



Incident Response Management Plan Template

5509 Baker Road, Suite 500 Minnetonka, MN 55345

[securitystudio.com](https://securitystudio.com) info@securitystudio.com

 **Table of Contents**

[**Version History**](#_r6a0le3ab8y6) **5**

[**Introduction**](#_yyibko1ws8cb) **5**

[Event Definition](#_2et92p0) 5

[Adverse Events Definition](#_tyjcwt) 5

[Incident Definition](#_3dy6vkm) 5

[Reference](#_1t3h5sf) 5

[Contact Information](#_2s8eyo1) **6**

[Roles and Responsibilities](#_3rdcrjn) **7**

[Cyber Security Incident Handling Team (IHT)](#_26in1rg) 7

[Chief Information Officer (CIO/Director of Technology & Information Services)](#_lnxbz9) 7

[Cyber Security Incident Response Team (CSIRT)](#_35nkun2) 8

[IR Commander](#_1ksv4uv) 8

[Incident Response Team Members](#_44sinio) 8

[Recorder](#_2jxsxqh) 9

[Incident Response Framework](#_3j2qqm3) **10**

[Phase I – Preparation](#_1y810tw) 10

[Phase II – Identification and Assessment](#_4i7ojhp) 10

[Phase III – Containment and Intelligence](#_2xcytpi) 10

[Phase IV – Eradication](#_1ci93xb) 10

[Phase V – Recovery](#_3whwml4) 10

[Phase VI – Lessons Learned](#_2bn6wsx) 10

[Reference](#_3as4poj) 11

[Phase I – Preparation Details](#_49x2ik5) 12

[Reporting Incidents](#_2p2csry) 12

[Phase II - Identification and Assessment](#_147n2zr) 14

[Identification](#_3o7alnk) 14

[Events versus Incidents](#_23ckvvd) 14

[Assessment](#_32hioqz) 15

[Incident Categorization](#_1hmsyys) 16

[Incident Scope](#_41mghml) 16

[Incident Impact](#_2grqrue) 16

[Key Decisions for Exiting Identification and Assessment Phase:](#_vx1227) 18

[Phase III – Containment and Intelligence](#_3fwokq0) 18

[Containment Strategies](#_1v1yuxt) 18

[Common Containment Steps](#_4f1mdlm) 19

[Engage Resources](#_2u6wntf) 19

[Preserve Evidence](#_19c6y18) 20

[Reduce Impact](#_28h4qwu) 20

[Collect Data and Increase Activity Logging](#_37m2jsg) 21

[Conduct Research](#_1mrcu09) 21

[Notify Interested Parties](#_46r0co2) 21

[Key Decisions for Exiting Containment Phase](#_2lwamvv) 21

[Investigation](#_111kx3o) 21

[Initial Cause (“Root Cause”) Investigation](#_3l18frh) 22

[Phase IV – Eradication Details](#_4k668n3) 22

[Eradication](#_2zbgiuw) 22

[Key Decisions for Exiting Eradication Phase](#_2dlolyb) 23

[Phase V – Recovery Details](#_sqyw64) 23

[Key Decisions for Exiting Recovery Phase](#_1rvwp1q) 23

[Phase VI - Lessons Learned](#_2r0uhxc) 23

[Documentation](#_3q5sasy) 24

[Lessons Learned and Remediation](#_25b2l0r) 24

[Forensic Analysis & Data Retention](#_34g0dwd) 25

[Key Decisions for Exiting Lessons Learned Phase](#_1jlao46) 25

[Notification and Communication](#_43ky6rz) **25**

[Interaction with Law Enforcement](#_2iq8gzs) 26

[Regulatory Authorities](#_3hv69ve) 26

[Stakeholders](#_1x0gk37) 26

[Public Media Handling](#_4h042r0) 26

[Plan Testing and Review](#_1baon6m) **26**

[Appendices](#_2afmg28) **27**

[Logging, Alerting, and Monitoring Activities List](#_39kk8xu) 28

[Two Minute Incident Assessment Reference](#_1opuj5n) 30

[Step 1: Understand impact/potential impact (and likelihood if not an active incident)](#_48pi1tg) 30

[Step 2: Identify suspected/potential cause(s) of the issue](#_2nusc19) 30

[Step 3: Describe recommended remediation activities](#_1302m92) 30

[Step 4: Communicate to Management](#_3mzq4wv) 30

[Pre-scripted Immediate Responses to Media Inquiries](#_45jfvxd) 33

[Pre-scripted Responses](#_2koq656) 33

[Statement Writing Tips](#_zu0gcz) 34

[Honesty](#_3jtnz0s) 34

[Context](#_1yyy98l) 34

[Framing Effect](#_4iylrwe) 34

[Partnership](#_2y3w247) 35

[Action](#_1d96cc0) 35

[Positives](#_3x8tuzt) 35

[Empathy](#_2ce457m) 35

[Be Concise](#_rjefff) 35

[Statements Should Avoid](#_3bj1y38) 36

[Formal Email and/or Letter Template](#_4anzqyu) 37

[Stolen credentials](#_243i4a2) 39

[Containment](#_j8sehv) 39

[Investigation](#_338fx5o) 39

[Eradication and Recovery](#_1idq7dh) 39

[Ransomware](#_42ddq1a) 39

[Containment](#_2hio093) 39

[Eradication & Recovery](#_wnyagw) 40

[Virus Outbreak](#_3gnlt4p) 40

[Containment](#_1vsw3ci) 40

[Eradication & Recovery](#_4fsjm0b) 40

#

# Version History

|  |  |  |  |
| --- | --- | --- | --- |
| **Revision** | **Date** | **Name** | **Description** |
| 1.0 | 2/4/2021 |  | Initial draft |
|  |  |  |  |
|  |  |  |  |

# Introduction

The ***[District]*** Incident Response Management Plan has been developed to provide direction and focus to the handling of information security incidents that adversely affect ***[District]*** **Information Resources**. The ***[District]*** Incident Response Management Plan applies to any person or entity charged by the ***[District]*** Incident Response Commander with a response to information security-related incidents at the organization, and specifically those incidents that affect ***[District]*** **Information Resources**.

The purpose of the Incident Response Management Plan is to allow ***[District]*** to respond quickly and appropriately to information security incidents.

#### Event Definition

Any observable occurrence in a system, network, environment, process, workflow, or personnel. Events may or may not be negative in nature.

#### Adverse Events Definition

Events with a negative consequence. This plan only applies to adverse events that are computer security-related, not those caused by natural disasters, power failures, etc.

#### Incident Definition

A violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices that jeopardizes the confidentiality, integrity, or availability of information resources or operations. A security incident may have one or more of the following characteristics:

1. Violation of an explicit or implied ***[District]*** security policy
2. Attempts to gain unauthorized access to a ***[District]*** Information Resource
3. Denial of service to a ***[District]*** Information Resource
4. Unauthorized use of ***[District]*** Information Resources
5. Unauthorized modification of ***[District]*** information
6. Loss of ***[District]*** Confidential or Protected information

#### Reference

* Blue Team Handbook: Incident Response Edition, Don Murdoch
* [NIST SP800-61r2: Computer Security Incident Handling Guide](https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf)

# Contact Information

*Linked from and maintained within IR/DR Contacts/Call Tree*

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Name, Title** | **Mobile** | **Office** | **Email(s)** | **IR** | **IR Handling Team** | **IR Response Team** | **IR Escalation** |
| Director, Technology & Information Services |  |  |  | A01 | Chief Information OfficerIR Commander | Chief Information OfficerIR Commander | 1 |
| Network Infrastructure Manager |  |  |  | A02 | Network Infrastructure Lead | IR Response Team Member | 1 |
| Network Systems Administrator |  |  |  | A03 | Network Systems Lead | IR Response Team Member | 1 |
| Information Systems Manager |  |  |  | A04 | Information Systems Lead | IR Response Team Member | 1 |
| Support Supervisor |  |  |  | A05 | Building Network Support | IR Response Team Member | 1 |
| Support Supervisor |  |  |  | A06 | Building Network Support | IR Response Team Member | 1 |
| vCISO |  |  |  | A07 | vCISO | IR Response Team MembervCISO security support | 2 |
| Incident Response |  |  |  | A08 | Forensics Support | IR Response Team MemberIR Retainer | 2 |
| Superintendent |  |  |  | B01 |  |  | 3 |
| Communications Director |  |  |  | B02 | Primary communications |  | 3 |
| Principal for Technology |  |  |  | B03 |  |  | 3 |
| Principal for Technology |  |  |  | B04 |  |  | 3 |
| District Attorneys |  |  |  | C01 |  |  | 3 |
| Asst. Supt. Staff Services |  |  |  | B05 |  |  | 3 |
| Director, Physical Plant & Operations |  |  |  | C02 | Physical infrastructure |  | 3 |
| Business Manager |  |  |  | C03 |  |  | 3 |
| School Resource Officer (SRO) |  |  |  | C04 |  |  | 3 |
| Law Enforcement |  |  |  | C05 |  |  | 3 |
| Cyber Insurance |  |  |  | C06 |  |  | 3 |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |

\*Escalation level determines the order in which notification should occur:

1. Notify first, required on all incidents
2. Required on all moderate or high-severity incidents
3. Involve as needed

# Roles and Responsibilities

## Cyber Security Incident Handling Team (IHT)

* Consists of senior leadership, department managers, and legal experts that may be consulted or notified during incident response.
* Advise on incident response activities relevant to their area of expertise.
* Maintain a general understanding of the Plan and policies of the organization.
* Ensure incident response activities are in accordance with legal, contractual, and regulatory requirements.
* Participate in tests of the incident response plan and procedures.
* Responsible for internal and external communications pertaining to cybersecurity incidents.

## Chief Information Officer (CIO/Director of Technology & Information Services)

* Seek approval from District Leadership for the administration of the Incident Response Program.
* Coordinate response activities with auxiliary departments and external resources as needed to minimize damages to information resources.
* Provide updates on response activities to Incident Handling Team (IHT) and other stakeholders during an incident.
* Ensure service level agreements with service providers clearly define expectations of the organization and the service provider in relation to incident response.
* Ensure policies related to incident management accurately represent the goals of the organization.
* Review the Cyber Security Incident Response Plan (“the Plan”) to ensure that it meets policy objectives and accurately reflects the goals of the organization. Seek Plan approval from IHT.
* Work with the IR Commander to periodically evaluate the effectiveness of the Plan and CSIRT.
* Ensure CSIRT managers are given the necessary authority to seize assets and stop services quickly to contain a moderate or critical-severity incident.
* Approve close of moderate or critical-severity incidents.
* Ensure Cyber Insurance is maintained as necessary and appropriate stakeholders are informed. (See Appendix IX)
* Ensure lessons learned are applied/weighed based on risk for Severity 1 incidents.

## Cyber Security Incident Response Team (CSIRT)

The CSIRT is composed of IT management and experienced personnel. The role of the CSIRT is to promptly handle an incident so that containment, investigation, and recovery can occur quickly. Where third-party services are leveraged, ensure they are engaged as necessary.

Roles within the CSIRT include:

### IR Commander

The incident response manager oversees and prioritizes actions during the detection, analysis, and containment of an incident. They are also responsible for conveying the special requirements of high severity incidents to the rest of the organization as well as communicating potential impact to the CIO. Additionally, they are responsible for understanding the SLAs in place with third parties, and the role third parties may play in specific response scenarios.

Further responsibilities:

* Act as a liaison for all communications to and from the CIO.
* Assemble a Cyber Security Incident Response Team (CSIRT).
* Ensure personnel tasked with incident response responsibilities are trained and knowledgeable on how to respond to incidents.
* Update Plan and procedures as needed based on results from testing, incident response lessons learned, industry developments, and best practices.
* Review the Plan and procedures at least annually.
* Initiate tests of the Plan and procedures at least annually.
* Ensure team activities comply with legal and industry requirements for incident response procedures.
* Act as the primary Incident Response Manager, responsible for declaring a cybersecurity incident, managing team response activities, and approving close of Severity 2 & 3 incidents.
* Be aware of Cyber Insurance Policies, contact mechanisms, and when to include providers. (See Appendix IX)

### Incident Response Team Members

The Incident Response Manager is supported by a team of technical staff that works directly with the affected information systems to research the time, location, and details of an incident. Team members are typically composed of subject matter experts (SMEs), senior-level IT staff, third parties, outsourced security, or forensic partners.

Further responsibilities:

* Assist in incident response as requested. CSIRT responsibilities should take priority over normal duties.
* Understand the [DISTRICT] incident response plan and procedures to appropriately respond to an incident.
* Continue to develop skills for incident response management.
* Ensure tools are properly configured and managed to alert on security incidents/events.
* Analyze network traffic for signs of denial of service, distributed denial of service, or other external attacks.
* Review log files of critical systems for unusual activity.
* Monitor core applications and services for signs of attack.
* Collect pertinent information regarding incidents at the request of the IR Commander.
* Consult with qualified information security staff for advice when needed.
* Ensure evidence gathering, chain of custody and preservation is appropriate.
* Participate in tests of the incident response plan and procedures.
* Be knowledgeable of service level agreements with service providers in relation to incident response.

### Recorder

The Incident Response Manager may assign a team member to begin formal documentation of the incident.

**Table 1: [DISTRICT] CSIRT Team Members**

*Linked from and maintained within IR/DR Contacts/Call Tree*

|  |  |  |
| --- | --- | --- |
| **IR** | **Name, Title** | **IR Handling Team** |
| A01 | Director, Technology & Information Services | Chief Information OfficerIR Commander |
| A02 | Network Infrastructure Manager | Network Infrastructure Lead |
| A03 | Network Systems Administrator | Network Systems Lead |
| A04 | Information Systems Manager | Information Systems Lead |
| A05 | Network Support Supervisor | Building Network Support |
| A06 | Network Support Supervisor | Building Network Support |
| A07 | vCISO | vCISO |
| A08 | Incident Response | Forensics Support |
| B02 | Communications Director | Primary communications |
| C02 | Director, Physical Plant & Operations | Physical infrastructure |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

# Incident Response Framework

[DISTRICT] recognizes that, despite reasonable and competent efforts to protect **Information Resources**, a breach or other loss of information is possible. The organization must make reasonable efforts and act competently to respond to a potential incident in a way that reduces the loss of information and potential harm to customers, partners, and the organization itself.

Developing a well-defined incident response framework is critical to an effective incident response plan. The [DISTRICT] incident response framework comprises **six phases** that ensure a consistent and systematic approach.

### Phase I – Preparation

It is essential to establish a Cyber Security Incident Response Team (CSIRT), define appropriate lines of communication, articulate services necessary to support response activities, and procure the necessary tools. (See Phase I – Preparation Details)

### Phase II – Identification and Assessment

Identifying an event and conducting an assessment should be performed to confirm the existence of an incident. The assessment should include determining the scope, impact, and extent of the damage caused by the incident. In the event of possible legal action, digital evidence will be preserved, and forensic analysis may be conducted consistent with legislative and legal requirements. (See Phase II - Identification and Assessment)

### Phase III – Containment and Intelligence

Containment of the incident is necessary to minimize and isolate the damage caused. Steps must be taken to ensure that the scope of the incident does not spread to include other systems and Information Resources. Root cause analysis is required prior to moving beyond the Containment phase and may require expertise from outside parties. (See Phase III – Containment and Intelligence)

### Phase IV – Eradication

Eradication requires the removal or addressing of all components and symptoms of the incident. Further, validation must be performed to ensure the incident does not reoccur. (See Phase IV – Eradication Details)

### Phase V – Recovery

Recovery involves the steps required to restore data and systems to a healthy working state allowing core operations to be returned.

### Phase VI – Lessons Learned

The Lessons Learned phase includes post-incident analysis on the system(s) that were impacted by the incident and other potentially vulnerable systems. Lessons learned from the incident are communicated to executive management and action plans are developed to improve future incident management practices and reduce risk exposure.



**Figure 1:PICERL Framework Model**

#### Reference

* [SANS PICERL Incident Response Model](https://www.sans.org/reading-room/whitepapers/incident/incident-handlers-handbook-33901)

## Phase I – Preparation Details

The Preparation phase is easily the most important and often overlooked phase. Without proper preparation incident response activities may be disorganized, expensive, and could cause irreparable harm to [DISTRICT]. Tasks included in the Preparation phase include but are not limited to the following.

* Establish Cyber Security Incident Handling Team (IHT) and Cyber Security Incident Response Team (CSIRT).
* Ensure appropriate parties are aware of incident reporting processes. (See Reporting Incidents)
* Document and share cyber insurance details with appropriate parties. (See Appendix IX)
* Validate Logging, Alerting, and Monitoring policy compliance.
* Ensure CSIRT receives appropriate training based on skill gap analysis, career development efforts, and skill retention needs.
* Ensure CSIRT has access to the tools and equipment needed based on estimated ROI and the organization’s risk appetite.
* Define and document standard operating procedures and workflows for both IHT and CSIRT.
* Improve documentation, checklists, references, etc.
* Maintain and validate Network Diagrams and Asset Inventories.
* Review Penetration Test reports and validates remediations to findings.
* Review Vulnerability Management reports and validate remediation efforts.
* Establish disposable and disabled Administrative credentials to be enabled and used for investigations.

Finally, it should be noted that Phase I is continuous or at least cyclical as incidents are brought to conclusion.

### Reporting Incidents

Effective ways for both internal and outside parties to report incidents is equally critical as sometimes users of [DISTRICT] systems and information may be the first to observe a problem. Review the different types of incidents addressed in Phase II under *Incident Categorization* and list or establish reporting methods for a variety of incident types.

**Table 2: Incident Reporting Guide**

|  |  |  |  |
| --- | --- | --- | --- |
| **Incident Type** | **Reporting Method** | **MTTD** | **MTTR** |
| *Fill in the table below based on the criteria to the right* | *How are we made aware that an incident is occurring?* | *Mean time to discovery (MTTD)* | *Mean time to response (MTTR)Find, Investigate, and Address* |
| Data theft, breach, corruption, or unauthorized distribution | Phone, email, in-person, alert |  |  |
| Email Phishing/Spoofing | Phone, email, in-person, alert,  |  |  |
| Privilege escalation |  |  |  |
| Physical access breach | Security alarms, in-person |  |  |
| Network sniffing, or other unauthorized reconnaissance | Firewall alerts |  |  |
| Ransomware | Phone (avoid computer use), in-person |  |  |
| Service disruption, e.g. Denial of service attack | Phone, email, traffic alert, in-person, personal observation |  |  |
| Theft or the loss of device | Phone, email, in-person |  |  |
| Unauthorized attempted or successful access to critical network infrastructure | Firewall alerts |  |  |
| Unauthorized attempted or successful access to a computer, system, or data | Phone, email, alert, in-person, personal observation |  |  |
| Video conferencing disruption | Phone, email, traffic alert, in-person |  |  |
| Violation of an explicit or implied [DISTRICT] security policy | Phone, email, in-person |  |  |
| Virus or worm infection, spyware, or other types of malware | Phone, email, alert, in-person |  |  |
| Website defacement, data modification, or exposure | Phone, email, alert, in-person, personal observation |  |  |
| Involuntary termination | Notification from HR |  |  |

##

## Phase II - Identification and Assessment

## Identification

When a [DISTRICT] employee or external party notices a suspicious anomaly in data, a system, or the network, or a system alert generates an event, Security Operations, Help Desk, or CSIRT must perform an initial investigation and verification of the event.

#### Events versus Incidents

As defined above, events are observed changes in the normal behavior of the system, environment, process, workflow, or personnel. Incidents are events that indicate a possible compromise of security or non-compliance with the [DISTRICT] policy that negatively impacts (or may negatively impact) the organization.

To facilitate the task of identification of an incident, the following is a list of typical symptoms of security incidents, which may include any or all of the following:

1. Email or phone notification from an intrusion detection tool.
2. Suspicious entries in system or network accounting, or logs.
3. Discrepancies between logs.
4. Repetitive unsuccessful login attempts within a short time interval.
5. Unexplained new user accounts.
6. Unexplained new files or unfamiliar file names.
7. Unexplained modifications to file lengths and/or dates, especially in system files.
8. Unexplained attempts to write to system files or changes in system files.
9. Unexplained modification or deletion of data.
10. Denial/disruption of service or inability of one or more users to log in to an account.
11. System crashes.
12. Poor system performance of dedicated servers.
13. Operation of a program or sniffer device used to capture network traffic.
14. Unusual time of usage (e.g. users log in during unusual times)
15. Unusual system resource consumption. (High CPU usage)
16. The last logon (or usage) for a user account does not correspond to the actual last time the user used the account.
17. Unusual usage patterns (e.g. a user account associated with a user in Finance is being used to login to an HR database).
18. Unauthorized changes to user permission or access.

Although there is no single symptom to conclusively prove that a security incident has taken place, observing one or more of these symptoms should prompt an observer to investigate more closely. Do not spend too much time with the initial identification of an incident as this will be further qualified in the containment phase.

***NOTE: Compromised systems should be disconnected from the network rather than powered off. Powering off a compromised system could lead to loss of data, information, or evidence required for a forensic investigation later. ONLY power off the system if it cannot be disconnected from the wired and wireless networks completely.***

### Assessment

Once a potential incident has been identified, part or all of the CSIRT will be activated by the IR Commander to investigate the situation. The assessment will determine the category, scope, and potential impact of the incident. The CSIRT should work quickly to analyze and validate each incident, following the process outlined below, and documenting each step taken.

**The 2 Minute Incident Assessment, found in Appendix II, should be leveraged to rapidly determine if further investigation is necessary.** Further, it can be modified and used to report the incident to appropriate leadership as required.

The Incident Response Manager will assign a team member to be “Recorder” to begin formal documentation of the incident. The below-determined categorization, scope, and impact must be included with documentation of the incident.

#### Incident Categorization

The [MITRE ATT & CK Framework](https://attack.mitre.org/) is a globally accessible knowledge base of adversary tactics and techniques and should be leveraged when categorizing security incidents. While many techniques may be used in a single incident, select the method that was primarily leveraged by the adversary. Some examples of this may be:

|  |  |
| --- | --- |
| * Phishing
* Unsecured Credentials
* Network Sniffing
* Man-in-the-Middle
* Data Destruction
* OS Credential Dumping
* Event-Triggered Execution
 | * Account Creation
* Disk Wipe
* Network Denial of Service
* Resource Hijacking
* Defacement
* File and Directory Permissions Modification
 |

It should be noted that the MITRE ATT & CK Framework may not address some situations, specifically those without malicious intent, that trigger the Incident Response Management Plan. The following exceptions may require categories of their own as dictated by the organization’s Risk Management entities or policies:

|  |  |
| --- | --- |
| * Data Loss
* Administrative Errors
* Unsecured Credentials
* Data Destruction
* Lax File and Directory Permissions
 | * Account Creation
* Disk Wipe
* Network Denial of Service
* Resource Misuse (non-malicious)
* Others as needed
 |

#### Incident Scope

Determining the scope will help the CSIRT understand the potential impact of the incident. The following are some of the factors to consider when determining the scope:

* How many systems or users are affected by this incident?
* Is Confidential or Protected information involved?
* What is/was the entry point for the incident (e.g., Internet, network, physical)?
* What is the potential damage caused by the incident?
* What is the estimated time to recover from the incident?
* What resources are required to manage the situation?
* How could the assessment be performed most effectively?

#### Incident Impact

Once the categorization and scope of an incident have been determined, the potential impact of the incident must be agreed upon. The severity of the incident will dictate the course of action to be taken in order to provide a resolution; however, in all instances, an incident report must be completed and reviewed by the Incident Response Commander. Functional and informational impacts are defined with initial response activity below:

|  |  |  |
| --- | --- | --- |
| Functional Impact | Definition | CSIRT Response |
| None | No effect on the organization’s ability to provide all services to all users. | Create a ticket and assign it for remediation. |
| Limited | Minimal effect: the organization can still provide all critical services to all users but has lost efficiency. | Create a ticket and assign it for remediation,notify the CIO and IHT. |
| Moderate | The organization has lost the ability to provide a critical service to a subset of system users. | Initiate full CSIRT, involve the CIO and IHT |
| Critical | The organization is no longer able to provide some critical services to any user. | Initiate full CSIRT, CIO, and IHT. Consider activation of the Disaster Recovery Plan. |

|  |  |  |
| --- | --- | --- |
| Informational Impact | Definition | CSIRT Response |
| None | No information was accessed, exfiltrated, changed, deleted, or otherwise compromised. | No action required |
| Limited | Public or non-sensitive data was accessed, exfiltrated, changed, deleted, or otherwise compromised. | Notify the data owners to determine the appropriate course of action. |
| Moderate | Internal Information was accessed, exfiltrated, changed, deleted, or otherwise compromised. | Notify the CIO and IHT. CIO will work with management, legal, and data owners to determine the appropriate course of action. |
| Critical | Protected Data was accessed, exfiltrated, changed, deleted, or otherwise compromised. | Notify the CIO and IHT. CIO will work with legal to determine whether reportable and the appropriate notification requirements. |

All incidents must be logged in the **Incident Handling Log & Assessment Tool**. A record of all action taken to remediate the incident, including chain of custody records, and deviations from SOP must be included in the documentation.

The Response Level table below will help determine the severity of the incident and the urgency of response activities.

|  |  |
| --- | --- |
| **Response Level Classification** | **Informational Impact** |
| **None** | **Limited** | **Moderate** | **Critical** |
| **Functional Impact** | **None** | N/A | Sev. 3 | Sev. 2 | Sev. 1 |
| **Limited** | Sev. 3 | Sev. 3 | Sev. 2 | Sev. 1 |
| **Moderate** | Sev. 2 | Sev. 2 | Sev. 2 | Sev. 1 |
| **Critical** | Sev. 1 | Sev. 1 | Sev. 1 | Sev. 1 |

The severity level should be used to determine how rapidly initial response activities should occur.

|  |  |
| --- | --- |
| **Severity Level** | **SLA** |
| Sev. 3 | Within three days |
| Sev. 2 | Within 24 hours |
| Sev. 1 | Within 2 hours |



### Key Decisions for Exiting Identification and Assessment Phase:

* If the Identification and Assessment process has determined the event constitutes a real incident, the IR process must be continued.
* All details in the Identification phase must be documented in the Incident Reporting Form if the event is determined to be an incident.

## Phase III – Containment and Intelligence

The objective of the containment phase of the incident response is to regain control of the situation and limit the extent of the damage. To achieve this objective, [DISTRICT] has defined a number of containment strategies relevant to a variety of incident types. Reference the procedures related to one or more of the Containment Strategies listed below.

### Containment Strategies

Use the list of strategies below to choose the procedure(s) most appropriate for the situation. Full procedures for each of the strategies listed below can be found in Appendix VIII. If none of these strategies match the current situation, refer to ***Common Containment Steps*** listed below.

* Stolen credentials – disable account credentials, reset all active connections, review user activity, reverse changes, increase alerting, harden from future attacks.
* Ransomware – isolate the impacted system, validate the ransomware claim, contact the insurance carrier, identify whether additional systems have been impacted, and isolate as needed.
* If DOS/DDOS - control WAN/ISP.
* Virus outbreak – contains LAN/system.
* Data loss – review user activity, implement data breach response procedures.
* Website defacement – repair site, harden from future attacks.
* Compromised API – review changes made, repair API, harden from future attacks.

### Common Containment Steps

Containment requires critical decision-making related to the nature of the incident. The Incident Response Manager, in coordination with the Incident Response Commander and other members of Executive Management, should review all the containment steps listed below to formulate a strategy to contain and limit damages resulting from the incident.

All attempts to contain the threat must consider every effort to minimize the impact on district operations. Third-party resources or interested parties may need to be notified. Where law enforcement may become involved, efforts must be made to preserve the integrity of relevant forensic or log data and maintain a clear chain of custody. Where evidence cannot be properly maintained due to containment efforts, the introduced discrepancy must be documented.

When evaluating containment steps, consider the following:

* Enable disposable Administrative accounts for use during the investigation and reset associated passwords if believed to have been at risk of compromise while being used. (See Phase I – Preparation Details)
* Will the ability to provide critical services be impacted? How? For how long?
* When should the Cyber insurance carrier be notified? (See Contact Information)
* Is a legal investigation or other action likely? Does evidence need to be preserved? (See Preserve Evidence)
* How likely is the containment step to succeed? What is the end result, full containment or partial?
* What resources are required to support the containment activity?
* What is the potential damage to equipment and other resources?
* What is the expected duration of the solution? (temporary, short-term, long-term, or permanent)
* Should IR team members act discretely to attempt to hide their activities from the attacker?
* Is the assistance of a third party required? What is the expected response time?
* Do interested parties (customers, partners, investors) need to be notified? If so, when? (see Appendix IV)
* Does the impact on [DISTRICT] equipment, network, or facilities necessitate the activation of the Disaster Recovery Plan?
* Does the data impacted include protected data such as cardholder data? If yes, refer to Notification Requirements.

#### Engage Resources

The CSIRT should select the option based on the severity of the incident, the damage incurred by [DISTRICT], and legal considerations.

|  |  |  |  |
| --- | --- | --- | --- |
|  | **In-house investigation** | **Law enforcement** | **Private forensic specialist** |
| **Time Response** | Quick response | Varies by area and agency | Quick response |
| **Competency** | Skills vary | Depends on local law enforcement | Highly skilled, often with a law enforcement background |
| **Preservation of evidence** | Does not ensure evidence integrity | Preserve evidence integrity and present evidence in court | Preserve evidence integrity and present evidence in court |
| **Reputation impact** | Minimal effect | The potential loss of reputation if certain incidents reach public | The potential loss of reputation if certain incidents reach public |

#### Preserve Evidence

***NOTE: If there is strong reason to believe that a criminal or civil proceeding is likely, the [DISTRICT] Chain of Custody form must be used any time evidence has been taken into custody, or custody is transferred for the purpose of investigation.***

Consult legal counsel regarding applicable laws and regulations related to evidence collection and preservation. Create a detailed log for all evidence collected, including:

* Identification information (e.g. serial number, model, hostname, MAC address, IP address, or another identifier).
* Name and contact information for all individuals who have handled the evidence during the investigation.
* Date and time of each transfer or handling of the evidence.
* List of all locations where the evidence was stored.
* Deviations from SOP and associated justifications.

Follow guidance from NIST SP 800-86, *Guide to Integrating Forensic Techniques into Incident Response,* when preserving evidence.

#### Reduce Impact

Depending on the type of incident, the team must act quickly to reduce the impact on affected systems and/or reduce the reach of the attacker. Actions may include, but are not limited to the following:

* Stop the attacker using access controls (disabling accounts, resetting active connections, changing passwords, implementing router ACLs or firewall rules, etc.).
* Isolate compromised systems from the network.
* Avoid changing volatile state data or system state data early on.
* Identify critical external systems that must remain operational (e.g. email, client application, DNS) and deny all other activity.
* Maintain a low profile, if possible, to avoid alerting an attacker that you are aware of their presence or giving them an opportunity to learn the CSIRT’s tactics, techniques, or procedures.
* To the extent possible, consider preservation of system state for further investigation or use as evidence.

#### Collect Data and Increase Activity Logging

Increase monitoring and packet capture on affected systems while the CSIRT investigates the scope and impact of the incident. Continue increased logging and monitoring as you move onto the Eradication and Recovery phases.

* Enable full packet capture.
* Collect and review systems, networks, and other relevant logs.
* Create a memory image of impacted systems.
* Take a forensic image of affected systems.
* Monitor possible attacker communication channels.

#### Conduct Research

Performing an Internet search, employing internal log investigation tools, consulting third-party resources, and/or consulting an IT Insurance carrier using the apparent symptoms and other information related to the incident you are experiencing may lead to more information on the attack. For example, if the insurance carrier has received multiple reports of similar incidents, or if a mailing list message contains the same IP or text of the message you received.

#### Notify Interested Parties

Once an incident has been identified, determine if there are others who need to be notified, both internal (e.g. human resources, legal, finance, communications, building leadership, etc.) and external (e.g. service providers, local government, media relations, parents, the general public, etc.). Always follow the “need to know” principle in all communications. Most importantly, remain factual and avoid speculation. See Notify Interested Parties for more detail.

Depending on the degree of sensitivity of the incident, it may be necessary for Legal/Management to require employees to sign NDAs for those who need to be involved.

### Key Decisions for Exiting Containment Phase

* The attacker’s ability to affect the network has been effectively controlled/stopped.
* The affected system(s) are identified.
* Compromised systems volatile data collected, memory image collected, and disks are imaged for analysis.

### Investigation

As the CSIRT works to contain, eradicate, and recover from the incident, the investigation will be ongoing. As the investigation proceeds, you may find that the incident is not fully contained, eradicated, or recovered. If that is the situation, it may be necessary to revisit earlier phases (see Figure 1:PICERL Framework Model). The Containment, Eradication, and Recovery phases are frequently cyclical.

The investigation attempts to fully identify all systems, services, and data impacted by the incident, including root cause analysis, which helps to determine the entry point of an attacker or weakness in the system that allowed the event to escalate into an incident.

A third party may need to be contacted if the investigation is beyond the skills of the CSIRT, impacted systems are owned by a Cloud Service Provider, or forensic analysis is required.

### Initial Cause (“Root Cause”) Investigation

The investigation should be conducted with consideration given to the ongoing impact on critical operations. Ideally, the Initial Cause Investigation should be concluded before leaving the Eradication phase. At times, however, it may be necessary or appropriate to continue investigation during or after eradication and recovery. Delaying the Investigation should only be considered when the CSIRT is confident that the incident has been fully contained and the full scope of the impact is known. Delays or modifications to the scope of investigation activities must be approved by the Incident Response Commander.

The investigation techniques utilized will vary by the type of incident. The investigation may rely on some (or all) of the following:

* Interviews with witnesses and/or affected persons.
* Capturing images, snapshots, or memory dumps of affected systems.
* Obtaining relevant documents.
* Conducting observations.
* Taking photographs of physical locations.
* Reviewing security camera footage.
* Analyzing the logs of the various devices, technologies, and hosts involved (e.g. firewall, router, anti-virus, intrusion detection, host).
* Reviewing email rules (compromised email account).
* Compare the compromised system to a known good copy.
* Anomaly detection/behavior monitoring (compare to pre-established baseline).

## Phase IV – Eradication Details

The Eradication consists of the full elimination of all components of the incident.

### Eradication

***NOTE: The specific administrative tools on a compromised host could be altered versions of the originals. Use a separate set of administrative tools (e.g. boot disk) than those on a compromised host for investigation whenever possible.***

Steps to eradicate components of the incident may include:

* Disable breached user accounts.
* Reset any active sessions for breached accounts.
* Identify and mitigate vulnerabilities leveraged by the attacker.
* Close unnecessary open ports.
* Increase authentication security measures (implement MFA, add geolocation restrictions).
* Increase security logging, alerting, and monitoring.
* Clean installation of affected operating systems and applications.

All re-installed operating systems and applications must be installed according to [DISTRICT] system build standards, including but not limited to:

1. Applying all the latest security patches.
2. Disabling all unnecessary services.
3. Installing anti-virus software.
4. Applying [DISTRICT] hardened system configuration baselines.
5. Changing all account passwords (including domain, user, and service accounts).

NOTE: It may be possible to restore the system without the need to perform a full clean installation. IT personnel, at the direction of the CSIRT, will make this determination.

### Key Decisions for Exiting Eradication Phase

* Has the root cause been identified and identified vulnerabilities have been remediated?
* Have all impacted accounts, including CSIRT burner credentials been reset?
* CSIRT is confident that the network and systems are configured to eliminate a repeat occurrence.
* There is no evidence of repeat events or incidents.
* Sign-off from IR Manager for limited-severity incidents or CIO for moderate and critical-severity incidents

## Phase V – Recovery Details

Prior to restoring systems to normal operation, it is critical that the CSIRT validate the system(s) to determine that eradication was successful, and the network is secure. Once the organization has been attacked successfully, the same attackers will often attack again using the same tools and techniques leveraged in the initial attack. Having gained access to the compromised system(s) or network once, the attacker has more information at their disposal to leverage in future attacks.

If feasible, the system should be installed in a test environment to determine functionality prior to re-introduction into a production environment.

Furthermore, network monitoring should be implemented for as long as necessary to detect any unauthorized access attempts.

Recovery steps may include:

* Restoring systems from a clean backup.
* Replacing corrupted data from a clean backup.
* Restoring network connections and access rules.
* Communicating with interested parties about changes related to increased security.
* Increasing network and system monitoring activities (short or long-term).
* Increasing internal communication/reporting related to monitoring.
* Engaging a third party for support in detecting or preventing future attacks.

### Key Decisions for Exiting Recovery Phase

* Have district operations been restored?

## Phase VI - Lessons Learned

The follow-up phase includes reporting and post-incident analysis on the system(s) that were the target of the incident and other potentially vulnerable systems. The objective of this phase is the continued improvement of applicable security operations, response capabilities, and procedures.

### Documentation

All details related to the incident response process must be formally documented and filed for easy reference. The following items must be maintained, whenever possible:

1. All system events (audit records, logs).
2. All actions that were taken (including the date and time that an action is performed).
3. All external conversations.
4. Investigator Notes compiled.
5. Any deviations from SOP and justifications.

An incident report, documenting the following will be written by the CSIRT at the end of the response exercise:

1. A description of the exact sequence of events.
2. The method of discovery.
3. Preventative measures put in place.
4. Assessment to determine whether recovery was sufficient and what other recommendations should be considered.

The objective of the report is to identify potential areas of improvement in the incident handling and reporting procedures. Hence, the review of the report by district leadership should be documented, together with the lessons learned, to improve on the identified areas and used as a reference for future incidents.

### Lessons Learned and Remediation

The CSIRT will meet with relevant parties (technical staff, management, vendors, security team, etc.) to discuss and incorporate lessons learned from the incident to mitigate the risk of future incidents. Based on an understanding of the root cause, steps will be taken to strengthen and improve [DISTRICT] information systems, policies, procedures, safeguards, and/or training as necessary. Where mitigations or proposed changes are rejected, a Risk Acceptance Process must be followed. Incidents should be analyzed to look for trends and corrective action should be considered where appropriate.

Lessons Learned discussion should cover:

* Review of discovery and handling of the incident(s).
* How well staff and management performed and whether documented procedures were followed.
* Review of actions that slowed or hindered recovery efforts.
* Proposed improvements to future response and communication efforts.
* Recommendations to increase the speed of future detection and response efforts.
* Recommendations for long and short-term remediation efforts.

At the end of Lessons Learned meetings, some sort of remediation needs to occur, either resolving the issues, installing compensating controls, or at a minimum formally assessing and accepting the risk. Recommendations for long and short-term remediation efforts must be added to the overall treatment plan.

Updates to the incident response procedures should also be considered and incorporated where areas of improvement are found.

Voluntary information sharing should occur whenever possible with external stakeholders to achieve broader cybersecurity situational awareness (InfraGard, MS-ISAC, etc.). Legal and Management must be consulted before doing so if a formal Information Sharing policy and process do not exist.

### Forensic Analysis & Data Retention

In the event of possible legal action, the forensic analysis will ensue in such a manner as to preserve digital evidence consistent with legislative and legal requirements. Outside legal counsel and forensic experts may be required.

Consider the following when deciding whether and for how long to retain evidence related to the incident:

* Prosecution – is it likely that the attacker will be prosecuted? If so, evidence may need to be retained for multiple years.
* Reoccurrence – consider whether the evidence collected may be useful in case the attacker or a similar attack should occur in the future.
* Data Retention Policies – Consider the contents of evidence held (such as a system image capture) and retention policies related to this data (e.g. email retention policy).
* Cost – Depending on the type and amount of data or equipment preserved as evidence, the cost may be a limiting factor.

### Key Decisions for Exiting Lessons Learned Phase

* Management is satisfied that the incident is closed.
	+ IR Manager makes the decision for limited-severity incidents. CIO makes the decision for moderate and critical-severity incidents.
* There is an action plan to respond to operational issues that arose from this incident. At this point, it is time to return to the Preparation Phase (See Figure 1:PICERL Framework Model).

# Notification and Communication

Required notification and communication both internally and with third parties (parents, staff, students, community members, vendors, law enforcement, etc.) based on legal, regulatory, and contractual requirements must take place in a timely manner.

* The Incident Response Commander must report the incident to the senior leadership.
* The senior leadership must report any potential breaches and/or incidents involving district data to the Incident Handling Team (IHT) promptly.
* The IHT is responsible for appropriate notification to:
	+ Personnel.
	+ Affected stakeholders and/or partners (within 48 hours, based on SLA, based on legal or regulatory compliance, whichever is shorter).
	+ Local, state, or federal law officials as required by applicable statutes and/or regulations.

### Interaction with Law Enforcement

Interaction between law enforcement and emergency services personnel should be coordinated by the Incident Response Commander. The Incident Response Commander will manage ongoing communication with authorities. It must be noted however that Law Enforcement’s priorities are eventual prosecution of offenders and not necessarily returning the District to a functional state. Ensure Legal is consulted and provides direction before and while communicating with Law Enforcement.

### Regulatory Authorities

* [DISTRICT] is subject to various regulatory oversight, depending on the data impacted. If there is the potential that regulated data were breached, it may be necessary to notify various authorities. (See Appendix IV).
* Depending upon the nature of the breach it may be required to contact other governmental regulators.
* Only members of the IHT are permitted to discuss the nature and/or details of an incident with any regulatory agencies.
* The IHT should contact regulators as soon as practical. (See Appendix IV)

### Stakeholders

* All stakeholders who are affected by the incident must be notified according to applicable contract language, service level agreements (SLAs), applicable laws and statutes, and/or regulations.
* Communications with stakeholders must be consistent, with the same or similar message delivered to each. The message sent to stakeholders will be created by members of the Communications Team.

### Public Media Handling

All Information concerning an incident is to be considered **confidential** and at no time should any information be discussed with anyone outside of [DISTRICT] without the approval of executive management and our legal counsel.

The process of making public or media statements must be carefully managed to ensure that any investigation/legal proceedings are not jeopardized, and reputational damage is minimized. The superintendent and/or [DISTRICT] communications team must be alerted to inquiries from the media; they will coordinate a response and/or designate a spokesperson, depending on the inquiry.

It is critical that all communications only flow through the [DISTRICT] communications team. Employees found to be discussing incidents with stakeholders, the general public, or media members without approval from executive management/legal counsel may be subject to disciplinary action.

Refer to Appendix V for guidance in communicating with the Media.

# Plan Testing and Review

The [DISTRICT] Incident Response Plan and procedures must be tested at least annually. The IR Commander will conduct training using a scheduled simulated incident to guide and test procedures. (Refer to [*NIST SP 800-61r2*](https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf)*, Appendix A—Incident Handling Scenarios* for test scenarios) The plan and procedures will be updated to reflect lessons learned and to incorporate any new industry developments.

CSIRT members, the CIO, and members of the IHT must participate in test exercises at least annually.

The Incident Response Plan and procedures are reviewed no less than annually and updates are tracked in the version history on page 1.

Plan review should include:

* Review supporting documents and forms listed in Supporting Document List (Appendix X) to ensure they are accurate and effective.
* Review Appendices to ensure they are accurate and effective.
* Review completed Incident Reporting Forms and corrective action plans for the recommended plan and procedure updates.
* Compare recent changes to the organization’s infrastructure and management structure to documented plans and procedures.

# Appendices

Index of Appendices

* Logging, Alerting, and Monitoring Activities List
* Two Minute Incident Assessment Reference
* Incident Response Checklist
* Notification Requirements
* Media Statements
* Customer Letter Template
* Incident Response Organizations
* Containment Strategies
* Cyber Insurance and Third-Party Service Agreements
* Supporting Document List

## Logging, Alerting, and Monitoring Activities List

Logging, alerting, and monitoring activities may target individual systems or a range of activities across multiple systems and applications. Keep a list of logging, alerting, and monitoring activities and review the list regularly to ensure that technicians can respond to abnormal events quickly. If you have a managed asset inventory these activities may be added to the existing list.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **System/Application Name** | **Logging System** | **Events Logged**  | **System Owner** | **Monitoring frequency** | **Alerting** |
|  | None | ISP Maintenance Notifications | TIS Director | When alerts are received | Automated email/   |
|  | Local  | Wireless Network Authentications/ ISE Node performance issues/ License and certificate Notifications | Infrastructure Manager | Daily/When alerts are received | Automated email/  |
|  | Local | DDoS monitoring and mitigation service  | TIS Director | When alerts are received | Automated email/  |
|  | None | Internet, District WAN Provider - Maintenance Notifications | TIS Director | When alerts are received | Automated email/  |
| Google Workspace | Cloud | Google drive, email, apps, user suspicious activity, phishing, leaked passwords, | TIS Director | Daily/ When alerts are received | Automated email/ |
|  | Local  | Administrator Authentication, System Discovery/availability, Disk/storage events, Invalid sign-In Attempts, Warranty Notifications,  | Network Administrator | Weekly | Automated email/  |
|  | Local | Email phishing notifications | Network Administrator | Monthly/When alerts are received | Automated email/  |
|  | Local | Malware, PII leaving organization, externally shared files | TIS Director | When alerts are received | Automated email/  |
| AD |  |  |  |  |  |
| Firewall | Local  | Critical Threat Alerts | Infrastructure Manager | When alerts are received | Automated email/ |
| Monitor | Local | System Availability/Health | Infrastructure Manager | When alerts are received | Automated email/ |
|  | Local | Vulnerability scanner | Infrastructure Manager | When alerts are received | Automated email/ |
|  | Local | Vendor Connections | Infrastructure Manager | When alerts are received | Automated email/ |
|  | Local | Event monitoring and alerting. Log analysis  | Network Administrator | When alerts are received | Automated email/  |
|  |  |  |  |  |  |

## Two Minute Incident Assessment Reference

### Step 1: Understand impact/potential impact (and likelihood if not an active incident)

* What is the value of the asset? If not significant, why react?
* Roughly quantify the potential worst-case impact.
* Include rough estimates of the likelihood of experiencing this impact.

### Step 2: Identify suspected/potential cause(s) of the issue

* Any and all possible scenarios should be considered.
* Quickly eliminate those that can be proven incorrect.
* Share most likely scenarios when communicating.

### Step 3: Describe recommended remediation activities

* How do you close the hole/stop the bleeding?
* Include any steps that could reduce the experienced impact.
* Don’t forget about reputation damage and legal expectations.

### Step 4: Communicate to Management

* Describe the issue at a high level. (what and how it happened)
* Explain what it means to the district. (learning continuity, data privacy, financial, reputation, etc.)
* Share short-term actions needed to move the risk from critical/high to something more acceptable.

|  |  |
| --- | --- |
| **Value of the Asset****(H/M/L)** | An example of high might be access to the full district database vs. low might be a proprietary internal process document with limited IP. |
| **Potential Impact** | What would the loss or felt impact be if the incident were real and fully realized? Try to quantify into both $ and impact like reputation or legal liability. |
| **Likelihood of Impact** | Immediate risk (internet accessible cataloged trivial vulnerability to exploit) of not likely known and complex (requires sophisticated expertise and specific circumstances to exploit) |
| **Suspected causes (list all potential causes that should be investigated)** | Configuration error, the remote vulnerability exploited, lost device, targeted denial of service by the political or financially motivated party (DDOS to cover up a fraud), etc. |
| **Most likely cause(s)** | These sources should be quickly pursued to prove correct or incorrect. |
| **Recommended Remediation Short-term** | Turn off the internet, remove servers from external access, implement a patch or configuration change, communicate issues to employees, parents, or students, etc. |
| **Long-term Actions** | Change in a process, or architecture, acquisition of tools or systems to reduce the risk to an acceptable level over the long term. |
| **Communication** |  |
| **Describe the Issue in simple terms** | Describe the problem within a school district context if possible. Examples are useful to illustrate the issue in operational terms. |
| **Explain the “So What” factor** | Why is this important to our district? What could it cost us if we fail to act? |
| **Suggested Immediate Actions** | Propose specific responses and why we should take them. What will take that action provide the district with regards to reduced impact or liability? There may be more than one potential path. If there are viable options, they should be presented for decision-making. |
| **Other Proposed Remediation** | Are there follow-on risks that require additional action? Examples are communication strategy, user awareness activities, process changes, systems/tools enhancements or implementations (long-term actions) |

1. **Incident Response Checklist**

Refer to the Incident Response Form in (Location).

|  |  |  |
| --- | --- | --- |
| **No.** | **Description** | **Remarks** |
|  | **Preparation Phase (IR Commander)** |  |
| 1 | Prepare contact list and disseminate to relevant parties |  |
|  | **Identification (IT Support)** |  |
| 2 | Complete sections 1 and 2 of the Incident Response Form |  |
|  | **Assessment (CSIRT)** |  |
| 3 | Complete sections 3 – 5 of the Incident Response Form |  |
| 4 | Notify relevant parties. |  |
|  | **Containment (CSIRT/Support)** |  |
| 5 | Perform system backup to maintain the current state of the system |  |
| 6 | Change local passwords for the affected system(s) |  |
|  | **Eradication (CSIRT/Support)** |  |
| 7 | Do not use the system administration tools. Use separate administrative toolsets for investigation. |  |
| 8 | Re-install a clean operating system |  |
| 9 | Harden the operating system (e.g. apply patches, disable unnecessary services, install anti-virus software, etc.) |  |
|  | **Recovery (CSIRT/Support)** |  |
| 10 | Validate that the system has been hardened |  |
| 11 | Restore system data with clean backup |  |
| 12 | Put the affected system(s) under network surveillance for future unauthorized attempts |  |
|  | **Follow-up (IR Commander)** |  |
| 13 | Perform post-mortem analysis on the affected system(s) to identify (potential) vulnerable areas |  |
| 14 | Submit an Incident Response Report for management review |  |
| 15 | File all documentation on the incident response process for future reference |  |

1. **Notification Requirements**

*List all requirements that apply to the organization*

|  |  |  |  |
| --- | --- | --- | --- |
| **Requirement** | **Clients Impacted** | **Notification Timing**  | **Notes** |
| [GDPR](https://gdpr-info.eu/art-33-gdpr/) | Parents, Students, Staff | 72 hours after becoming aware of a breach | Applicable for foreign exchange students in attendance |
| State Law |  |  |  |
| Privacy Law |  |  |  |

**Media Statements**

Below are sample statements to use if members of the media call before a press release is issued. ***All communications with the media should be directed to the Incident Response Commander or other representative designated by executive management.*** Getting the facts correct is a priority. Do not give information to the media before confirming facts with internal personnel and management. Changing information after it is released can lead to media confusion and loss of focus on the key messages.

### Pre-scripted Immediate Responses to Media Inquiries

Use this template if the media is “at your door” and you need time to assemble the facts for the initial press release statement.

Getting the facts is a priority. It is important that [DISTRICT] not give in to pressure to confirm or release information before you have confirmation.

The following responses give you the necessary time to collect the facts.

### Pre-scripted Responses

**If on the phone to the media:**

* “We’ve just learned about the [situation, incident, event] and are trying to get more complete information now. How can I reach you when I have more information?”
* “All our efforts are directed at [bringing the situation under control]. I’m not going to speculate about [the situation]. How can I reach you when I have more information?”
* “I’m not the authority on this subject. Let me have [name] call you right back.”
* “We’re preparing a statement now. Can I get back to you in about [number of minutes or hours]?”
* “You may check our website for background information, and I will fax/e-mail you with the time of our next update.”

**If in-person at the incident site or in front of a press meeting:**

* This is an evolving [situation, incident, event], and I know you want as much information as possible right now. While we work to get your questions answered, I want to tell you what we can confirm right now:
* At approximately [time], a [brief description of what happened].
* At this point, we do not know [how long the advisory will last, how many people are affected, etc.].
* We have a [system, plan, procedure, operation] in place. We are being assisted by [local officials, experts, our legal team] as part of that plan.
* The situation is [under, not yet under] control. We are working with [local, state, federal] authorities to [correct this situation, determine how this happened].
* We will continue to gather information and release it to you as soon as possible. I will be back to you within [amount of time in minutes or hours] to give you an update. As soon as we have confirmed information, it will be provided.
* We ask for your patience as we respond to this [situation, incident, event].

### Statement Writing Tips

The following information/tips can be used to create a good media statement.  Not all of them need to be included, but typically two or three will ensure an effective statement.

#### Honesty

If [DISTRICT] is at fault, admit it.  By attempting to deflect responsibility, journalists and the public will be far less forgiving when the details around the incident are exposed and the District is found wanting. Even in a real crisis, you can gain respect for holding your hands up.

If it is not your fault, you need to make it very clear without overtly blaming any other individual or organization.

* Words to use: take or share responsibility, committed to openness, transparent.
* Words not to use: blame, fault.

#### Context

Presenting negatives in a broad context can go a long way to minimizing the impact of the bad news.

If the story is about a user who has had a bad experience, you can refer to the many other users who have had good experiences.  This is where external advocates are useful – particularly other users.

Broadening context also means isolating the incident – simply a case of stating that the negative incident is ‘very rare’/’isolated’ and placing it within a wider, more positive framework.

* Words to use: very rare, isolated.
* Words not to use: frequent mistakes, another error.

#### Framing Effect

A Framing Effect is a form of cognitive bias, which causes people to prefer positive-sounding statements over negative ones, despite otherwise being logically identical. For example, when discussing a risky surgery, patients will be a lot more likely to go through with surgery when it is explained that “the odds of survival one month after surgery is 90%” as opposed to “mortality within one month of surgery is 10%” despite both statements equating to the same amount of risk. Be aware of this form of cognitive bias when developing and delivering messages to the public.

#### Partnership

There are occasions when it is useful to subtly remind a critical audience that you are not solely responsible for the conduct of a particular individual. This can be achieved without it appearing as if you are ‘buck-passing’ or absolving yourselves of responsibility and without upsetting relations with other key partners.

For example, you may simply state that ‘as one of a number of organizations involved in supporting the individual concerned, you are ‘committed to providing the best possible service for service users in the area’.

* Word to use: working together, joint responsibility, as one of a number of organizations.
* Words not to use: X is to blame, we don’t know what others think of this but.

#### Action

Media statements should not merely talk about the problem; they should stress action on the part of the organization.

You will not improve any media situation if you are seen to be passive in the case of a negative situation or media crisis.

A word of caution: avoid saying you will be holding an ‘investigation’/’inquiry’ in the case. These words are headline fodder for the media and can imply guilt.

* Words to use: taking immediate action, taking appropriate measures, working closely with.
* Words not to use: we are holding an investigation, we will look into it.

#### Positives

Don’t be afraid to point out how successful your organization is in any media statement.  Mistakes happen and emphasizing the positive things you’ve done can help people see past minor blips.

* Words to use: we have seen positive results, we have been successful in, we will continue to provide the best service
* Words not to use: there are a number of areas we need to work on (unless you accompany that with a positive statement e.g. that you will be taking measures to change this).

#### Empathy

Negative media situations obviously create a gap between you and the public involved. Expressions of empathy can help bridge the gap.

* Words to use: we understand, we appreciate, we know, we recognize.
* Words not to use: these things happen, everyone faces these issues.

#### Be Concise

Journalists are typically not interested in lengthy statements – they would prefer to spend the effort on details of the event/incident. Further, if the person speaking with the media is not accustomed to doing so, lengthy statements may result in the speaker making an error.

As a rule, statements for printed media should be no more than two paragraphs long – one tight sentence per paragraph.

Broadcast media may give you more space, but you should still bear length in mind as the producer/editor may be looking to produce a shortened version of your statement to drop into a later news bulletin.

#### Statements Should Avoid

* **Confrontation** - the objective of media statements in a crisis is to diffuse the situation – not make it worse. Avoid blaming/buck-passing because it will simply result in a media-based argument between opposing parties – remember journalists love confrontational stories. e.g. ‘They were wrong’, ‘it is not our fault’…
* **Ambiguity** - weak, ambiguous statements have no place in handling negative media situations and can leave room for the journalist to re-interpret your response. Be robust and clear at all times. Use strong positive words e.g. ‘we are committed to X and will not tolerate Y’. Make sure your statement is completely unambiguous.
* **Personal pronouns** - try and avoid referring to your organization by name in your media statement as doing this could reinforce the link between your organization and the negative issue concerned. You may simply use the first-person plural (‘we’/’us’). This also has the advantage of adding a slightly personal and less bureaucratic feel to the statement.
1. **Stakeholder Letter Template**

### Formal Email and/or Letter Template

Dear [DISTRICT] Parent,

As you may be aware, [DISTRICT] has announced that it experienced a criminal intrusion into a portion of its computer network.  This criminal intrusion may have resulted in the theft of student/staff information.  The district has not determined that any such data was in fact stolen by the intruder, and it has no evidence of any misuse of such data.

[DISTRICT] is providing this notice out of an abundance of caution to all of its stakeholders.  **YOUR INFORMATION IS NOT NECESSARILY AFFECTED**.

[DISTRICT] believes that the potentially impacted systems were breached during the period of <insert date> through <insert date>.

Upon recognition of the intrusion, [DISTRICT] took immediate steps to secure the affected part of its network.  An investigation supported by third-party data forensics experts is going on to understand the nature and scope of the incident.  [DISTRICT] believes the intrusion has been contained.  [DISTRICT] currently has no reason to believe that additional information beyond that described above was stolen by the intruder.  However, given the continuing nature of this investigation, it is possible that time frames, location, and/or at-risk data in addition to those described above will be identified in the future.

The District has notified law enforcement authorities and is cooperating in their efforts to investigate this intrusion and identify those responsible for the intrusion.  The press release and this letter have not been delayed as a result of this law enforcement investigation.

Should you have questions, you may contact [DISTRICT] at xxx-xxx-xxxx or xxxxx@[District]

Thank you and regret any inconvenience that this may cause you.

Sincerely,

<insert name and title>

Possible other considerations to include depending on the nature of the incident

* Provide free credit reports ([www.annualcreditreport.com](http://www.annualcreditreport.com/) or 1-877-322-8228)
* Fraud Alerts – Equifax ([www.equifax.com](http://www.equifax.com/) or 1-877-478-7625), Experian ([www.experian.com](http://www.experian.com/) or 1-888-397-3742), TransUnion Fraud Victim Assistance Division ([www.transunion.com](http://www.transunion.com/) or 1-800-680-7289)

**Incident Response Organizations**

Below is a list of incident response organizations that may be useful in planning for or responding to an incident:

|  |  |
| --- | --- |
| Organization | URL |
| Anti-Phishing Working Group (APWG) | <https://www.antiphishing.org/> |
| CERT Coordination Center | <https://www.sei.cmu.edu/about/divisions/cert/index.cfm> |
| Computer Crime and Intellectual Property Section (CCIPS), US Department of Justice | <https://www.justice.gov/criminal-ccips> |
|  [DISTRICT] ’s Incident Response Provider |  |
| Government Forum of Incident Response and Security Teams (GFIRST) | <https://www.us-cert.gov/government-users/collaboration/gfirst> |
| High Technology Crime Investigation Association (HTCIA) | <https://htcia.org/> |
| InfraGard | <https://www.infragard.org/> |
| Internet Store Center (ISC) | <https://isc.sans.edu/> |
| National Council of ISACs | <https://www.nationalisacs.org/> |
| United States Computer Emergency Response Team (US-CERT) | <https://www.us-cert.gov/> |

1. **Containment Strategies**

The following containment strategies have been defined to assist in incident response. If none of the containment strategies outlined below fit the current situation refer to Phase III – Containment*:* Common Containment Steps.

### *Stolen credentials*

#### Containment

Reduce Impact:

* Change the password or disable affected accounts
* Disable and re-enable MFA
* If the compromised account had administrator access review activity logs for additional accounts that may have been created.
* Disable any accounts created by the attacker.

Notify Interested Parties:

* Check with VCISO at this point
* Notify the users responsible for the impacted accounts

#### Investigation

* Attempt to determine the date and time that the account was compromised
* Review all activities completed by the compromised account during the period of compromise. If logs do not exist, check all configurations the account has access to modify. (e.g. for a compromised email account, check for added or changed forwarding rules)
* Check [Have I Been Pwned](https://haveibeenpwned.com/) for email address

#### Eradication and Recovery

* Reverse changes made by the compromised account during the time of compromise

### *Ransomware*

#### Containment

1. *Isolate and disconnect network segment*
2. *Call VCISO*
3. *Identify and block access to command and control (C2) servers (the bad guy server)*
4. *Set file shares into read-only mode*
5. *Check ownership of encrypted files to determine infected users*
6. *Recall known phishing emails from user mailboxes*
7. *Take infected systems offline*
	1. *Disconnect, do not power off*

***If unable to contain, call IR Provider***

#### Eradication & Recovery

1. *Call IR Provider for current information and potential assistance*
2. *Patch third-party applications as soon as possible*
3. *Test and validate backup processes*
4. *Deploy GPO to block executables and disable macros*
5. *Block email attachments based on file signature and/or extension*
6. *Remove local administrative rights*

### *Virus Outbreak*

#### Containment

1. *Update antivirus software*
	1. *Obtain detection signature and technical description for the virus from AV vendor*
	2. *Test detection signature update provide in a test environment*
	3. *Distribute fix to environment*
2. *Submit sample file to AV vendor if latest virus signature does not detect the infection*
	1. *Offline infected device*

#### Eradication & Recovery

1. *Eradicate the virus, if necessary*
	1. *Contain virus/attack (depending on virus this could include partitioning the network, disabling SMTP email, changing content filtering to block attachments or specific strings of text, removing workstations from the network, etc.)*
	2. *Identify infected systems*
2. *Environment cleanup:* (**scan and patch stuff)**
	1. Obtain the detection signature and any required fix tools for the virus from your antivirus vendor.
	2. Test the fix provided by your vendor for the virus in your virus signatures staging lab. This may include separate repair tools that you need to run before using the updated virus signatures.
	3. Develop a deployment methodology for the fix process.
	4. Create a cleanup plan and validate it with all affected teams and your antivirus vendor.
	5. Clean all infected perimeter and email servers and update the virus signatures of the antivirus software providing protection of these avenues of infection.
	6. Distribute the fix to all the workstations and servers in your environment using whatever method you have in place for rapid deployment.
	7. Isolate systems that are infected and require repair.
	8. Run all required fix tools on all infected systems in order to remove the virus from memory or disable it.
	9. Scan all systems with the updated virus signatures to remove all infected files.
	10. Eliminate all temporary and suspicious files, including hidden directories and files.
	11. Remove or alter configuration information used for the functionality of the virus or that might allow the virus to reappear.
	12. Remove configuration information that may cause system failures.
	13. Search for newly mounted partitions created by the virus and eliminate them.
	14. Search for missing log partitions and restore.
	15. Search for added or altered user accounts and remove or restore them.
	16. Restore changed or deleted files.
	17. Distribute patch updates to all systems and update patch levels

***New Scenario - Student Caused Event (process differently because it’s a student - add these specifics)***

Password stolen and used

Browser redirects

Bitcoin mining

DDoS

Ransomware

Access and manipulation of PA, HVAC, alarms, cameras, etc.

***New Scenario - Staff Caused Event***

Misuse of permissions - data, students

Malicious intent - ransomware, spyware, etc.

1. Cyber Insurance and Third-Party Service Agreements

Where Cyber Insurance or Third-Party Services are involved, having a clear understanding of their incident response and detection services is essential. For example, many cyber insurance carriers require the organizations they cover to follow a predefined process. Examples of third-party service providers that may be involved in IR activities include insurance providers, internet service providers (ISP), cloud service providers (CSP), software vendors, or multi-service providers (MSP).

The CIO is responsible for reviewing all SLAs with service providers to ensure that responsibilities and expectations are defined in relation to incident response.

IR Commanders are responsible for understanding SLAs with service providers and knowing when the team should engage the service provider.

**Table 3: THIRD-PARTY Support and Response**

|  |  |  |  |
| --- | --- | --- | --- |
| **Service Provider** | **Applications/Services** | **When to contact** | **Service Level/Response Time** |
|  | IR Services | As soon as we suspect an incident has occurred |  |
|  |  |  |  |
|  |  |  |  |

**Table 4: Insurance Coverage and Contact Information**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Insurance Provider** | **Limits** | **Term Dates** | **When to contact** | **Contact Information** |
|  | $2,000,000 |  | As soon as we confirm need |  |

*\*Additional coverage sub-limits may apply per claim.*

Find a copy of the Insurance Declaration pages [here]. Direct questions about insurance coverage limits to the Risk Manager. Notify the Risk Manager to activate the insurance plan.

1. **Supporting Document List**
* Incident Management Policy – Owner & Location (Incident management policy)
* Incident Assessment Form/Categorization Sheet - Owner & Location (Incident management policy)
* Incident Reporting Form - Owner & Location (Incident intake form/ reporting form) [DISTRICT]
* Chain of Custody Form - Owner & Location [DISTRICT] form
* Executive Incident Assessment Checklist – Owner & Location
* Logging Standard – Owner & Location (what is our logging standard, what are we collecting and why and how long do we retain a given set of logs)
* Customer Data Breach Report – Owner & Location (this is a premade document for notifying Students, staff, families, vendors, and others that are impacted by a data breach)
* Logging, Alerting, and Monitoring Activities List – Owner & Location (What are we collecting and alerting on? what logs are collected, what alerts do we receive, what monitoring steps and systems are we using)
* Notification Requirements (no template) - Owner & Location (this is insurance notification and State notification law, timetables for reporting)
* Relevant documented procedures (no template) – see Containment Strategies (Play books)
* Vulnerability Management Policy/Standard – Owner & Location (Vulnerability management policy)
* Risk Acceptance Policy/Process – Owner Location (Risk management policy)
* Data Classification Policy – Owner & Location (privacy related - governance doc)
https://securitystudio.com/policy-templates/information-classification-and-management-policy/