



Origination 12/2024
 Last Approved 12/2024
 Effective 12/2024
 Last Revised 12/2024
 Next Review 12/2034

Chapter Lead Nohemy Ornelas:
 Chapter 3(CC),4&5
 Policy Area Chapter 3
 General Institution
 References Non CCLC

AP 3732 Information Security Security Incident Response

1. PURPOSE AND SCOPE

The purpose of the Security Incident Response Administrative Procedure is to ensure a standardized method for handling changes to District internally developed systems. Change control promotes the stability of the environment, which is essential to its security and integrity.

This is one of a series of information security Administrative Procedures designed to protect District information systems. The District Information Technology (IT) department has district-wide fiduciary responsibility to set, maintain, and ensure the regulations' provisions. District IT accomplishes this through collaborative engagement with the college Technology Services departments.

This Administrative Procedure has been written to align with the best practices as outlined in the NIST SP 800-61 Guidance.

a. Applicability

This Administrative Procedure applies to all full-time and part-time regular academic and classified employees, such as, short-term (temporary) staff, substitutes, professional experts, Federal Work Study students, and student help who are employed by, and volunteers who assist, the District for the purpose of meeting the needs of students.

b. Applicability to External Parties

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

c. References and Related Administrative Procedures

Please refer to Information Security Administrative Procedures for additional information, references, and definitions.

2. INFORMATION SECURITY INCIDENT RESPONSE

Information in this regulation may be supplemented with other District information external to this document. Such information may include other business continuity plans, processes, procedures, technical standards, runbooks, etc.

In addition to providing a standardized process flow, this regulation:

- Identifies the incident response (IR) stakeholders and establishes their roles and responsibilities;
- describes incident triggering sources, incident types, and incident severity levels; and
- includes requirements for maintenance. This Administrative Procedure aligns with best practices as outlined in NIST SP 800-61.

a. Glossary/Definitions

Business Services Response Teams	Business Services Response Teams can be activated to enhance District incidents that affect specific business services areas. These teams have designated contacts for handling incidents or security breaches and encourage collaboration between diverse groups.
Computer Incident Response Team (CIRT)	The CIRT will act as the core incident coordination team for severe security breaches and is represented by individuals from District IT, College Teaching departments, and business areas. The composition of the CIRT will vary based on requirements.
Incident	An Incident is defined as an event that presents the potential of unauthorized, unintended exposure, modification, restriction from access, or deletion of assets, both physical and electronic, under the care of the District.
Incident Response Coordinator (IRC)	The IRC serves as the primary point of contact for response activities of all incidents. This role has overall responsibility and ownership of the process. The Director, Security and User Services is assigned this role. Other positions may act as IRC where appropriate.
Security Breach	Unauthorized release or exposure of information that is confidential, sensitive, or identifiable. The definition of a breach and the actions that must be taken are based on regulatory or contractual requirements.
Security Incident	A security incident is any adverse event that compromises the confidentiality, integrity of information. An incident may be noticed or recorded on an information network controlled by the District or by a service provider acting on behalf of the District.
Security Violation	An act that bypasses or contravenes District security Administrative Procedures or procedures. A security violation may result in a security incident or breach.
External Entities	In consultation with the CIRT, external entities may conduct hands-on investigative response activities, or may provide guidance. External entities may include service providers, or law enforcement, such as: • Multi-State Information Sharing and Analysis Center (MS-ISAC) • Federal Bureau of Investigation (FBI) • Attorneys (e.g., "Cyber Coaches") and Forensics Consultants • Service Providers such as Internet and Security • Data Holder Vendors

b. Incident Reporting

Unplanned information security events must be reported to the appropriate manager and the district-wide IT Service Desk as quickly as possible. Suspected data breaches must be reported to the IT Service Desk within eight (8) hours of identification.

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

c. Maintenance

This Administrative Procedure will be reviewed and updated minimally every five years or as relevant personnel, locations, threats, or regulatory/contractual requirements change.

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

d. 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.

i. 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.

Documentation of the incident must minimally include:

- Date/time the incident was reported
- Type of Incident
- Reporting source of incident
- Summary of the incident
- Current status of the incident
- All actions taken concerning the incident
- Contact information for all involved parties
- Evidence gathered during the incident investigation
- Relevant comments from IR team members
- Proposed next steps to be taken

ii. Security Incident Categories

District Security incident categories can be found in the district-wide IT Service Desk.

iii. Security Incident Severity Levels

Incident Severity Level	Description	Action Required
	Significant risk of negative financial or public relations impact	Management team mem
HIGH	• Hacking or denial of service attack attempted with limited impact on operations	1. Log incident in

Incident Severity Level	Description	Action Required
	- Widespread instances of a new computer virus not handled by anti-virus software - Possible breach of student information or PII - Some risk of negative financial or public relations impact	2. Notify IRC or d 3. IRC will notify members as n
MEDIUM	- Hacking or denial of service attacks attempted with no impact on operations - Widespread computer viruses are easily handled by anti-virus software - Lost laptop/smartphone, but no data compromised	1. Log incident in 2. IRC will review team member
LOW	- Password compromises – single user - Unauthorized access attempts - Account sharing - Account lockouts	1. Log the incident Service Desk v appropriate. 2. IRC will review remediation as

e. Escalation

If it is discovered that the scope or severity of an incident has changed, it is important to communicate this change to the CIRT.

If an incident involves a breach of Payment Card Industry (PCI) data, the acquirer and related payment brands must be notified of the incident as soon as possible.

Include the appropriate IR stakeholders in identifying the reporting procedures for each payment brand and acquirer involved in the incident. (PCI DSS 12.10.1)

If an incident potentially involves a breach of student personally identifiable information (PII) or financial aid data, the IRC must be notified immediately. The IRC will then communicate to appropriate CIRT team members (e.g., Financial Aid Directors). It is their responsibility to follow the U.S. Department of Education Privacy laws specified in the Family Educational Rights and Privacy Act (FERPA).

For all other incidents, the Vice Chancellor of Educational and Student Support Services or designee(s) must be consulted prior to discussion with any person outside of the District.

Approval Signatures

Step Description

Approver

Date

COPY