**Cyber Security Incident Response Plan For [DISTRICT\_NAME]**

[Logo HERE]

**Table of Contents**

[VERSION HISTORY 4](#_Toc126060994)

[[District\_Name] Cyber Security Incident Response Plan 4](#_Toc126060995)

[Purpose 4](#_Toc126060996)

[Scope 5](#_Toc126060997)

[Definitions 6](#_Toc126060998)

[Event 6](#_Toc126060999)

[Incident 6](#_Toc126061000)

[Personally Identifiable Information (PII) 6](#_Toc126061001)

[Protected Health Information (PHI) 6](#_Toc126061002)

[Security Incident Response 7](#_Toc126061003)

[Maintenance 8](#_Toc126061004)

[Roles and Responsibilities 8](#_Toc126061005)

[Incident Response Coordinator 8](#_Toc126061006)

[Cybersecurity Incident Response Team (CIRT) 8](#_Toc126061007)

[Business Response Teams 8](#_Toc126061008)

[Users 9](#_Toc126061009)

[Department Managers 9](#_Toc126061010)

[Contact Information 9](#_Toc126061011)

[Incident Response Process 9](#_Toc126061012)

[Documentation and Preservation of Evidence 9](#_Toc126061013)

[Control of Information 10](#_Toc126061014)

[Security Incident Categories 10](#_Toc126061015)

[Security Incident Severity Levels 11](#_Toc126061016)

[Security Incident Phases 12](#_Toc126061017)

[Immediate Actions 13](#_Toc126061018)

[Investigation 13](#_Toc126061019)

[Resolution 14](#_Toc126061020)

[Recovery and Reporting 14](#_Toc126061021)

[Incident Response Contact List 14](#_Toc126061022)

[Glossary / Definitions 14](#_Toc126061023)

[Appendix A: Incident Response Quick Reference Guide 16](#_Toc126061024)

[Information Security Incident Response Execution Phases 16](#_Toc126061025)

[Assessing the Suspicious Event, Machine, or Situation 16](#_Toc126061026)

[If You Believe a Compromise is Likely 17](#_Toc126061027)

[Windows Initial System Examination Tips 17](#_Toc126061028)

[Linux Initial System Examination 18](#_Toc126061029)

[Appendix B: Reporting and Notification Quick Start Guide 19](#_Toc126061030)

[Communication Oversight 19](#_Toc126061031)

[Communicating with District Management 19](#_Toc126061032)

[Managing Incident Response 19](#_Toc126061033)

[Major Risk Incidents 19](#_Toc126061034)

[Moderate and Minor Risk Incidents 20](#_Toc126061035)

[[DISTRICT\_INITIALS] Incident Response Team ([DISTRICT\_INITIALS]-IRT) 20](#_Toc126061036)

[Detection 20](#_Toc126061037)

[Activation 20](#_Toc126061038)

[Containment 20](#_Toc126061039)

[Notification 20](#_Toc126061040)

[Remediation 21](#_Toc126061041)

[Resolution 21](#_Toc126061042)

[After-Action Analysis 21](#_Toc126061043)

[Appendix C: Incident Questionnaire and Information Gathering 22](#_Toc126061044)

[Information Needed about Detection 22](#_Toc126061045)

[Information Needed from the User 22](#_Toc126061046)

[Questions about the Incident 22](#_Toc126061047)

[Information Needed from IT Support 23](#_Toc126061048)

[Infection Details and Analysis 23](#_Toc126061049)

[Incident Analysis 23](#_Toc126061050)

[Appendix D: Communication Strategy and Plan Worksheet 24](#_Toc126061051)

[Communicate through channels known to be unaffected by the incident. 24](#_Toc126061052)

[Potential stakeholders 24](#_Toc126061053)

[Identify authorized individuals to communicate about the incident to internal and external constituencies. 24](#_Toc126061054)

[Internal communications channels 24](#_Toc126061055)

[External communications channels 24](#_Toc126061056)

[Schedule and frequency of communication 25](#_Toc126061057)

[The plan should identify 25](#_Toc126061058)

[Appendix E: Notification of External Organizations Involved in an Information Security Incident 26](#_Toc126061059)

[Appendix F: After-Action Analysis Report Template 27](#_Toc126061060)

[Executive Summary 27](#_Toc126061061)

[Context and Background 27](#_Toc126061062)

[Findings 27](#_Toc126061063)

[Notifications Required and Performed 27](#_Toc126061064)

[Recommendations for Improved Security 27](#_Toc126061065)

VERSION HISTORY

This plan is to be considered a living document and shall be reviewed and updated on an annual basis.

|  |  |  |  |
| --- | --- | --- | --- |
| **Version#** | **Revision****Date** | **Approved****By** | **Reason** |
| 1.0 | 02/01/2023 | Carl Fong | Initial Draft |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

#  [District\_Name] Cyber Security Incident Response Plan

Purpose

In response to ever-increasing cyber attacks in the K-12 education sector, [DISTRICT\_NAME] ({DISTRICT\_INITIALS]) has developed this cybersecurity incident response plan.

A cybersecurity incident response plan is a crucial document for any organization as it outlines the procedures to be followed in case of a cyber-attack or data breach. Having a well-structured response plan in place is essential for minimizing damage and restoring normal operations as quickly as possible. This cybersecurity incident response plan will include several key components such as the identification of key personnel and their roles and responsibilities in the incident response process, procedures for reporting and documenting incidents, communication protocols for internal and external stakeholders, guidelines for containing and eradicating the incident, procedures for restoring normal operations and recovering lost data, roles of the incident response team post-incident review and updating of the incident response plan, and regular training and testing of incident response plan to ensure readiness and effectiveness. The incident response plan is a critical component of an organization's overall cybersecurity strategy. It can help mitigate the impact of a cyber-attack or data breach and minimize the risk of future incidents and also reduce the likelihood of the incident happening again.

Scope

This plan applies to the Information Systems, Data, and networks of [DISTRICT\_INITIALS], and any person or device that has access to these systems and/or data.

This Procedure contains:

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

[DISTRICT\_INITIALS] 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 incident response plan is the Cybersecurity Incident Response Team (CIRT), system and network administrators, and those 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\_INITIALS] 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.

Definitions

Event

A cybersecurity event is any observable occurrence in a network or system that has the potential to compromise the confidentiality, integrity, or availability of the network or system. Examples of cybersecurity events include network scans, attempted logins, and software crashes.

Incident

A cybersecurity incident, on the other hand, is a cybersecurity event that has resulted in or has a significant risk of resulting in an adverse impact on the confidentiality, integrity, or availability of the network or system. Examples of cybersecurity incidents include successful hacking attempts, data breaches, and ransomware attacks.

Personally Identifiable Information (PII)

For the purpose of meeting security breach notification requirements, PII is defined as a

person’s first name or first initial and last name in combination with one or more of the

following data elements:

* Address
* Email
* Telephone number
* Date of birth
* Passport number
* Social security number
* State-­‐issued driver’s license number
* State-­‐issued identification card number
* Financial account number in combination with a security code, access code or password that would permit access to the account
* Medical and/or health insurance information

Protected Health Information (PHI)

PHI is defined as "individually identifiable health information" transmitted by electronic

media maintained in electronic media or transmitted or maintained in any other form or

medium by a Covered Component, as defined in Carnegie Mellon’s HIPAA Policy. PHI is

considered individually identifiable if it contains one or more of the following identifiers:

* Name
* Address (all geographic subdivisions smaller than state, including street address,
* city, county, precinct or zip code)
* All elements of dates (except year) related to an individual including birth date, admissions date, discharge date, date of death and exact age if over 89)
* Telephone numbers
* Fax numbers
* Electronic mail addresses
* Social security numbers
* Medical record numbers
* Health plan beneficiary numbers
* Account numbers
* Certificate/license numbers
* Vehicle identifiers and serial numbers, including license plate number
* Device identifiers and serial numbers
* Universal Resource Locators (URLs)
* Internet protocol (IP) addresses
* Biometric identifiers, including finger and voice prints
* Full-face photographic images and any comparable images
* Any other unique identifying number, characteristic or code that could identify an individual

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.

This document is based on the NIST (National Institute of Standards and Technology) Incident Response Framework. It is a set of guidelines and best practices for incident response and management. It is designed to help organizations, such as school districts, to respond effectively to cyber incidents and minimize their impact. The framework is based on the NIST Cybersecurity Framework (CSF) and is intended to be used in conjunction with it.



The NIST Incident Response Framework is divided into four phases: Preparation, Detection and Analysis, Containment, Eradication, Recovery, and post-incident activity.

1. Preparation phase: This phase focuses on the development of an incident response plan and the identification of incident response team members and their roles and responsibilities. It also includes the identification of the organization's critical assets and the development of incident response procedures and guidelines.
2. Detection and Analysis phase: This phase focuses on the detection of a cybersecurity incident and the collection and analysis of information about the incident. The goal of this phase is to identify the scope and nature of the incident and to determine the appropriate response.
3. Containment, Eradication, and Recovery phase: This phase focuses on containing the incident to prevent it from spreading, eradicating the incident by removing the cause, and recovering from the incident. This includes steps such as disconnecting affected systems from the network, restoring normal operations, and recovering lost data.
4. Post-incident activity: This phase focuses on reviewing the incident response process, identifying areas for improvement, and updating the incident response plan.

Maintenance

The Incident Response Plan will be reviewed and updated annually 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 by tabletop exercise or red teams

Roles and Responsibilities

This section defines roles and teams involved in the Incident Response process. The 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\_INITIALS] IT through the District-wide IT Service Desk. Where appropriate, District Management will determine who will be the overall Incident Response Coordinator (IRC). The IRC or Cybersecurity team will maintain this Security Incident Response Plan, incident reports, records, and will coordinate tests and any required training.

Cybersecurity Incident Response Team (CIRT)

The Cybersecurity Incident Response Team (CIRT) will be responsible for handling the overall [DISTRICT\_INITIALS] response effort. CIRT members represent the IT, Legal, HR, and any District Cabinet members. CIRT members who are [DISTRICT\_INITIALS] 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\_INITIALS] 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. End users need to be vigilant for signs of unusual system or application behavior which may indicate a security incident in progress.

All [DISTRICT\_INITIALS] 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\_INITIALS] IT Help Desk.

Department Managers

[DISTRICT\_INITIALS] 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\_INITIALS] IT Help Desk as soon as possible.

Contact Information

Refer to [DISTRICT\_INITIALS] 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 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\_INITIALS] IT 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\_INITIALS] staff member, except the Chief Technology Officer (CTO)/ Director of IT or their designee(s) has the authority to discuss any security incident anyone without prior approval from their senior level management. The district Public Information Officer (PIO) or Cabinet designee has the authority to contact any person outside of the [DISTRICT\_INITIALS]. If there is evidence of criminal activity, the CTO/Director of IT or their designee(s) will notify their senior leadership/Cabinet before 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 Superintendent 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 and PIO, will handle any questions regarding the release of any information pertaining to a security incident. Communication may be from the IRC, PIO, 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 teams to determine the specific procedures that should be followed and the nature of notification processes.

The Superintendent or their designee(s) will be the only persons who may authorize contacting external law enforcement agencies should this be necessary.

Security Incident Categories

Security incidents at [DISTRICT\_INITIALS] fall into one of the following four categories:

|  |  |  |
| --- | --- | --- |
| Incident Category | Description | Examples |
| Internal  | Any user (authorized or unauthorized) misusing resources, violating the acceptable use ITSS, or attempting to gain unauthorized access | * Unauthorized use of another’s account
* Authorized user misusing privileges
* Intentionally modifying production data
* Inappropriate use of 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
* Vulnerability exploit attempts
* Brute force or spaying attempts
* Phishing / Vishing 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\_INITIALS]-owned hardware, software; loss or theft of *Restricted* information. | * Lost laptop
* Lost smart phone
* Lost device or documents containing confidential [DISTRICT\_INITIALS] data
* Airport authority confiscation of [DISTRICT\_INITIALS] hardware or software
* Theft of [DISTRICT\_INITIALS] 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 information (PII)
* 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 PII 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 are easily handled by anti-virus software
* Lost laptop/smartphone, 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\_INITIALS] 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 [DISTRICT\_INITIALS] IRT directs users to notify the [DISTRICT\_INITIALS] 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.

Investigation

Once reported to the [DISTRICT\_INITIALS] IT Help 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 Chief Technology Officer/Director of IT or their designee (designee may include [DISTRICT\_INITIALS] IT 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
* Notification of [DISTRICT\_INITIALS] 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

[DISTRICT\_INITIALS]’s immediate objective after an incident has been reported and a 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\_INITIALS] IT.

Incident Response Contact List

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Title** | **Dept.** | **Role** | **Name** | **Contact Info** |
| Superintendent |   |  |  |  |
| Assistant Superintendent  |   |  |  |  |
| Assistant Superintendent |   |  |  |  |
| CTO/Director IT |  |  |  |  |
| Security Architect  |   |  |  |  |
| IT Manager |   |  |  |  |
| FBI /Local Law Enforcement |   |  |  |  |

Glossary / Definitions

|  |  |
| --- | --- |
| Term | Definition |
| Business Response Teams | Business Response Teams can be activated to enhance [DISTRICT\_INITIALS]’s response to incidents that affect specific business areas. These teams have established designated contacts for handling incidents or security breaches and enhancing collaboration between diverse groups.  |
| Cybersecurity 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\_INITIALS] 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 [DISTRICT\_INITIALS] or by a service provider acting on behalf of [DISTRICT\_INITIALS].  |
| Security Violation | An [act](http://www.businessdictionary.com/definition/act.html) that bypasses or contravenes [DISTRICT\_INITIALS]  [Information Technology Security Standards,](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. |

Appendix A: Incident Response Quick Reference Guide

Information Security Incident Response Execution Phases

1. *Preparation:*
	1. Identifying the individuals with requisite skills
	2. Establishing communication protocols
	3. Training and familiarization, tool acquisition
	4. Practice
2. *Detection:*
	1. Intelligence
	2. Identification of anomalous events
	3. Monitoring; Correlation
	4. Analysis
	5. Threat determination
	6. Impact analysis
	7. Damage assessment
3. *Activation and or Response:*
	1. Activate [DISTRICT\_INITIALS]-IRT
4. *Containment:*
	1. Minimize and stop the damage
	2. Preserve evidence
5. *Notification:*
	1. Notify individuals, entities, and or organizations per the District’s legal, regulatory, or affiliation agreement obligations.
6. *Remediation:*
	1. Remove artifacts left by attacker
	2. Verify integrity
	3. Restore data and systems
7. *Resolution:*
	1. Return systems to production
	2. Monitor
8. *After-Action Analysis:*
	1. Document findings
	2. Analyze event and response
	3. Implement improvements in system, infrastructure, and or application protection

Assessing the Suspicious Event, Machine, or Situation

Suggestions for examining a suspicious system; may help determine incident risk classification.

1. To retain attacker’s footprints, avoid taking actions that access many files or installing tools.
2. Look at system, security, and application logs for unusual events.
3. Look at network configuration details and connections; note anomalous settings, sessions, or ports.
4. Look at the list of customers for accounts that do not belong or should have been disabled.
5. Look at a listing of running processes or scheduled jobs for those that do not belong.
6. Look for unusual programs configured to run automatically at system’s start time.
7. Check ARP and DNS settings; look at contents of the hosts file for entries that do not belong.
8. Look for unusual files and verify integrity of OS and application files.
9. Use a network sniffer, if present on the system or available externally, to observe for unusual activity.
10. A rootkit might conceal the compromise from tools; trust your instincts if the system just doesn’t feel right.
11. Examine recently-reported problems, intrusion detection, and related alerts for the system.

If You Believe a Compromise is Likely

1. Immediately contact the [DISTRICT\_INITIALS] Help Center and alert your manager/supervisor who will then contact the CTO in the event that the Help Center is not available. The IR technical team will perform initial triage and call in third party resource for forensics investigation.
2. Do not panic or let others rush you; concentrate to avoid making careless mistakes.
3. If stopping an ongoing attack, unplug the system from the network; do not reboot or power down.
4. Take thorough notes to track what you observed, when, and under what circumstances.

Windows Initial System Examination Tips

Useful tools and commands when exploring a Windows OS for Normal Security Incidents:

1. Review event logs: eventvwr
2. Examine network configuration using: arp –a, netstat –nr
3. Review open ports, network connections and related details: netstat –nao, netstat –vb, net session, net use
4. Review customers and groups: lusrmgr, net users, net localgroup administrators, net group administrators
5. Review scheduled jobs: schtasks
6. Review auto-start programs: msconfig
7. Review processes: taskmgr, wmic process list full
8. Review services: net start, tasklist /svc
9. Verify DNS settings and the hosts file: ipconfig /all, ipconfig /displaydns, more %SystemRoot%\System32\Drivers\etc\hosts
10. Verify integrity of OS files: sigverif
11. Research recently-modified files: dir /a/o-d/p %SystemRoot%\System32

Windows Explorer should be avoided since it modifies useful file system details. Instead, open a command window and use command-line commands.

Linux Initial System Examination

1. Review event log files in directories (normally found in one of these, but could be located elsewhere): /var/log, /var/adm, /var/spool
2. Focus on recent security events wtmp, who, last, lastlog
3. Examine network configuration: arp –an, route print
4. Review open ports, network connections and related details: netstat –nap, lsof –i
5. Review users: more /etc/passwd
6. Review scheduled jobs: more /etc/crontab, ls /etc/cron.\*, ls /var/at/jobs
7. Check DNS settings and the hosts file: less /etc/resolv.conf, less /etc/hosts
8. Verify integrity of installed packages: rpm -Va (LinuxReview autostart services: chkconfig --list
9. Review running processes: ps aux
10. Review recently-modified files: ls –lat /, find / -mtime -2d –ls

Appendix B: Reporting and Notification Quick Start Guide

Security is everybody's job.

Employees should immediately report any suspected or confirmed information security incident to the [DISTRICT\_INITIALS] Help Center <Email and Phone #> The [DISTRICT\_INITIALS] Help Center will escalate the notification on your behalf to the CTO/Director of IT.

Once notified, the CTO/Director of IT:

1. Determines initial risk classification through initial incident analysis. The initial incident analysis considers:
	* Data risk classification
	* Number of systems, persons, accounts or data records affected
	* Functional impact, information impact, and recoverability effort of the incident
2. Activates response:
	* For Major Risk incidents, activate the [DISTRICT\_INITIALS]-IRT.
	* For Moderate Risk and Minor Risk incidents, the CTO/Director of IT determines if [DISTRICT\_INITIALS]-IRT is required. For Moderate and Minor Risk incidents, components of the [DISTRICT\_INITIALS]-IRT may be incorporated into the response, depending on the incident details.
3. CTO/Director of IT Contacts the SUPERINTENDENT to determine if and when to alert the SUPERINTENDENT's Cabinet.
4. Determines the appropriate personnel and roles.
5. Prioritizes incident response in the event of multiple simultaneous instances.

Communication Oversight

All internal communications (emails to stakeholders, campus customers, etc.) should be vetted and approved by SUPERINTENDENT, ASSISTANT SUPERINTENDENT(S) and/or PUBLIC INFORMATION OFFICER or approved designee of [DISTRICT\_INITIALS].

All external communications will be coordinated by Superintendent, Public Information Officer or approved designee. See section "External Communication" for more information.

Communicating with District Management

For major risk incidents, the CTO/Director of IT (or designee) is required to contact the District Superintendent and/or their Cabinet.

For Moderate or Minor Risk incidents, the CTO/Director of IT (or designee) may contact District Cabinet at his/her discretion, depending on the specific nature of the incident.

Managing Incident Response

Major Risk Incidents

* The CTO/Director of IT manages the overall response for Major Risk incidents or when multiple units are involved.
* The CTO/Director of IT is required to contact the or Assistant Superintendent of Human Resources/Director of Human Resources if the incident includes protected health information (PHI) or personal information.

Moderate and Minor Risk Incidents

* Depending on the nature, urgency and impact of the incident, the CTO/Director of IT may directly manage or delegate responsibility of moderate and minor risk incidents.

[DISTRICT\_INITIALS] Incident Response Team ([DISTRICT\_INITIALS]-IRT)

* CTO/Director of IT leads the [DISTRICT\_INITIALS]-IRT
* [DISTRICT\_INITIALS]-IRT is authorized to take appropriate steps to contain and remediate an incident.
* [DISTRICT\_INITIALS]-IRT is activated and leads the response for Major Risk incidents.
* [DISTRICT\_INITIALS]-IRT may be activated for Moderate or Minor Risk incidents at the discretion of the CTO/Director of IT.

Detection

1. Notify the Help Center.
2. Help Center notifies logs the incident in the ticketing system.
3. Help Center notifies CTO/Director of IT
4. CTO/Director of IT notifies Superintendent, CABINET and [DISTRICT\_INITIALS]-IRT.
5. CTO/Director of IT conducts an initial incident risk classification.
6. Local support staff begins to or continues to mitigate the incident, depending on the nature of the incident.
7. Begin documentation. Templates are available here: <https://www.sans.org/information-security-policy/?page=3>
8. Begin to develop and implement a communication plan and strategy.

Activation

1. [DISTRICT\_INITIALS]-IRT is activated for Major Risk incidents or other risk levels as deemed necessary by CTO/Director of IT and Superintendent’s Cabinet.
2. CTO/Director of IT communicates with Superintendent’ Cabinet the details of the incident and risk factors..

Containment

1. If possible, determine the cause of the incident and how the attack was executed.
2. Remove threat.
3. Take necessary steps to prevent an incident from spreading.
4. Document containment steps.

Notification

1. Notify individuals, entities, and or organizations per the District’s legal, regulatory, or affiliation agreement obligations and in keeping with the communication plan and strategy.

Remediation

1. Perform a vulnerability assessment and remediate vulnerabilities.
2. Return systems to a trusted state. For example, by re-imaging the workstation for a low-risk event or restoring the server from a known good backup.

[Close the incident response: Resume normal operations]

Resolution

1. Compare the system against the original baseline gathered during the preparation phase.
2. Business units test the service and or system to verify functionality.
3. Restore the system to the production environment.
4. Perform ongoing system monitoring to ensure system integrity and detect incident recurrence.

After-Action Analysis

1. Finalize incident response documentation, including the *After-Action Analysis* Report, and share with appropriate stakeholders as identified in the communication plan and strategy.
2. Information provided to stakeholder groups and/or individuals may vary depending on the need to know specifics of the incident.

Appendix C: Incident Questionnaire and Information Gathering

The following questions are illustrative, not exhaustive. Depending on the nature of the incident, it may be appropriate for additional questions to be considered.

Information Needed about Detection

* What is the incident type?
* What time was the incident detected?
* How was the incident detected?
* Who detected the infection?
* What is the incident machine IP address and DNS name?
* Who is the IT Support for the incident machine?
* Was a Help Ticket created? What is the ticket number?
* What time was the initial notification sent?
* Was network access disabled?
* Were people contacted? If so, who?

Information Needed from the User

* Gather the user’s contact information. User (name, email, phone #)
* What is the user’s job function?
* What is the primary function of this department? Who is the user’s manager/direct report?
* Does the user work with Category 1- Restricted Data, Category 2-Private Data, or covered PII data? If yes, what types of data?
* How much sensitive data? (# of files, GBs?, file types, location)
* What files did the user access during the time of the incident?
* Did the user work with research data? If so, what types of research data?
* How much research data (# of files, size?, file types, location)
* Does the user use District or departmental enterprise systems? If so, what level of access does the user have?
* Does the user have access to shared network storage?
* Are the shared drives automatically mounted?
* Who else shares the data in those folders?
* Did the user use encryption on files? If so, what kind(s) of encryption, and where are the keys? CTO may require access to encryption keys.

Questions about the Incident

* What was the user doing during the incident?
* Did the user notice any strange things about the computer around that time?
* Did the user receive any strange emails or open any unknown attachments?
* Did the user enter credentials (username, password) on any sites?
* Did the user install any software?
* Did the user receive any software updates?
* Did the user’s antivirus software complain or alert?
* Did the user notice a change in computer performance?
* Did the user receive any strange Instant Messages?
* Does the user use their computer for non-work related functions?
	+ If so, what function(s)? Facebook/social media? Internet Radio? Email? Banking?

Information Needed from IT Support

* IT Support contact information (name, email, phone #)
* Do they have shared drives?
* Who has access to these drives?
* What type of data is accessed or used by the system? HIPAA, FERPA, GLBA, District PII, etc.
* Are they automatically mounted?
* What types of security precautions have you placed on the system? (AV, Malware Bytes)
* Is administrative access granted to the user?
* What types of encryption are used?

Infection Details and Analysis

* IT person (name, email, phone #)
* Do they have shared drives?
* Who has access to these drives?
* Types of data (see above)
* Are they automatically mounted?
* What types of security precautions have been placed on the system?
* What type of anti-virus is used?
* Does the user have administrative access?
* Is there file-based encryption?
* What type of encryption?

Incident Analysis

* When was the first sign of an infection?
* Was this sign indicative of the initial infection?
* What is the confidence level of the initial infection notice?
* Is a copy of the malware package available?
* How long was the machine online after the first sign of an infection?
* How long before the CTO/Director of IT was notified?
* How many Command & Control (C&C or C2) servers are involved?
* Where are they located?
* How much data went to each C&C server?
* Are other devices on the network communicating with these C&C servers?
* How much data was transferred between the time of the believed initial infection and when the device was pulled off the network?
* Who were the top talkers?
* Are they legitimate top talkers?
* What other network security alerts were triggered by the device?
* How much traffic remains for the incident period after the top talkers are removed?

Appendix D: Communication Strategy and Plan Worksheet

The Chief Communication Officer/Public Information Officer serves on the [DISTICT\_INITIALS]-IRT, and is responsible for the incident response communication strategy and plan. The Chief Communication Officer/Public Information Officer works with the Superintendent’s Cabinet and CTO/Director of IT to ensure appropriate and timely messaging about the incident and the District’s response.  This worksheet helps formulate a communication strategy and plan. It is illustrative rather than exhaustive.

Communicate through channels known to be unaffected by the incident.

Potential stakeholders

* + Superintendents
	+ Assistant Superintendents
	+ CTO/IT Directors
	+ Legal Counsel
	+ Faculty, Staff, Students
	+ District / School affiliates
	+ Law enforcement agencies
	+ Technical support community
	+ Outside agencies
	+ Vendors
	+ Others

Identify authorized individuals to communicate about the incident to internal and external constituencies.

Internal communications channels

* + Email
	+ Listserv (can be event specific)
	+ Phone/video conferences
	+ Meetings
	+ Office phones
	+ Cell phones
	+ Others

External communications channels

* + Email
	+ Web
	+ Social Media
	+ Listserv (can be event specific)
	+ Phone/video conferences
	+ Meetings
	+ Office phones
	+ Cell phones
	+ Others

Schedule and frequency of communication

The plan should identify

* + Information that can be shared outside of the [DISTICT\_INITIALS]-IRT, including to what degree stakeholder groups should be provided with varying levels of information about the incident. For example, The CTO/Director of IT’s team may need technical information about the incident that the Superintendent’s Cabinet would not need.
	+ Information must be kept confidential within the [DISTICT\_INITIALS]-IRT.

Appendix E: Notification of External Organizations Involved in an Information Security Incident

It may be necessary to contact an external organization to let them know that a machine under their control may negatively impact the [DISTRICT\_INITIALS] IT systems and networks. The steps provided below are intended to guide communication.

1. Determine technical and administrative contacts of the source machine.
2. Determine WHOIS is the contact for the upstream provider, if one exists.
3. Determine if a US-CERT or “abuse” email address exists if the source machine is from a foreign country.
4. Contact [EMAIL\_ADDRESS] to see if other Districts have been attacked/scanned by the source machine.
5. Notify the County Office of Education.
6. Send a concise email to the WHOIS contact of the source machines. Include:
	* The source site’s US-CERT
	* Copy for CTO/Director of IT
	* Copy affected department(s) and personnel.
	* Log excerpts in text of e-mail. Do NOT send attachments or HTML.

**Example Email Notification:**

Subject: Potential Compromised Email Account

Dear [Organization],

I am writing to inform you that we have reason to believe that one of your email accounts may have been compromised. We have gathered evidence to support this claim, and we strongly recommend that you take immediate action to investigate and secure the account in question.

Please let us know if you need any further information or assistance from us in addressing this issue.

<Include Evidence>

Sincerely, [Your Name]

Appendix F: After-Action Analysis Report Template

Executive Summary

* Incident summary
* Indicate if compromise been contained or event mitigated

Context and Background

* Initial analysis of incident
* Investigative procedures
* Individual(s) performing investigation. Identify their roles/functional title.
* Identify forensic tools used during investigation

Findings

* Method of event detection: Monitoring, IDS, internal staff, external entity, etc.
* Identify ALL systems analyzed and why:
	+ Domain Name System (DNS) names
	+ Internet Protocol (IP) addresses
	+ Operating System (OS) version
	+ Function of system(s)
* Classification of data at risk or transaction affected
* Established cause, mechanism, and source of incident
* Start time and duration of access, if compromise
* Any data view, exported, or modified during an intrusion
* Relevant unknowns
* Risk classification potential consequences and or damage, and simple explanation
* Service disruption details and timeframes
* Remediation steps performed

Notifications Required and Performed

* Internal notifications: Senior leadership and affected individuals.
* Identify notification method.
	+ The following is a recommendation for notification:
		- If fewer than ten individuals are affected: email
		- Between ten and one hundred: email and hotline/calls to affected individuals
		- More than one hundred: to be determined by [DISTRICT\_INITIALS]-IRT
* External notifications: Law enforcement, government oversight agencies, and public
* Any notification required by law or regulation

Recommendations for Improved Security

* Review practices and compare to appropriate policy for data classification affected
* Identify gaps with respect to normal controls
* Identify compensating controls
* Document risk analysis of gaps
* Recommend controls improvements