# ADMINISTRATIVE REGULATION 37xx

**NAME OF CC DISTRICT** BUSINESS

## INFORMATION SECURITY-SECURITY INCIDENT RESPONSE

### 1.0 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 **NAME OF CC DISTRICT** security incidents.

This is one of a series of information security Administrative Regulations maintained by the District Information Technology (IT) department designed to protect **NAME OF CC DISTRICT** 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 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 **NAME OF CC 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.

#### 1.1 Applicability to all Employees and Volunteers

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 **NAME OF CC DISTRICT** for the purpose of meeting the needs of students.

This Administrative Regulation applies to all employees of **NAME OF CC DISTRICT** and all **NAME OF CC DISTRICT** consultants or contractors.

#### 1.2 Applicability to External Parties

Not Applicable.

#### 1.3 References and Related Documents

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

* AR 37xx: Acceptable Use
* AR 37xx: Change Control
* AR 3726: Data Classification
* AR 37xx: Disaster Recovery
* AR 37xx: Information Security Program Overview
* AR 3729: Logging and Monitoring
* AR 37xx: Network Security
* AR 3728: Physical Security
* AR 3730: Remote Access
* AR 37xx: Secure Operations
* AR 37xx: Security Incident Response

### 2.0 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.

#### 2.1 Incident Response Administrative Regulation

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.

#### 2.2. 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.

#### 2.3 Roles and Responsibilities

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

##### 2.3.1 Incident Response Coordinator

All security incidents must be reported to District IT or Campus IT through the District-wide IT Service Desk. Where appropriate, District Management or Campus 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.

##### 2.3.2 Computer Incident Response Team (CIRT)

The Computer Incident Response Team (CIRT) will be responsible for handling the overall **NAME OF CC DISTRICT** response effort. CIRT members represent the IT, Legal, HR, and campus organizations. CIRT members who are **NAME OF CC 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.

##### 2.3.3 Business Response Teams

Business Response Teams may be involved in the incident response process when an incident occurs in an **NAME OF CC DISTRICT** business area. Both primary and secondary contacts have been designated for each business area.

##### 2.3.4 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 37xx, end users need to be vigilant for signs of unusual system or application behavior which may indicate a security incident in progress.

All **NAME OF CC 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 the District-wide IT Service Desk.

##### 2.3.5 Managers

**NAME OF CC DISTRICT** 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 the District-wide IT Service Desk as soon as possible.

#### 2.4 Contact Information

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

### 3.0 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.

#### 3.1 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, **NAME OF CC 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.

#### 3.2 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 **NAME OF CC DISTRICT** staff member, except the Vice Chancellor of Technology and Learning Services or his designate(s) has the authority to discuss any security incident with any person outside of the District. If there is evidence of criminal activity, he or his designates 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 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 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 Vice Chancellor of Technology and Learning Services or his designates will be the only persons who may authorize contacting external law enforcement agencies should this be necessary.

#### 3.3 Security Incident Categories

Security incidents at **NAME OF CC DISTRICT** 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 **NAME OF CC DISTRICT**-owned hardware, software; loss or theft of *Restricted* information. | * Lost laptop * Lost smart phone * Lost device or documents containing confidential **NAME OF CC DISTRICT** data * Airport authority confiscation of **NAME OF CC DISTRICT** hardware or software * Theft of **NAME OF CC DISTRICT** hardware or other materials * Breach of student data |

#### 3.4 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. |

#### 3.5 Security Incident Phases

The process for handling all **NAME OF CC DISTRICT** security incidents has four general phases:

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

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

The **NAME OF CC DISTRICT** Information Security Administrative Regulation 37xx directs users to 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.

##### 3.5.2 Investigation

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.

The Vice Chancellor of Technology and Learning Services or his designate (designate 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 and/or campus 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

##### 3.5.3 Resolution

**NAME OF CC 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.

##### 3.5.4 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.

#### 3.6 Incident Response Contact Matrix

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

|  |  |  |
| --- | --- | --- |
| Category | User Group | 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 |

### 4.0 Glossary / Definitions

|  |  |
| --- | --- |
| **Business Response Teams** | Business Response Teams can be activated to enhance **NAME OF CC 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, campus 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** | 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 **NAME OF CC DISTRICT** or by a service provider acting on behalf of **NAME OF CC DISTRICT**. |
| **Security Violation** | An [act](http://www.businessdictionary.com/definition/act.html) that bypasses or contravenes **NAME OF CC DISTRICT** [security Administrative Regulations,](http://www.businessdictionary.com/definition/security-policy.html)  [practices](http://www.businessdictionary.com/definition/practice.html), or [procedures](http://www.businessdictionary.com/definition/procedure.html). A security violation may result in a security incident or breach. |