpose.

   The process for handling security incidents has the following phases:

   - Immediate actions
   - Investigation
   - Resolution
   - Recovery and Reporting

   The recommended actions for each phase are described in Section II.4.

   Any directives issued by a member of the CIRT during a response may supersede this document.

2. Maintenance

   This Administrative Regulation will be reviewed and updated every two years at a minimum, or as relevant personnel, locations, threats or regulatory/contractual requirements change.

   The Incident Response plan and procedures should be tested at least annually.

3. Roles and Responsibilities

This section defines roles and teams involved in Incident Response process. Procedures and processes these teams may follow are in Section II.4 of this document.

3.1 Incident Response Coordinator

All information security incidents must be reported through the District-wide IT Service Desk. IT Director: Infrastructure and Security will be the overall Incident Response Coordinator (IRC). The IRC will maintain this Security Incident Response Administrative Regulation and Incident Reports and records, and also coordinate tests and any required training.

3.2 Computer Incident Response Team (CIRT)

CIRT will be responsible for handling the overall SOCCCD response effort. CIRT members represent District IT, college Technology Services, and other departments. CIRT members who are SOCCCD managers may assign others to work on specific tasks of the incident response process.

Not all members of the CIRT will be involved in any given incident. All CIRT members must be willing to accept the responsibility that is required of them and to be able to respond to an emergency at any hour.

3.3 Business Services Response Teams

Business Services Response Teams may be involved in the information security incident response process when an incident occurs in an SOCCCD business area. Both primary and secondary contacts have been designated for each business area.

3.4 Users

Despite the existence of system and audit logs, computer and network users may be the first to discover an information security event or possible breach. All SOCCCD users are responsible for reporting incidents they detect, which may include virus or malware infections, a system compromise, or other suspected security incidents. Incidents must be reported to the District-wide IT Service Desk.

3.5 Managers

SOCCCD managers must ensure that employees are aware of their monitoring and reporting responsibilities. They are also responsible that all suspected information security incidents are reported to the District-wide IT Service Desk as soon as possible.

3.6 Contact Information

Refer to District IT and College Technology Services departmental procedures for designated personnel and contact information for the IRC, CIRT, and Business Services Response Teams.

4. Incident Response Process

The following section describes the procedures that are common to all types of security incidents and the recommended steps for each phase of a security incident. Please refer to Section II.4.3 for specific security incident types.

4.1 Documentation and Preservation of Evidence

Evidence of a computer security incident may be required for civil or criminal prosecution or to document the event for insurance reasons. In order to preserve evidence, all relevant information collected during the incident must be protected. To maintain the usefulness of possible evidence, SOCCCD staff must be able to identify each note or piece of evidence and be prepared to explain its meaning and content.

The chain of custody for all evidence must be preserved. Documentation will be required that indicates the date, time, storage location, and sequence of individuals who handled the evidence. There must not be any lapses in time or date. The hand-off of evidence to authorities must also be documented.

4.2 Control of Information

The control of information during a security incident or investigation of a suspected security incident or breach is critical. If people are given incorrect information, or unauthorized persons are given access to information, there can be undesirable side effects, for example, if the news media is involved.

No SOCCCD staff member, except the Vice Chancellor of Technology and Learning Services or designate(s) has the authority to discuss any security incident with any person outside of the District. If there is evidence of criminal activity, the Vice Chancellor of Technology and Learning Services or designates will notify law enforcement and request their assistance in the matter.

The Incident Response Coordinator (IRC) is the main point of contact for all communications (internal or external) to reduce the spread of misinformation, rumors, and compromise of the response. All CIRT members should refer requests for information to the IRC, who will work with the Vice Chancellor and the Public Information Officer (PIO) regarding any communications.

If a hacking incident were to occur, a secure communications mechanism may need to be implemented since the attacker may be monitoring network traffic. All parties must agree on what technology to use to exchange messages. Even the act of two people communicating could indicate to an intruder that they have been detected. Greater care needs to be exercised when an internal person is suspected or could be an accomplice to the compromise.

Incident-specific information is not to be provided to any callers claiming to be involved. This includes but not limited to systems or accounts involved, programs or system names. All requests for information should be documented and forwarded to the IRC. Members of the CIRT, working with the IRC, will handle any questions regarding the release of any information pertaining to a security

incident. Communication may be from the IRC, a member of the CIRT, or through voicemail or IT bulletins.

If a breach involving personally identifiable or cardholder / credit card information has potentially occurred, the relevant Business Response teams must work with IT and Legal to determine the specific procedures that should be followed and the nature of notification processes.

The Vice Chancellor of Technology and Learning Services or designates will be the only persons who may authorize contacting external law enforcement agencies should this be necessary for Information Security related events.

4.3 Security Incident Categories

Security incidents at SOCCCD fall into one of the following four categories:

Incident Category	Description	Examples
Internal	Any user (authorized or unauthorized) misusing resources or attempting to gain unauthorized access	• Unauthorized use of another's account • Authorized user misusing privileges • Intentionally modifying production data
External	Unauthorized person attempting to gain access to systems or cause a disruption of service	• Denial of service attacks • Mail spamming • Malicious code • Hacking / cracking attempts
Technical Vulnerabilities	A weakness in information system hardware, operating systems, applications or security controls	• Compromised passwords • Data that should be protected appears to be available • Data integrity issues
Loss or theft	Loss or theft of SOCCCD-owned hardware, software; loss or theft of *Restricted* information.	• Lost laptop • Lost smart phone • Lost device or documents containing confidential SOCCCD data • Airport authority confiscation of SOCCCD hardware or software • Theft of SOCCCD hardware or other materials • Breach of student data

4.4 Security Incident Severity Levels

An incident could be any one of the items noted in the "Description" column, and be classified as having a severity level, with corresponding actions to be taken to begin investigation of the incident.

Incident Severity Level	Description	Action required
SEVERE / URGENT	• Successful hacking or denial of service attack • Confirmed breach of personally identifiable (PI) information • Significant operations impact • Significant risk of negative financial or public relations impact	1. Activate CIRT team and notify the IRC. 2. Notify all necessary management team members **3. If a breach of PI or regulated information is suspected**
HIGH	• Hacking or denial of service attack attempted with limited impact on operations • Widespread instances of a new computer virus not handled by anti-virus software • Possible breach of student information or PI • Some risk of negative financial or public relations impact	1. Notify Incident Response Coordinator, who will notify CIRT team members as necessary. **2. If a breach of Confidential information is suspected**
MEDIUM	• Hacking or denial of service attacks attempted with no impact on operations • Widespread computer viruses easily handled by anti-virus software • Lost laptop / smart phone, but no data compromised	1. Notify Incident Response Coordinator, who will notify CIRT team members if necessary.
LOW	• Password compromises – single user • Unauthorized access attempts • Account sharing • Account lockouts	1. Notify Incident Response Coordinator.

4.5 Security Incident Phases

The process for handling all SOCCCD security incidents has four general phases:

1. Immediate actions
2. Investigation
3. Resolution
4. Recovery and Reporting

4.5.1 Immediate Actions

The first actions to be taken are to make an initial identification of the category of incident occurring (Internal, External, Technical Vulnerabilities, Loss or Theft) as described in the 4.4 table, and notify the District-wide IT Service Desk.

Users must notify the District-wide IT Service Desk immediately upon identifying a security incident of any type. As a rule, users should also notify their immediate manager to inform them of the incident. The District-wide IT Service Desk will then notify the appropriate response teams to begin investigation and resolution phases.

Response to an incident must be decisive and be executed quickly. Reacting quickly will minimize the impact of resource unavailability and the potential damage caused by system compromise or a data breach.

4.5.2 Investigation

The Vice Chancellor of Technology and Learning Services or designates has the authority to determine the Severity level of an incident and activate the CIRT.

Once reported to the District-wide IT Service Desk, a determination will be made as to the Severity Level (Severe / Urgent, High, Medium, or Low) of the incident based on initial reports.

It is the intent of this Administrative Regulation that, routine issues or Medium and Low Severity level incidents be handled by District IT or the appropriate College Technology Services departments, but could be escalated to High or Urgent levels depending based on additional information.

Upon declaration of a security incident, the following actions may also occur depending on the severity and nature of the incident:

- Notification of executive management team members / campus Security
- Notification of District IT Management and College Technology Departments, if applicable.
- Notification of any outside service providers

- Notification of Business Response Teams impacted by the security event
- Initiation of a public relations response plan or development of emergency communications
- Notification of business partners and others who may be impacted by the security event
- Implementation of incident response actions for the containment and resolution of the situation needed to return to normal operations

4.5.3 Resolution

SOCCCD's immediate objective after an incident has been reported and preliminary investigation has occurred is to limit its scope and magnitude as quickly as possible.

4.5.4 Recovery and Reporting

After containing the damage and performing initial resolution steps, the next priority is to begin recovery steps and make necessary changes to remove the cause of the incident. Reports and evidence must also be organized and retained.

A process to modify and evolve the incident response plan according to lessons learned and to incorporate industry developments will be managed by District IT.

5.0 Glossary / Definitions

Business Services Response Teams	Business Services Response Teams can be activated to enhance SOCCCD's response to incidents that affect specific business services areas. These teams have established designated contacts for handling incidents or security breaches and enhance collaboration between diverse groups.
Computer Incident Response Team (CIRT)	The CIRT will act as the core incident coordination team for severe security incidents or breaches, and is represented by individuals from District IT, College Technology Services departments, and business areas.
Incident Response Coordinator (IRC)	The IRC serves as the primary point of contact for response activities and maintains records of all incidents. This individual has overall responsibility and ownership of the Incident Response process.
Security Breach	Unauthorized release or exposure of information that is confidential, sensitive, or personally identifiable. The definition of a breach and the actions that must be taken can vary based on regulatory or contractual requirements.

Security Incident	A security incident is any adverse event that compromises the confidentiality, availability, or integrity of information. An incident may be noticed or recorded on any system and or network controlled by SOCCCD or by a service provider acting on behalf of SOCCCD.
Security Violation	An act that bypasses or contravenes SOCCCD security Administrative Regulations, practices, or procedures. A security violation may result in a security incident or breach.