Book	Administrative Procedures
Section	Chapter 3 - General Institution
Title	Information Security - Security Incident Response
Code	AP 3725
Status	Active
Adopted	March 9, 2021
Last Revised	March 9, 2021
Last Reviewed	March 9, 2021

Purpose and Scope

The purpose of the Security Incident Response Administrative Procedure is to provide requirements and procedural steps that will enable a quick and effective recovery from unplanned **COLLEGE OF THE REDWOODS** security incidents.

This is one of a series of information security Administrative Procedures maintained by the district Information Technology (IT) department designed to protect the district's information systems.

This Policy contains:

- Requirements for responding to information security incidents or breaches
- Roles and responsibilities
- Basic procedures needed to respond in a systematic manner

District IT Departmental Procedures exist which contain:

- Security Incident Report template
- Contact information
- Preservation of Evidence
- Breaches of Confidential or Personal Information
- Additional Resources

The primary audience for this Administrative Procedure 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 district 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.

Applicability to all Employees and Volunteers

This Administrative Procedure 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 by the district for the purpose of meeting the needs of students.

This Administrative Procedure applies to all employees of the district and all district consultants or contractors.

Applicability to External Parties

Not Applicable.

References and Related Documents

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

- AP 3720: Acceptable Use
- AP 3721: Change Control

- AP 3722: Disaster Recovery
- AP 3723: Network Security
- AP 3724: Secure Operations
- AP 3725: Security Incident Response
- AP 3726: Data Classification
- AP 3727: Physical Security
- AP 3728: Logging and Monitoring
- AP 3729: Remote Access

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.

Incident Response Administrative Procedure

Unplanned 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 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 local campus IT management. 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 3.

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

Maintenance

This Security Incident Response Administrative Regulation will be reviewed and updated on a bi-annual basis 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.

Roles and Responsibilities

This section defines roles and teams involved in Incident Response process. Procedures and processes these teams may follow are in Section 3 of this document.

Incident Response Coordinator

All security incidents must be reported to district IT. Where appropriate, district management will determine who 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.

Computer Incident Response Team (CIRT)

The Computer Incident Response Team (CIRT) will be responsible for handling the overall district response effort. CIRT members represent the IT, Legal, and HR. CIRT members who are district 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.

Business Response Teams

Business Response Teams may be involved in the incident response process when an incident occurs in a district business area.

Both primary and secondary contacts have been designated for each business area.

Users

Despite the existence of system and audit logs, computer and network users may be the first to discover a security event or possible breach. As noted in the Information Security Administrative Regulation 3725, end users need to be vigilant for signs of unusual system or application behavior which may indicate a security incident in progress.

All district 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 district IT.

Managers

COLLEGE OF THE REDWOODS managers must ensure that employees are aware of their monitoring and reporting responsibilities. They are also responsible for reporting all suspected information security incidents to district IT as soon as possible.

Contact Information

Refer to district IT departmental procedures for designated personnel and contact information for the IRC, CIRT, and Business Response Teams.

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 3.3.2 for specific security incident types.

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, district 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.

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 district staff member, except the Director of Information Technology or designee has the authority to discuss any security incident with any person outside the district. If there is evidence of criminal activity, designees will notify law enforcement and request their assistance in the matter.

The 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 Director of Information Technology 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.

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 Incident Response Coordinator (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 the IT and Legal to determine the specific procedures that should be followed and the nature of notification processes.

The President or designees will be the only persons who may authorize contacting external law enforcement agencies should this be necessary.

Security Incident Categories

Security incidents at **COLLEGE OF THE REDWOODS** fall into one of the following four categories:

Incident Category	Description	Examples

Internal	Any user (authorized or unauthorized) misusing resources, violating the acceptable use administrative regulation, or attempting to gain unauthorized access	• Unauthorized use of another's account • Authorized user misusing privileges • Intentionally modifying production data • Inappropriate use of College and District computing resources.
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 district-owned hardware, software; loss or theft of *Restricted* information.	• Lost laptop • Lost smart phone • Lost device or documents containing confidential district data • Airport authority confiscation of district hardware or software • Theft of district hardware or other materials • Breach of student data

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)	1. Activate CIRT team and notify the IRC. 2. Notify all necessary management team members

	information • Significant operations impact • Significant risk of negative financial or public relations impact	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.

Security Incident Phases

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

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

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 table above, and notify the District-wide IT Service Desk.

The **COLLEGE OF THE REDWOODS** Information Security Administrative Procedure 3725 directs users to notify the district IT 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. IT 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.

Investigation

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

The Director of Information Technology or designee (designee may include college management) has the authority to declare a *Severity* level incident and activate the CIRT.

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.
- 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

Resolution

The district'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.

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.

Incident Response Contact Matrix

The following table describes common incidents and the recommended primary reporting contact for each. The Primary contact will be responsible for assigning an IRC.

Category	User Group	Recommended Primary Contact
Internal, External, Loss or Theft	Students	Vice President of Student Services
Technical Vulnerability	Students	Vice President Student Services, College IT Director
Internal, External, Loss or Theft	Faculty	Vice President of Instruction
Technical Vulnerability	Faculty	Vice President of Instruction, College IT Director
Internal, External, Loss or Theft	Staff	Vice-Chancellor of Human Resources
Technical Vulnerability	Staff	Vice-Chancellor of Human Resources, District IT Director

Glossary / Definitions

Business Response Teams	Business Response Teams can be activated to enhance the district's response to incidents that affect specific business 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, 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	i. 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 the district or by a service provider acting on behalf of the district.
Security Violation	An act that bypasses or contravenes district security Administrative Regulations, practices, or procedures. A security violation may result in a security incident or breach.