**Cyber Security Incident**

**Response Guide**

**Version 1.2**

Table of Content

1. **Introduction 4**
2. Purpose 4
3. Scope 4
4. Plan Objectives 4
5. Training, Exercise, and Maintenance 5
6. Procedures Review and Revisions 5
7. Policies and Authorities 5
8. **Situations and Assumptions 6**
9. Assumptions 6
10. **Definitions of a Computer Security Incident 7**
11. Incident Response Categories 7
12. **Concept of Operations 8**
13. Cyber Incident Source Authentication 8
14. Detecting an Incident 8
15. Investigating and Confirming an Incident 8
16. Confirming the Incident 9
17. Changes During an Incident 9
18. Response Activation 9
19. Handling and Documenting the Incident 10
20. Handling and Documenting the Evidence 10
21. Limiting Incident Exposure 10
22. Incident Handling Resources 10
23. Escalating Incident Standard Operating Guidelines 11
24. Analyzing the Event and Determining Risk 12
25. Determine Response Strategy 13
26. Collecting Forensic Evidence 14
27. Cryptographic Hashes 14
28. Duplicating a Disk for Forensic Evidence 15
29. Responding to Common Incidents 15
    1. Responding to Inappropriate Use 15
    2. Responding to Denial Of Service Attack 16
    3. Responding to Misappropriation of Data 16
    4. Responding to Theft of Information 16
    5. Responding to Computer Intrusion 17
30. Identifying and Securing the Vulnerability 17
31. Using Passive Network Monitoring 17
32. Neutralizing/ Eradication of the Threat 18
33. Restoring Service 18
34. Data Backups 18
    1. Responding to Malicious Software/Viruses 19
    2. Responding to Physical Intrusions 19
35. Formal Incident Reporting 20
36. Reporting Incidents to Employees 20
37. Reporting Incidents to Other Jurisdictions 20
38. CORA Requests 20
39. Litigation Holds and E-Discovery 20
40. Root Cause Analysis 21
41. Follow-up and After Action Reporting 21

**APPENDICES 22**

1. Checklist & Form: Documenting the Incident 23
2. Checklist & Form: Investigating & Confirming the Security Incident 24
3. Checklist & Form: Determining & Executing IRP 25
4. Checklist: Incident Commander Guide 27
5. Incident Discovery Guide 28
6. Detection Methods 33
7. Alert Levels 35
8. Resource Typing 41
9. Roles and Responsibilities Defined 52
10. Terms and Definitions 57

**ANNEX**

1. Information Technology Employee Code of Conduct 60

# Introduction (RS.RP-1)

This document is a guideline for responding to cyber security incidents. The target audience includes both technical employees and management. This guide provides a framework for efficiently handling security incidents from the discovery to the after action report. Because a security incident may impact server availability, it is essential to have this guide easily accessible to staff in both online and hard copy formats.

While this plan will be valuable to the Information Technology (IT) Director and security team, it is important to follow an expandable emergency response process based on the National Incident Management System (NIMS). NIMS provides a common nationwide approach to enable responders, leaders and the community to work together to manage all threats and hazards. NIMS applies to all incidents regardless of cause, size, location, or complexity.

This plan is consistent with the NIST Framework v1.1. Each section with applicable NIST Framework Activities has a header in parenthesis that corresponds with the NIST *Framework Core*. These activities *present key cybersecurity outcomes identified by stakeholders as helpful in managing cybersecurity risk*. For example, Section I is consistent with the outcomes of function RS.RP. Each activity within the NIST Framework is also cross-walked with additional informative references for further detailed information.

1. **Purpose**

The purpose of this plan is to accomplish a coordinated response and recovery to cyber incidents involving the information technology (IT) systems and assets of local, state, tribal, and private entities.

1. **Scope**

The scope of this plan includes incidents that may be of a purely cyber nature, or a combination of cyber and physical impacts. These include local and multijurisdictional incidents. This plan will define the organization, responsibilities, operational concepts, and actions pertaining to the response to a cyber incident.

During certain response operations, this plan may be used in conjunction with the Emergency Operations Plan, its annexes, and/or other planning documents as required.

1. **Plan Objectives**

The objective of the Incident Response Guide is to:

* Limit immediate incident impact to the jurisdiction / organization.
* Assess the scope of the attack.
* Identify trigger points for escalation within the jurisdictions.
* Determine how the incident occurred.
* Share information, including vulnerabilities, exploited to other local governments, special districts and private sector partners in the 10-county Region to mitigate further incidents.
* Find out how to avoid further exploitation of the same vulnerability.
* Avoid further damage.
* Assess the impact and damage in terms of financial impact and loss of image.
* Recover from the incident.
* Update policies, procedures, standards and guidelines as needed based upon the After Action Report.
* (Possibly) Determine who initiated the incident for possible criminal and/or civil prosecution.

# Training, Exercise, and Maintenance

Training on this plan will be completed annually by at least all IT Staff and when new IT employees are hired. The IT Department will conduct one drill annually. These exercises should focus on identifying weaknesses in process, communications, and documentation. It is vitally important to treat this document as a living document, modifying it as gaps are found or as practices change. The plan will be reviewed on an annual basis for major updates.

# 

# Procedure Review and Revision

The document will be reviewed after events such as significant security incidents and changes to organizational or technical infrastructure. At a minimum, it will be reviewed in its entirety on an annual basis and updated as necessary. Policy sections may be reviewed and changed any time. It is the IT Director’s responsibility to approve and communicate any policy changes.

*RECORD OF CHANGES:*

|  |  |  |  |
| --- | --- | --- | --- |
| **Record of Changes** | | | |
| **Page No.** | **Change Comment** | **Date of Change** | **Signature** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

1. **Policies and Authorities**

*This plan was developed for local government use in response to cyber incidents. Policies should be added for reference.* *This may include password policy, remote desktop policy, and vendor policy.*

*Authorities for response to a cyber incident should be included in one or more job descriptions of the jurisdiction.*

Additionally, authorities for response to an incident may also include policies related to all-hazard response and the activating additional authorities, including law enforcement leadership (Sheriff or police chief) and jurisdictional leadership outside the IT Department (policy leaders).

C.R.S. 24-72-204 Open Records Act

LIST OTHER POLICY REFERENCE NUMBERS FROM JURISDICTION

The National Incident Management System (NIMS) is a standardized approach to incident management developed by the Department of Homeland Security in response to Homeland Security Presidential Directive-5. Due to the unique aspects of a cyber incident, Unified Command will likely be necessary. This Cyber Security document is built on the premise that the following partners will work together to form a Command Structure to coordinate the actions necessary for rapid identification, information exchange, response, and remediation to mitigate the damage caused by a cyber event. Unified Command may include members from the following organizations.

* + 1. Police Department/Sheriff’s Office
    2. Information Technology
    3. Emergency Management
    4. Fire Department
    5. Public Works
    6. Transportation
    7. Colorado Information and Analysis Center (CIAC)
    8. Technology resources from the private and public sectors
    9. Affected Agencies
    10. Leadership/Policy Group

Cyber incidents may result in activation of a cyber emergency response team. Emergency Management may be activated to implement the Emergency Operations Plan (EOP), its annexes as necessary, and/or Continuity of Operations Plan.

Additionally, if the Emergency Operations Center (EOC) is activated, resource ordering will be requested through the EOC and based upon the incident needs. Resources are ordered and follow the EOP (Resource Mobilization Plan) as all other incidents.

1. **Situation and Assumptions (RS.RP-1)**

Large scale cyber incidents may overwhelm government and private sector resources by disrupting the Internet and/or taxing critical infrastructure information systems. Complications from disruption of this magnitude may threaten lives, property, the economy, and national security. Rapid identification, information exchange, investigation, coordinated response and remediation often mitigate the damage caused by this type of malicious cyber activity. A cyber incident may occur at any time of day with little or no warning, may cross geographical boundaries and may lack an easily identifiable signature.

1. **Assumptions**
   * 1. The IT Department recognizes applicable cyber threats and will take reasonable precautions to protect their systems.
     2. The IT Department will develop and maintain the cyber security incident response guide (this information may also be incorporated as part of their Continuity of Operations Plan (COOP).
     3. Other departments and offices within the jurisdiction will report issues to the help desk per policy and report impacts during a cyber incident.
     4. The jurisdiction will make notifications related to specific data compromise per state and federal law through the appropriate regulatory agency.
     5. Government and private sector organizations will work together collectively on cyber related issues to protecting critical infrastructure and develop plans and processes for restoring those systems in the event of a failure or compromise.
     6. IT Departments must understand their roles and responsibilities in the emergency response structure as first responders. This includes understanding NIMS and the incident command structure, the importance of a command post and planning.
     7. The typical “first responders” to an emergency may not be impacted during a cyber incident. This is dependent upon the consequences of the incident. The first responders of a cyber incident that impact the cyber environment are the IT staff. The first responders of a cyber incident that impacts the cyber and physical environment will be inclusive of all personnel managing the consequences.
     8. The response to and recovery from a cyber incident must take into account numerous existing challenges. Resources must be appropriately prioritized to resolve identified challenges. Identifiable challenges include:

* Management of Multiple Cyber Incidents:

The occurrence or threat of multiple cyber incidents may significantly affect the ability of responders to adequately manage the cyber incident. Multi-jurisdictional planning and exercises should be conducted to assist in addressing this issue.

* Availability and Security of Communications:

An infrastructure attack could impede communication needed for coordinating response and recovery efforts. A secure, reliable communications system is needed to enable public and private sector entities to coordinate efforts in the event that routine communications channels are inoperable. A redundant system of communication should be in place prior to an attack.

* Availability of Expertise and Surge Capacity:

Leadership must ensure that sufficient technical expertise is developed and maintained to address the wide range of ongoing cyber threats. Sufficient technical expertise may require in-place contracts with private sector entities that specialize in cyber incident response. In addition, the ability to surge technical and analytical capabilities in response to cyber incidents that may occur over a prolonged period must be planned for, exercised and maintained.

* Staffing to support the response is limited:

Requesting resource support from other entities will be needed. The IT Department must understand the resource ordering process including the benefits of activating the EOC.

1. **Definition of a Computer Security Incident (RS.RP) (RC.RP)**

A computer security incident, as described by NIST 800-61 Revision 2, is “a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices.” The sensitivity of this data requires that all computer security incidents be treated as if sensitive data were involved, and appropriate measures should be taken to ensure the protection of this data.

1. **Incident Response Categories**

There are generally six (6) stages of incident response:

1. **Prepare**. Through Identification and Protection Functions develop an informed cyber incident response guide.
2. **Detect**. Detect and event and identify whether or not an incident has occurred. Identification may come from security monitoring, internal notification, and/or detection methods and processes.
3. **Respond**

**-Mitigate**. Activities are performed to prevent the expansion of an event, mitigate its effects and resolve the incident.

**-Eradicate**. Removing the cause of the incident can be a difficult process. It can involve virus removal, removing user permissions, and/or dismissing employees.

1. **Recover**. Restoring a system to its normal business status is essential. Once a restore has been performed, it is also important to verify that the restore operation was successful and that systems are back to normal condition.
2. **Follow-up/Improvements**. Some incidents require considerable time and effort. Performing follow-up activity is one of the most critical activities in the response procedure. This follow-up may include updates to policies, plans, equipment and configurations.
3. **Concept of Operations (RS.RP) (RC.RP)**

This section describes conceptually, how the cyber response is implemented. Response is implemented using a formal cyber incident response process:

* + - Detect (Processes, Monitoring)
    - Respond (Communication, Analysis, Mitigation, Improvement)
    - Recover (Processes, Improvement, Communication)

1. **Cyber Incident Source Authentication (DE.AE) (DE.CM)**

It is critical that there is a mechanism to identify the authenticity of a reported cyber incident prior to committing further resources. (NIST 800-61)

* Ports, logs, and change documentation
* Documentation for Operating Systems, applications, protocols, and intrusion detection and antivirus products
* Network diagrams and lists of critical assets, such as database servers
* Current baselines of expected network, system, and application activity
* Cryptographic hashes of critical files to speed incident analysis, verification, and eradication
* Access to images of clean Operating System and application installations for restoration and recovery purposes
* Physical environment logs or other information sources

1. **Detecting an Incident (DE.DP)**

The first sign of a security incident can come from a number of different sources. A user may report a locked account to the IT Help Desk, a server administrator could notice unusual log activity, or a network administrator could notice increased bandwidth use. It is important to accept input on possible incidents from those individuals associated including employees, guests, vendors, and partners.

Incident reports from non-IT staff should be directed to the IT Help Desk. Vendors, service providers, guests, and employees should report incidents and critical vulnerabilities to the IT Help Desk. If the individual contacting the IT Help Desk doesn’t open a trouble ticket, the IT Help Desk will open one at this time. Once an incident is identified, the IT Help Desk should immediately notify the IT staff with the trouble ticket number.

Technical IT staff should bypass the IT Help Desk and directly notify the IT Director. This is an important step in reducing risk of exposure and decreasing incident response time. Other department directors may report incidents directly to the IT Director. For example, Human Resources may report inappropriate use incidents in this manner.

1. **Investigating and Confirming the Incident (RS.AN-1)**

The incident should be confirmed before taking further action within the system. Many incidents occur weeks or months before they are discovered, so a quick reaction doesn’t necessarily make a substantive difference. The damage that can be caused by reacting to a false incident is usually worse than the damage that might be caused by taking the additional time required to confirm it.

If an EOC is activated, this support organization may assist in collecting and compiling impact information across the jurisdiction and sending it to the IT Department. The IT Department and its limited staff can continue to analyze and investigate the incident.

## Confirming the Incident (RS.AN-1) (RS.CO-1) (PR.DS-6)

The goal is to determine whether an event is a threat to assets, misinterpretation, or false alarm. Facts must be discovered and documented that show an incident is happening or has happened.

If an incident cannot be confirmed within 20 minutes, then it should be escalated to the appropriate administrator or staff member. Involving an administrator may provide the expertise required to confirm the incident. Still, there may be cases where there is not enough security expertise to confidently identify an incident. In some cases, third-party services may need to be contacted to assist in validating the entire incident issue.

Ensure there is a baseline of normal system operations as this is vital to confirming an incident and should be a routine practice of the IT Department. Without an understanding of what applications, servers, and networks look like when they are healthy, it is nearly impossible to identify security problems in these entities. Documentation of expected applications, services, and users should be available to identify strange behavior rapidly.

## Changes during Incidents (RS.CO-1)

While attempting to confirm an incident, some attention should be focused on minimizing the changes made to the systems, software, and network. Any changes will affect electronic evidence and may even indicate awareness of the incident to the attacker. If there is a need to make modifications to systems or network configurations, the changes should be recorded in detail*.*

1. **Response Activation (RS.RP) (DE.DP-4)**

The alert levels developed by MS-ISAC (See Appendix Seven) allow the IT Department to assess the current situation as it evolves. Using the result from the formula, the Alert Level Indicator would generally reflect severity levels as follows: ·

**Alert Level Indicator - Severity**

o **Green - Low: -8 to -5**

o **Blue - Guarded: -4 to -2**

o **Yellow - Elevated: -1 to +2**

o **Orange - High: +3 to +5**

o **Red - Severe: +6 to +8**

The IT Director (if unavailable the senior most IT position) will notify staff of an activation to include the Emergency Management Office when a cyber incident reaches level Blue as described in Appendix Seven “Alert Levels (developed by MS-ISAC)” of this Cyber Security Incident Response Guide. This notification could simply come in the form of a short email depending on the situation. This allows Emergency Managers to evaluate what their office may need to do if the level increases.

The Emergency Operations Plan (Cyber Annex) should reference these levels to ensure consistency across these two departments.

1. **Handling and Documenting the Incident**

During a security incident it is essential to document as much information as possible. This allows other responders who may investigate the incident to follow a process and method. It is important to document any changes that are made to systems or networks.

Identify one individual to be the record keeper. Having a single position responsible for documenting the incident allows for consistent, accurate records.

A third party may be contracted to perform this duty based upon insurance contracts.

## Handling and Documenting Evidence (DE.AE-3)

Evidence may be needed to prosecute criminal activity, therefore, evidence must be documented with accurate dates, times, and individuals involved. The notes the record keeper(s) take should allow others to recreate the steps taken to confirm and respond to the incident. Proper chain of custody must be maintained. The chain of custody should document what the type of evidence, how it was collected, who has been responsible for the evidence since collection, and a process that allows for the security of the evidence. Follow current chain of custody forms used by law enforcement for electronic evidence.

## Limiting Incident Exposure (RS.MI-2)

The responsibility of limiting exposure should be controlled by the IT Director or designee to minimize several different personnel trying to resolve the situation as the same time.

The chances of someone trusted being involved are reasonably high. This may make investigation more difficult and could greatly increase the chances of alerting the attacker as a result of unusual activity. By notifying only the staff who are part of the incident handling process, the risk of alerting an attacker is greatly reduced.

At this time in the incident handling process, it may be necessary to ensure public information is strategic and controlled through the incident command structure.

# Incident Handling Resources (RS.RP) (RC.RP)

No matter how up-to-date this document is, there will be new technologies, vulnerabilities, and techniques in use in the field. Therefore, it is critical for staff to maintain ongoing awareness of new trends in technology, security, and specifically incident handling. This should kept in hard copy within the department. The following resources are considered authorities in incident handling by the community:

NIST Security Incident Handling Guide (SP 800 61)

<https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf>

SANS Incident Handling Guides

<http://www.sans.org>

MS-ISAC Resource Home Page and Contact Information for Consulting through CERT

<https://www.cisecurity.org/ms-isac/>

HSIN Registration and Login Link

<https://www.dhs.gov/homeland-security-information-network-hsin>

[https://**hsin**.dhs.gov](https://hsin.dhs.gov)

Forum of Incident Response and security teams (FIRST)

<http://www.first.org>

1. **Escalating Incident Standard Operating Guidelines: (RS.CO) (RC.RP) (RC.CO)**

The following steps outline the standard operating procedure for the jurisdiction. These are outlined in a typical order for response.

1. Help desk/IT staff receive information or discover a possible incident that needs investigating. Discovery can come from numerous sources.
2. Help desk follows internal ticketing process.
3. Through process IT Administration either confirms the Incident or the incident was determined to be a misinterpretation or false alarm. (NO FURTHER FOR MISINTERPRETATION OR FALSE ALARM)
4. Execute Incident Response Plan(s) and possibly Continuity of Operations Plans (COOP)
5. Determine if Departmental Operation Center / War Room is necessary
6. Determine if assets are threatened within the jurisdiction.
7. Identify the severity of the incident through the Incident Response Plan and form an initial incident command structure (this structure may be expanded as the incident progresses and can be modified into a unified command).
8. Notifications are made based on severity level and following the proper process.

(Documents needed to guide this procedure: Help desk Checklist, IT Staff emergency organizational structure and roles/responsibilities, Communications plan/protocol for activations (who, what, when, where, why and how), county administration policies related to cyber security)

1. IT Department may activate a team if this resource exists internally or their emergency response organizational structure. (this ensures roles and responsibilities are covered across the incident response and there is not overlap of work being accomplished or conflicting work being completed)
2. Through notifications, the IT Director or designee contacts Emergency Management. Emergency Management recommends a level of Emergency Operations Center activation based on their Emergency Operations Plan and/or Cyber Annex.
3. The IT Director or designee contacts the Public Information Officer to start coordinating the decisions and release of information (both internal and external). (Documents needed to guide this procedure is public release templates, EOC activation level triggers within the EOP or Cyber Annex, policy group coordination within the EOP, Disaster Declaration templates within the EOP, and COOP activation level and coordinating plans).
4. EOC Manager will Activate Appropriate Staff based upon internal plans (EOC operations should include triggers related to activating for a cyber incident, annex for specifics related to cyber incidents, and checklists and flow charts for EOC staff).
5. EOC Policy Group or jurisdictions’ administration (if no activated EOC) will make policy level decision as needed.
6. EOC Policy Group or IT Director (if no activated EOC) will notify Risk Management about possible insurance claim and/or services required (if the jurisdiction has cyber insurance).
7. EOC will order resources based upon the incident need following the jurisdictions resource mobilization and/ or logistics process.
8. If the incident impacts life safety at any time: the law and fire departments will be involved and the command structure should be modified.
9. The incident may activate a command post at any time. This could be the conference room in the IT Department. The command post allows leadership across departments a location to meet.
10. Planning personnel (likely Planning Section Chief in incident command structure) will ensure common incident objectives and potentially an incident action plan are developed and updated as determined by the incident. \*\*\*Ensure Cyber Annex within jurisdiction EOP outlines a command post option, incident planning, and an incident action plan.

*EXTERNAL ELEMENTS:*

\*EOC IT Liaison or IT Staff (dependent upon the response structure) should have information sharing procedures and processes for the notification laterally to other governments that may be vulnerable as well.

## Analyzing the Event and Determining Risk (PR.IP) (DE.AN) (RS.AN)

Before responding to a known security incident, the following should be answered:

* What systems and networks have been attacked?
* What data is exposed to the attacker?
* What critical systems and services are at risk?
* Will this incident directly affect customers or customer data?
* Is the incident visible to the public?

The answers to these questions come from detailed analysis of servers, network devices, desktop computers, log files, and user experience.

Specific technical steps that can be taken to analyze systems include the following:

* **Profile Networks and Systems.** Profiling includes running file integrity checking software on hosts to derive checksums for critical files and monitoring network bandwidth usage to determine what the average and peak usage levels are on various days and times.
* **Understand Normal Behaviors.** Incident response team members should study networks, systems, and applications to understand what their normal behavior is so that abnormal behavior can be recognized more easily. One way to gain this knowledge is through reviewing log entries and security alerts.
* **Log Retention Policy.** The length of time to maintain log data is dependent on several factors, including the organization’s data retention policies and the volume of data. See NIST SP 800-92, Guide to Computer Security Log Management.
* **Event Correlation.** Evidence of an incident may be captured in several logs that each contain different types of data. Correlating events among multiple indicator sources can be invaluable in validating whether a particular incident occurred.
* **Keep All Host Clocks Synchronized.** Protocols for Network Time Protocol (NTP)
* **Maintain and Use a Knowledge Base of Information.** The knowledge base should include information that staff need for referencing quickly during incident analysis. Text documents, spreadsheets, and relatively simple databases provide effective, flexible, and searchable mechanisms for sharing data among team members.
* **Internet Search Engines for Research.** Internet search engines can help analysts find information on unusual activity.
* **Run Packet Sniffers.** Sometimes the indicators do not record enough detail to permit the staff to understand what is occurring. If an incident is occurring over a network, the fastest way to collect the necessary data may be to have a packet sniffer capture network traffic. Configuring the sniffer to record traffic that matches specified criteria should keep the volume of data manageable and minimize the inadvertent capture of other information.
* **Filter the Data.** There is simply not enough time to review and analyze all the indicators; at minimum the most suspicious activity should be investigated. One effective strategy is to filter out categories of indicators that tend to be insignificant. Another filtering strategy is to show only the categories of indicators that are of the highest significance; however, this approach carries substantial risk because new malicious activity may not fall into one of the chosen indicator categories.
* **Seek Assistance from Others.** If current resources are unable to determine the full cause and nature of an incident, resource request may need to be made including contacting MS-ISAC, other teams outside jurisdiction, and US-CERT. It is important to accurately determine the cause of each incident so that it can be fully contained and the exploited vulnerabilities can be mitigated to prevent similar incidents from occurring.

When discussing risk, use four general categories of assets and consider how the confidentiality, integrity, and availability of each are threatened by this incident. The security team should fill out this table together:

|  |  |  |  |
| --- | --- | --- | --- |
|  | Confidentiality | Integrity | Availability |
| Image |  |  |  |
| Data |  |  |  |
| Customer Data |  |  |  |
| Negotiable Assets |  |  |  |

Each of these categories can be at risk; many times multiple categories are at risk at one time. Assigning general levels of risk to each asset category is a good way of concretely understand the business risk the security incident poses.

Risk levels will vary depending on the severity of the incident. When filling out the table above, a corresponding severity should be entered into the box. Severity can be broken down into three categories:

**High Severity**

* Confidential data is at risk.
* Organization-wide disruption is occurring or imminent.
* Legal ramifications are serious.
* Media/public interest will be high.

**Medium Severity**

* Internal data is at risk.
* The disruption is somewhat localized, but not organization-wide.
* Media/public interest is possible.
* Potential legal ramifications exist.

**Low Severity**

* Only public data is at risk.
* The incident is limited to a single or very few machines.
* There are no legal implications.
* Service has not been disrupted.
* No potential media/public interest exists.

It is not required that each severity condition be met in order to classify a risk as High/Medium/Low severity. Once risk to the organization has been assessed and discussed by the security team, an appropriate response can be identified and executed.

## Determining Response Strategy (RS.RP-1) (RS.CO-1) (RS.AN) (RC.RP) (RS.AN-4)

Despite the many security risks, there are relatively few decisions to make about how to respond. To determine a response strategy, the following key questions must be answered:

* How (and when) should the threat be neutralized?
* Is it more important to investigate the incident or to restore service?
* What vulnerability caused the initial exposure, and how should it be secured?
* Should evidence be gathered to attempt to pursue the attacker?
* How should service be restored?
* What entities have/should be notified, when, and by whom?

\*\*\*See Incident Discovery Guide Appendix Five

During the course of developing and implementing a response to an incident, incident responders should keep in mind these general “rules of engagement”:

* Report all issues/incidents to the IT Director or designee for tracking and escalation.
* Include corresponding trouble tickets for all issues/incidents with existing tickets.
* Provide a comprehensive timeline of findings and actions associated with problem activities. This will be used with a chain of custody report
* Base all incident responses on issue/incident priority using established risk categories.

1. **Collecting Forensic Evidence (RS.RP)**

All of the information collected during an incident, from initial detection to resolution, may be useful as forensic evidence. However, some incidents warrant collecting forensic evidence with the specific intent of being able to use that evidence to support legal action. There are situations that will typically require that forensic evidence collection take place:

* Incidents that represent a serious risk
* Incidents that may result in employee termination or other disciplinary action
* Incidents where a root cause cannot be identified, and a system must be restored before analysis can be completed
* Incidents that require outside investigation in connection with other cases.

\*Ensure the use of chain of custody documentation when appropriate (contact law enforcement for jurisdictional updated chain of custody form)

The following three sections describe strategies for collecting digital evidence in such a manner that it can be reliably used in a court of law. If collecting this evidence requires the assistance of a third party, such as access logs from a connecting ISP, a search warrant or subpoena may be required. This is because many ISPs do not keep this type of information indefinitely and acquiring a subpoena or search warrant takes time, a retention letter can be sent to the third party requesting it hold the information until a search warrant can be acquired. Although the third party may legally disregard this request, it can prove beneficial. The first section briefly discusses cryptographic hashes and how they should be used to ensure the integrity of digital evidence.

The second section discusses the making of forensic copies of entire disks. This process is preferred for most serious security incidents. It preserves all the files and programs on a system, as well as files that have been recently deleted. It provides the most information for later analysis and is essential for completeness.

Unfortunately, making forensic copies of disks is a resource-intensive process that requires a great deal of evidence storage space and takes a significant amount of time and technical skill to accomplish. An alternative is to make only copies of specific files or directories. This strategy is used primarily for collecting evidence of inappropriate use, although it can also be appropriate for gathering evidence associated with a limited intrusion (such as copyrighted files illicitly stored on an anonymous FTP server).

Third-party service providers may be contacted to assist with evidence collection and preservation.

<https://resources.infosecinstitute.com/computer-forensics-tools/#gref>

## Cryptographic Hashes

A hash (or digest) is a small representation of a large set of data. Hashing algorithms are intended to produce unique hash values for unique large sets of data and modern cryptographic hashing algorithms come close enough to accomplishing this for the court of law. A record of the hash of a file provides a method of proving that the file was not tampered with. This is essential for using data files, log files, or any other electronic evidence in court.

MD5 and SHA-256 are both suitable hashing algorithms for generating cryptographic hashes of evidence. While there are collision attacks on the MD5 algorithm, these do not invalidate the use of the algorithm for evidence integrity verification purposes. Depending on the platform and available tools, it may not always be possible to use a particular algorithm, and so two are noted as acceptable.

There are a variety of tools that can be used to generate cryptographic hashes using these algorithms.

* Windows: The File Checksum Integrity Verifier (FCIV) can be used to generate MD5 or SHA-256 hashes, and can operate in a single file or recursive mode. <https://support.microsoft.com/en-us/help/841290/availability-and-description-of-the-file-checksum-integrity-verifier-u>
* Mac OS X: OpenSSL is deployed by default with current versions of OS X. File hashes can be computed using “openssl sha256 <filename>” or “openssl md5 <filename>.”
* Linux: Typical Linux distributions include the tools md5sum and sha256sum, which can be used to generate hashes based on the respective algorithm in the name.
* File hashes should be stored on paper and attributed to a labeled (logical or physical) image.

## Duplicating a Disk for Forensic Evidence

There are a number of techniques to duplicate a disk for forensic purposes, including sending an image of the evidence drive across the network, moving an evidence drive to a forensics workstation, and installing a forensics drive into the evidence machine. Each is effective and useful in different situations. The incident response staff should consult with a qualified, experienced expert before undertaking any disk duplication forensics activity. Regardless of the duplication strategy chosen, the main ideas to keep in mind are the following:

* + Do not boot the system if the systems is turned off disk you are trying to duplicate for evidence.
  + Keep accurate records of what steps are taken, including serial numbers of drives and image hashes.
  + Create a hash of the system.

In the event that evidence must be replicated and delivered to an external party such as an attorney, it is important that the integrity of the copy/deliverable be verified. Cryptographic hashes must be verified for any electronic copies that are created.

**K. Responding to Common Incidents (RS.RP) (RS.CO) (RS.AN) (RS.MI)**

## Responding to Inappropriate Use

Inappropriate use typically involves a trusted user who is involved in an activity not permitted by security, code of conduct, or inappropriate use policies. (See Annex A for template Employee Code of Conduct that includes an Inappropriate Use policy)

If an employee is suspected of violating the Acceptable Use Policy, collect evidence about the action. All investigations of this nature must be initiated and supervised by the IT Director or designee. Evidence can include log files, email messages, network traffic, or any other information that implicates the individual.

Before choosing this strategy, have a high degree of confidence that the inappropriate use was not due to a computer intrusion. If it is suspected to be computer intrusion, the incident response staff may create a full forensic duplicate of the evidence machine as described previously.

Inappropriate use can usually be associated with a specific application or file type. Typically, it is related to image files, copyrighted music or applications, Web browsing, or email. By identifying the application or file type associated with the incident, it is possible to gather only relevant information, making for a faster, simpler investigation.

Files should be collected in a similar manner to the disk images discussed above. Either the files should be sent across the network to a secure location, or they should be locally copied to a portable disk (USB hard drive or zip drive). Ideally, all evidence files should be burned to a CD as soon as possible. Practice good evidence handling and documentation so this data can be used to support HR disciplinary action. It is particularly important to make and record hashes of all evidence as it is collected.

1. **Responding to a Denial-of-Service Attack**

A denial-of-service (DoS) attack involves an attacker using many Internet computers to send gigantic amounts of information toward a single target computer. That computer is overwhelmed with traffic and even the fastest servers are unable to handle the load.

DoS attacks are directed intentionally to one computer network at a time. This indicates that one or more individuals are spending effort to harm the system. DoS attacks can be mitigated through a few key strategies:

* + Verify the type of Denial-of-Service attack
    - Volume Base Attacks
    - Protocol Attacks
    - Application Layer Attacks
  + Depending type of attack, tracing back to origin can assist in determining optimal filtering locations
  + Enable backup links
  + Changing of IP addressing
  + Reconfigure the firewall to help manage the attack
  + Reconfigure upstream routers to block or divert the attack
  + Talk to upstream providers, such as your hosting provider or ISP

At least two of the three strategies must be employed to handle a serious DoS attack. The last one requires the cooperation of the Internet Service Provider. Internet Service Provider 24/7 contacts are essential.

ISP’s or Upstream providers may assist in tracing the attack back to the origin, this would allow notifying the owners of compromised systems.

## Responding to the Misappropriation of Data

The misappropriation of data typically involves sensitive information that is, whether accidental or not, sent from a secure location to a non-secure destination or unauthorized party. This type of incident can also cover any inadvertent access or data loss via unplanned means. Any such event is typically difficult to detect and will likely be reported by an internal individual.

When discovered, investigators should immediately document the exact situation, including what information was leaked, to whom it was sent, whether it is still available, what process led to the breakdown, and what customers may be affected. Multiple parties will need this data to resolve the situation, including:

* + Legal – to assess contract requirements in regards to leaked customer information.
  + System Administrator – to process changes.
  + IT Director – for notifications.

1. **Responding to Theft of Information**

Theft of information always results from some other security failure. The failure could be technical, such as an attacker breaking into an unpatched or misconfigured server, or it could be human, such as a disloyal employee that posts payroll information to a public mailing list. Ideally, theft of information can be detected when it occurs. Systems administrators may notice irregular use of a server or network, or an IDS may detect a violation of use policy. However, theft of information is often detected when it is discovered that a third party has the information against policy. In the worst case, confidential information may appear on the Internet somewhere. Should this happen, incident response staff need to review logs and systems to try and identify how the information was taken. This process can require significant effort, so it should be balanced with the sensitivity of the stolen data.

It is very important to collect evidence in the most responsible and well-documented manner possible. Where possible, forensic evidence collection practices, described later in this document, should be used to gather evidence.

## Responding to a Computer Intrusion

A computer intrusion could lead to interruption of services, corruption of data, or even theft of information. Handling a computer intrusion is done in three steps: identification and vulnerabilities, neutralizing the threat, and restoring service.

### Identifying and Securing the Vulnerability

Identifying the risk and the extent of the intrusion. This can be accomplished in several ways, including:

* Determine the type of threat
* Understanding the behavior or characteristics of the threat
* Evaluate the spread of the intrusion and any critical areas
* Identify which users and accounts have been compromised

Review sources that could provide further indicators

* IDS/IPS - Both Network and Host
* SIEM’s
* Antivirus and Antispam
* Operating system logs
* Network device logs - Firewalls and Routers
* Information on possibly new vulnerabilities

On Internet-facing production systems, check the vendors’ websites daily. Some vendors (Microsoft) have been known to release bug fixes at least once a week. Check with all IT vendors, including those for each application, operating system, and network device.

1. **Using Passive Network Monitoring (PR.PT-1) (DE.AE-3) (DE.CM)**

Once an incident is understood, network monitoring can provide valuable insight regarding incident spread and recurrence. Using a dedicated Unix or Windows machine, incident response staff can “sniff” local area network traffic between specified servers and network devices. Standard tools on either platform can be easily configured to monitor and (optionally) record traffic associated with almost every known cross-network attack. Tools are constantly changing and updating to perform these functions.

Network Intrusion Detection Systems (NIDS) are intended to catch as many security attacks as possible when they happen. Network monitoring can also be used to focus on a very specific attack vector; on a specific server or network. This type of monitoring is very common in many environments and systems.

Passive network monitoring may require a significant amount of personnel time or third-party vendor through contracting. Estimates of time are based on current activity and hours of active monitoring in a 24 hour period. This may need to change daily based on continuously changing circumstances. A third-party contract should allow for this type of fluctuation.

### Neutralizing / Eradication of the Threat

### Create a strategy to eliminate or reduce propagating threats, security team members must be sure the compromise is limited and isolated. This could include creating a quarantine network that would allow the security team to better understand the threat. After an incident has been contained, eradication may be necessary to eliminate components of the incident, such as deleting malware and disabling breached user accounts, as well as identifying and mitigating all vulnerabilities that were exploited. During eradication, it is important to identify all affected hosts within the organization so that they can be remediated. For some incidents, eradication is either not necessary or is performed during recovery.

Situations that pose a great risk may warrant unplugging machines from the network, or even the wall. Before removing a machine from the network, record as much information as possible, including users logged on, network connections, running processes and live memory captures. This information will be lost when the machine is isolated. It is highly advisable to create a forensic duplication of the compromised systems as early in the incident handling process as possible.

1. **Restoring Services**

In recovery, administrators restore systems to normal operation, confirm that the systems are functioning normally, and (if applicable) remediate vulnerabilities to prevent similar incidents. Recovery may involve such actions as restoring systems from clean backups, rebuilding systems from scratch, replacing compromised files with clean versions, installing patches, changing passwords, and tightening network perimeter security (e.g., firewall rulesets, boundary router access control lists). Higher levels of system logging or network monitoring are often part of the recovery process. Once a resource is successfully attacked, it is often attacked again, or other resources within the organization are attacked in a similar manner.

Restoring service depends on having reliable, up-to-date tape backups of important systems and data. These tape backups allow for recovery of a system to a variety of points in time. This is important because it is common for a few nights of backups to take place before a security incident is even discovered. Additionally, these backups provide a baseline for comparison. Without them, it is impossible to discover what files, permissions, and settings might have been changed by an attacker.

As mentioned in the previous section, it is very important that systems be restored from known-secure versions, as opposed to being fixed and reconnected to the Internet directly. Data files, application settings, and even the system itself may have been replaced with malicious software.

The technical steps for actually restoring a machine are identical to those that would be used in any other disaster recovery system. In the unfortunate situation that full backups of a system are not available, the original operating system media should be used to get the system back to a functional state. After the operating system is installed, the appropriate installation and configuration checklists should be followed to be sure the new system is secure.

Preparation is the key to successful service restoration after an incident. Having full, current system backups is the best way to be prepared. System restoration should be practiced regularly. The IT Department should be trained on restoring a production server.

1. **Data Backups**

Performing data backups is a strategy that is common to almost every serious security situation. Restoring systems from clean back-ups is essential to recovery. Back-ups should be redundant, secure and tested on a routine basis.

Regular backups should be in place on all servers. The IT staff must evaluate the time of the last data backup to determine if backed-up data is sufficiently recent. If the most recent backup was prior to the incident, then every effort should be made to backup critical data from the compromised system before moving forward with incident handling.

* 1. **Responding to Malicious Software/Viruses**

Although several tools are in use to help protect against computer viruses and worms, there is no perfect protection. New viruses are coming out hourly and virus protection software is updated daily at best.

The first action when dealing with malicious software should be to stop the spread of the software. This usually requires some knowledge of the vectors the virus or worm is using to distribute itself to new targets. Serious outbreaks may require isolating infected machines from the network or disabling organization infrastructure such as email or Web services. Some viruses can cause damage on machines that are shut down or rebooted, so the outbreak should be identified before machines are turned off. There are exceptions to this rule in extreme circumstances, such as when network isolation is not possible and confidential or otherwise mission-critical information is at risk.

In cases where staff have a good understanding of the malicious software, options for mitigation include installing patches from Microsoft (or another vendor), reconfiguring email servers, and modifying firewall configurations. Each of these depends on the specific actions and characteristics of the malicious software, so it must be identified before they can be used effectively. Virus protection definitions should be forcibly updated on computers once the vendor announces support for the virus or worm in question. Be warned that some malicious software actually opens holes on a computer through which attackers from the Internet gain access. An infected machine should not be allowed to stay on the network.

## Responding to Physical Intrusions

For any physical intrusion emergencies that happen on jurisdictional premises, dial 911.

Electronic incident response staff need to be involved in the investigation of any physical intrusion that leads to a computer intrusion security incident. It is especially important that electronic incident response staff investigate areas of physical intrusion for laptops, workstations, or servers that may have been accessed. Specifically, the incident response staff should:

* + Check to ensure the machine is running an OS that requires a login and password.
  + Check to ensure the machine has a screensaver password, and record the timeout.
  + Quickly review the machine for any signs of physical tampering.
  + Quickly compare the machine’s hardware to known inventory (if possible).
  + Quickly review the machine’s logs for any signs of unauthorized electronic use.

Electronic incident response staff should also be involved in any investigations involving the theft of an entire system. Losing an entire system could be disruptive to the regular flow of business. To determine the effect that any theft would have, incident response staff should:

* + Check records to get specific system information such as model and serial number. Report this information to the police as soon as possible.
  + Check with regular users of the system to verify what it was used for and determine how critical the information is.

# Formal Incident Reporting (RS.CO)

When incidents do occur, they will be reported to affected parties as appropriate and based upon regulatory agency requirements. The jurisdiction’s elected officials/leadership holds responsibility for controlling when and how incidents are reported. The IT Director and public information officer will develop the release. The public information officer for the jurisdiction or designee should be the single point of contact for media inquiries.

## Reporting Incidents to Employees

If there is any doubt that someone needs to know specific information about an incident, speak to the IT Director before sharing such information. Outside of those who need to know to handle an incident in the short-term, however, the IT Director, with approval from the jurisdiction’s administration, is responsible for deciding when and how to communicate the incident to employees. Employees should be given the name(s) of the public information officer or designee in case of media requests. Employees should be reminded to not speak directly to the media.

## Reporting Incidents to other jurisdictions- \*\*\*Discussion during June 2018 Cyber Committee Meeting. This is an important section to have agreement across the Region.

## CORA Requests (No direct NIST Function)

Colorado statutes (C.R.S. § 24-72-200.1, et seq) set forth the rights and requirements of the Colorado Open Records Act (CORA). Generally, the public has the right to access the public documents of a governmental entity. The IT Department, after consulting with the organization’s official record keeper and legal counsel, must process CORA requests in a way that proves the information provided is complete and has not been altered. CORA requests will be processed using similar techniques to E Discovery requests in order to show that processing is complete and does not modify, create, or delete information.

CORA requests will only be processed by the IT Department upon approval of the IT Director, the organization’s official record keeper, and legal counsel. The IT Director or designee will work with legal counsel and data custodians to determine the scope of request processing. The results will be provided to legal counsel for further review to ensure that no confidential information is released.

## Litigation Holds and E-Discovery (No direct NIST Function)

Electronic discovery is the electronic aspect of identifying, collecting, and producing electronically stored information (ESI) in response to a request for production in a lawsuit or investigation. ESI includes, but is not limited to, emails, documents, presentations, databases, voicemail, audio and video files, social media, and websites.

Electronic information relevant to upcoming litigations must be preserved and retained when there is reason to anticipate litigation or when a formal discovery or hold notice has been presented to legal counsel. Information relating to the request must be retained until there is no longer an anticipation of litigation or the formal litigation hold has been lifted.

The IT Director or designee will work with legal counsel and/or Risk Management to determine the scope of litigation holds focusing on: the claim, who was involved, the time period, and possible systems storing information relating to the claim. It is the responsibility of the records manager to document the technical processes used to gather and preserve information relating to the claim.

Electronic documents are more dynamic and often contain metadata such as time-date stamps, author and recipient information, and file properties. Preserving the original content and metadata for electronically stored information is required in order to eliminate claims of spoliation or tampering with evidence later in the litigation. Burn two copies of the data to DVD or CD’s and label them with a numerical value. One copy of the data is saved by the records manager and the other is sent to the requesting party.

# Root Cause Analysis (RC-IM)

Depending on the length of the incident, all affected parties will meet after to review the results of the investigation to determine the root cause of the compromise and evaluate the effectiveness of the incident response plan.

* Any identified areas in which the plan, policy, or security control can be made more effective or efficient, must be updated accordingly.
* The incident handler in charge of overseeing the incident response must prepare an after action report, which should include the following:
  + - List of staff involved
    - Date and Time of the event
    - Time to Detect and Time to Mitigation
    - Findings of the meeting between all affected parties;
    - Description of any risks such as:
      * Vulnerabilities
      * Attack vectors
      * Compromised System(s)
    - Identification of which mitigating factors had been used
    - Quantitative results including source of statistics
    - All findings and recommendations for further action, if applicable.
* The IT Director must review the information, approve it and add it to the after action report.

# Follow-Up and After Action Reporting (RS.IM) (RC.IM)

Each incident should have a follow-up. This meeting will ensure that:

1. The incident was handled per process, in a professional and standardized manner
2. The outcome of the incident was appropriate to the issue
3. All documentation, policies, and processes are accurate and appropriate. If not, then changes should be proposed and implemented per the change management process

Information from these meetings should be documented in a central location. Changes to technical configurations, practice and procedure, and policy should all be well-documented. A quality record of changes can act as an invaluable reference when evaluating the success of a security strategy. Any approved changes in incident handling practices should be recorded in this document. Keeping this document up-to-date with current incident handling practices will help ensure that evidence is protected and incidents are handled as efficiently as possible.

# 

# 

APPENDICES

**APPENDIX ONE: Documenting the Incident Form**

**(DE.DP-4) (RS.CO-2 and 3)**

Priorities:

-Collect and preserve initial information.

* Complete the form on this page quickly and accurately.
* Inform the IT Director or designee when this form is completed.

-Avoid alerting possible attacker(s).

* Gather only as much information as is necessary to confirm the incident is real.
* Inform individuals of the incident only as necessary to confirm it.

\*\*\*Transfer this document and any existing evidence to the IT Director/Chief Information Security Officer for ongoing documentation.

|  |
| --- |
| Your Name: |
| Your Contact Information: |
| Current Date and Time: |
| Source of Time Reference: |
| How did you become aware of this incident? |
| What do you know about the incident? (Users, systems, software, hardware involved? Time events occurred?) |
| What actions have been taken to this point? (Who performed these actions and when?) |
| Who is aware of this incident? (Name, department/organization, notes) |

# APPENDIX TWO: Investigating and Confirming the Security Incident Form

**(RS.AN-1)**

System Administrator responding to the incident.

Priorities:

-Avoid alerting possible attacker(s).

* Gather only as much information as is necessary to confirm the incident is real.
* Inform individuals of the incident only as necessary to confirm it.

-Ensure the right parties are notified based upon the notification section of this plan.

-Preserve evidence and chain-of-custody.

-Record every change you make to applications, systems, or the network.

-Move to the next section as soon as you’ve confirmed the incident is real.

|  |  |
| --- | --- |
| Your Initials: | Current Date and Time: |
| Source of Time Reference: | |
| What steps were taken/data was collected to confirm the incident? | |
| If you could determine, what led you to believe this is or is not a security incident? | |
| What actions have been taken to this point? (Who performed these actions and when?) | |

# APPENDIX THREE: Determining and Executing the IRP Form

**(RS.RP) (RC.CO) (RS.AN) (RC.RP)**

Priorities:

* Assemble personnel designated with a role in this incident response. This team may include (as positions exist):
* IT Director
* Chief Information Security Officer
* One or more network planners
* Server administrator of each affected server
* Application administrator/software developer/PC specialist/DBA as necessary
* Human resources as necessary
* Third-party resources as necessary
* EOC Liaison (if EOC is activated)
* Other Leadership and/or Other Department Directors (as needed)
* Determine IC and other needed positions in the Incident Command Structure (SEE APPENDIX 4)
* Quickly analyze the incident and determine risk.
* Determine and execute response strategy.
* Document every change you make as part of the response.
* Manage all evidence and its chain of custody.

|  |  |
| --- | --- |
| Your Initials: | Current Date and Time: |
| Source of Time Reference: | |
| What risk does this incident pose to the jurisdiction? (SEE PAGE 12) | |
| What vulnerability caused the initial exposure and how should it be secured? (SEE APPENDIX 5) | |
| How and when should service be interrupted and restored? (SEE PAGES 14-17) | |
| Should evidence be gathered to attempt to pursue the attacker or further analyze the incident? | |
| What entities should be notified, when, and by whom? (SEE PAGES 8 and 11) | |
| Record all changes made during this phase of incident handling: (SEE PAGE 10) | |

# APPENDIX FOUR: Incident Commander Guide (RS.RP) (RS.CO) (RC.RP)

# Answer the following questions (repeat this checklist as the situation evolves). If the answer is NO to any of the checklist questions, you should take the appropriate corrective action(s) IMMEDIATELY.

|  |  |  |
| --- | --- | --- |
| **Yes** | **No** | **Question** |
|  |  | Does everyone (Resources, EOC, Leadership, and Elected Officials) know who the Incident Commander is? |
|  |  | Have you sized up the situation and established Incident Objectives? |
|  |  | Have you activated the Incident Response Plan? |
|  |  | Do you know the impacts to public safety or other critical infrastructure (utilities)? |
|  |  | Have you developed a plan that prioritizes incident response and/or recovery tasks? And have you communicated this plan to all personnel assigned to the incident including new arrivals? |
|  |  | Can you respond and/or recover with the resources available (onsite and en route) under the expected conditions? |
|  |  | Do you have a sufficient command organization in place? |
|  |  | Do you have a complete list of onsite and incoming resources? |
|  |  | Are Standard Operating Procedures being followed? |
|  |  | Are personnel gathering information to understand the extent of the incident? |
|  |  | Can you communicate with everyone working on the incident response, supporting with resource orders, and making-decisions? |
|  |  | If the incident will not be controlled before the next operational period, have you informed the senior leadership? |
|  |  | Does the scope and complexity remain within your capabilities and qualifications to manage the incident? |

# 

# APPENDIX FIVE: Incident Discovery Guide

**(DE.CM) (DE.DP) (RS.RP) (RC.RP)**

|  |  |
| --- | --- |
| **Malicious Actions** | **Possible Indications of an Incident** |
| **Denial of Service (DoS) Examples** | **You might be experiencing a DoS if you see…** |
| Network- based DoS against a particular host | • User reports of system unavailability • Unexplained connection losses • Network intrusion detection alerts • Host intrusion detection alerts (until the host is overwhelmed) • Increased network bandwidth utilization • Large number of connections to a single host • Asymmetric network traffic pattern (large amount of traffic going to the host, little traffic coming from the host) • Firewall and router log entries • Packets with unusual source addresses |
| Network- based DoS against a network | • User reports of system and network unavailability • Unexplained connection losses • Network intrusion detection alerts • Increased network bandwidth utilization • Asymmetric network traffic pattern (large amount of traffic entering the network, little traffic leaving the network) • Firewall and router log entries • Packets with unusual source addresses • Packets with nonexistent destination addresses |
| DoS against the operating system of a particular host | • User reports of system and application unavailability • Network and host intrusion detection alerts • Operating system log entries • Packets with unusual source addresses |
| DoS against an application on a particular host | • User reports of application unavailability • Network and host intrusion detection alerts • Application log entries • Packets with unusual source addresses |

|  |  |
| --- | --- |
| **Malicious Software (malware) Examples** | **You might be infected with malware if you see…** |
| A virus that spreads through email infects a host. | • Antivirus software alerts of infected files • Sudden increase in the number of emails being sent and received • Changes to templates for word processing documents, spreadsheets, etc. • Deleted, corrupted, or inaccessible files • Unusual items on the screen, such as odd messages and graphics • Programs start slowly, run slowly, or do not run at all • System instability and crashes |
| A worm that spreads through a vulnerable service infects a host. | • Antivirus software alerts of infected files • Port scans and failed connection attempts targeted at the vulnerable service (e.g., open Windows shares, HTTP) • Increased network usage • Programs start slowly, run slowly, or do not run at all • System instability and crashes |
| A Trojan horse is installed and running on a host. | • Antivirus software alerts of Trojan horse versions of files • Network intrusion detection alerts of Trojan horse client-server communications • Firewall and router log entries for Trojan horse client-server communications • Network connections between the host and unknown remote systems • Unusual and unexpected ports open • Unknown processes running • High amounts of network traffic generated by the host, particularly if directed at external host(s) • Programs start slowly, run slowly, or do not run at all • System instability and crashes |
| Malicious mobile code on a Web site is used to infect a host with a virus, worm, or Trojan horse. | • Indications listed above for the pertinent type of malicious code • Unexpected dialog boxes, requesting permission to do something • Unusual graphics, such as overlapping or overlaid message boxes |
| Malicious mobile code on a Web site exploits vulnerabilities on a host. | • Unexpected dialog boxes, requesting permission to do something • Unusual graphics, such as overlapping or overlaid message boxes • Sudden increase in the number of emails being sent and received • Network connections between the host and unknown remote systems |
| A user receives a virus hoax message. | • Original source of the message is not an authoritative computer security group, but a government agency or an important official person • No links to outside sources • Tone and terminology attempt to invoke panic or a sense of urgency • Urges recipients to delete certain files and forward the message to others |

|  |  |
| --- | --- |
| **Unauthorized Access Examples** | **You might be experiencing unauthorized access on your system or network if you see…** |
| Root compromise of a host | • Existence of unauthorized security-related tools or exploits • Unusual traffic to and from the host (e.g., attacker may use the host to attack other systems) • System configuration changes, including—  - Process/service modifications or additions  - Unexpected open ports  - System status changes (restarts, shutdowns)  - Changes to log and audit policies and data  - Network interface card set to promiscuous mode (packet sniffing)  - New administrative-level user account or group • Modifications of critical files, timestamps and privileges, including executable programs, OS kernels, system libraries, and configuration and data files • Unexplained account usage (e.g., idle account in use, account in use from multiple locations at once, unexpected commands from a particular user, large number of locked-out accounts) • Significant changes in expected resource usage (e.g., CPU, network activity, full logs, or file systems) • User reports of system unavailability • Network and host intrusion detection alerts • New files or directories with unusual names (e.g., binary characters, leading spaces, leading dots) • Highly unusual operating system and application log messages • Attacker contacts the organization to say that he or she has compromised a host |
| Unauthorized data modification (e.g. Web server defacement) | • Network and host intrusion detection alerts • Increased resource utilization • User reports of the data modification (e.g., defaced Website) • Modifications to critical files (e.g., Web pages) • New files or directories with unusual names (e.g., binary characters, leading spaces, leading dots) • Significant changes in expected resource usage (e.g., CPU, network activity, full logs or file systems) |
| Unauthorized usage of standard user account | • Access attempts to critical files (e.g., password files) • Unexplained account usage (e.g., idle account in use, account in use from multiple locations at once, commands that are unexpected from a particular user, large number of locked-out accounts) • Web proxy log entries showing the download of attacker tools |
| Physical intruder | • User reports of network or system unavailability • System status changes (restarts, shutdowns) • Hardware is completely or partially missing (i.e., a system was opened and a particular component removed) • Unauthorized new hardware (e.g., attacker connects a packet sniffing laptop to a network or a modem to a host) |
| Unauthorized data access (e.g., database of customer information, password files) | • Intrusion detection alerts of attempts to gain access to the data through FTP, HTTP, and other protocols • Host-recorded access attempts to critical files |

|  |  |
| --- | --- |
| **Inappropriate Usage Examples** | **You might have identified inappropriate usage if you see…** |
| Unauthorized service usage (e.g., Web server, file sharing, music sharing) | • Network intrusion detection and network behavior analysis software alerts • Unusual traffic to and from the host • New process/software installed and running on a host  - Password cracking tools  - Unauthorized website running  - File transfer software  - Peer-to-Peer (P2P) sharing software running • New files or directories with unusual names (e.g., “warez” server style names) • Increased resource utilization (e.g., CPU, file storage, network activity) • User reports • Application log entries (e.g., Web proxies, FTP servers, email servers) |
| Access to inappropriate materials (e.g., downloading pornography, sending spam) | • Network intrusion detection alerts • Eyewitness reports or complaints to management, HR, or ethics  o Pornographic or explicit content displayed • Application log entries (e.g., Web proxies, FTP servers, email servers) • Inappropriate files on workstations, servers, or removable media |
| Attack against internal party | • Network intrusion detection alerts • Inside party reports (e.g. management, HR, or ethics)  - Harassing email or text messages sent to internal users  - Pornographic or explicit content sent to internal users • Network, host, and application log entries |
| Attack against external party | • Network intrusion detection alerts • Outside party reports  - Harassing email or text messages sent to external users  - Pornographic or explicit content sent to external users  - External attack traffic traced back to the company • Network, host, and application log entries |

**APPENDIX SIX: Detection Methods (DE.CM)**

|  |  |  |
| --- | --- | --- |
| **Type** | **Source** | **Description** |
| **Computer Security Software Alerts** | | |
| Technical | Network-based, host-based, and wireless IDS | Intrusion Detection System (IDS) or Intrusion Prevention System (IPS) products are designed to identify suspicious events and record pertinent data regarding them, including the date and time the attack was detected, the type of attack, the source and destination IP addresses, and the username (if applicable and known). Most IDPS products use a set of attack signatures to identify malicious activity; the signatures must be kept up to date so that the newest attacks can be detected. IDPS software often produces false positives—alerts that indicate malicious activity is occurring, when in fact there has been none. Analysts should manually validate IDPS alerts either by closely reviewing the recorded supporting data or by getting related data from other sources. |
| Technical | Antivirus, antispyware, and antispam software | Antivirus and antispyware software are designed to detect various forms of malicious code and prevent them from infecting hosts. When antivirus or antispyware software detects malicious code, it typically generates alerts. Current antivirus and antispyware products are effective at detecting and eradicating or isolating malicious code if their signatures are kept up to date. |
| Technical | File integrity checking software | Incidents may cause changes to important files; file integrity checking software can detect such changes. It works by using a hashing algorithm to obtain a cryptographic checksum for each designated file. If the file is altered and the checksum is recalculated, an extremely high probability exists that the new checksum will not match the old checksum. By regularly recalculating checksums and comparing them with previous values, changes to files can be detected. |
| Technical | 3rd Party Monitoring service | Some organizations pay a third party to monitor their publicly accessible services, such as Web, Domain Name System (DNS) and FTP servers. The third party automatically attempts to access each service every x minutes. If the service cannot be accessed, the third party alerts the organization using the methods specified by the organization, such as phone calls, pages, and emails. |
| **Logs** | | |
| Technical | Operating system, security, and application logs | Logs from operating systems, services, and applications (particularly audit-related data) are frequently of great value when an incident occurs. Logs can provide a wealth of information, such as which accounts were accessed and what actions were performed. |
| Technical | Network device logs | Logs from network devices such as firewalls and routers are not typically used as a primary source of precursors or indications. Although these devices are usually configured to log blocked connection attempts, they provide little information about the nature of the activity. |

|  |  |  |
| --- | --- | --- |
| **Publicly Available Information** | | |
| Human | Information on new vulnerabilities and exploits | Keeping up with new vulnerabilities and exploits can prevent some incidents from occurring and assist in the detection and analysis of new attacks. The National Vulnerability Database (NVD) contains information on vulnerabilities. Several organizations, such as US-CERT, CERT®/CC, IAIP, and the Department of Energy’s Computer Incident Advisory Capability (CIAC), periodically provide threat update information through briefings, Web postings, and mailing lists. |
| Human | Information on incidents at other organizations | Reports of incidents that have occurred at other organizations can provide a wealth of information. There are Websites and mailing lists where incident response teams and security professionals can share information regarding reconnaissance and attacks that they have seen. In addition, some organizations acquire, consolidate, and analyze logs and intrusion detection alerts from many other organizations. |
| **People** | | |
| Human | Internal Users | Users, system administrators, network administrators, security staff, and others from within the organization may report signs of incidents. It is important to validate all such reports. Not only do users generally lack the knowledge to determine if an incident is occurring, but also even the best-trained technical experts make mistakes. One approach is to ask people who provide such information how confident they are of the accuracy of the information. Recording this estimate along with the information provided can help considerably during incident analysis, particularly when conflicting data is discovered. |
| Human | Other Organizations | Although few reports of incidents will originate from people at other organizations, they should be taken seriously. A classic example is an attacker who identifies a serious vulnerability in a system and either informs the organization directly or publicly announces the issue. Another possibility is that the organization might be contacted by an external party claiming someone at the organization is attacking it. External users may also report other indications, such as a defaced Web page or an unavailable service. Other incident response teams also may report incidents. |

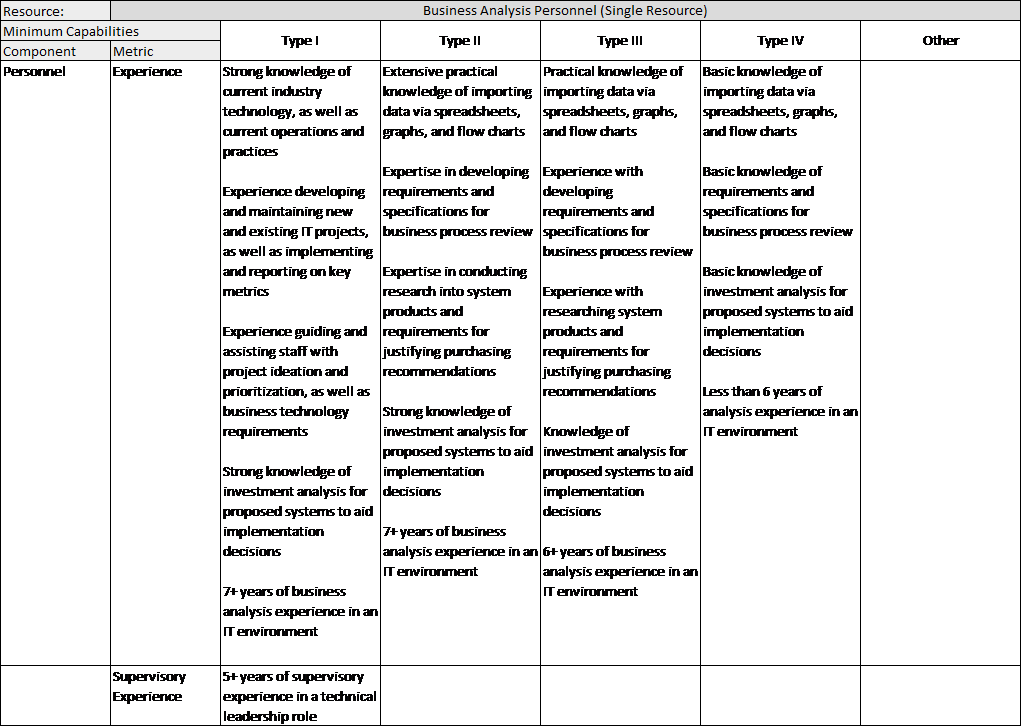
**APPENDIX SEVEN: Alert Levels (developed by MS-ISAC)**

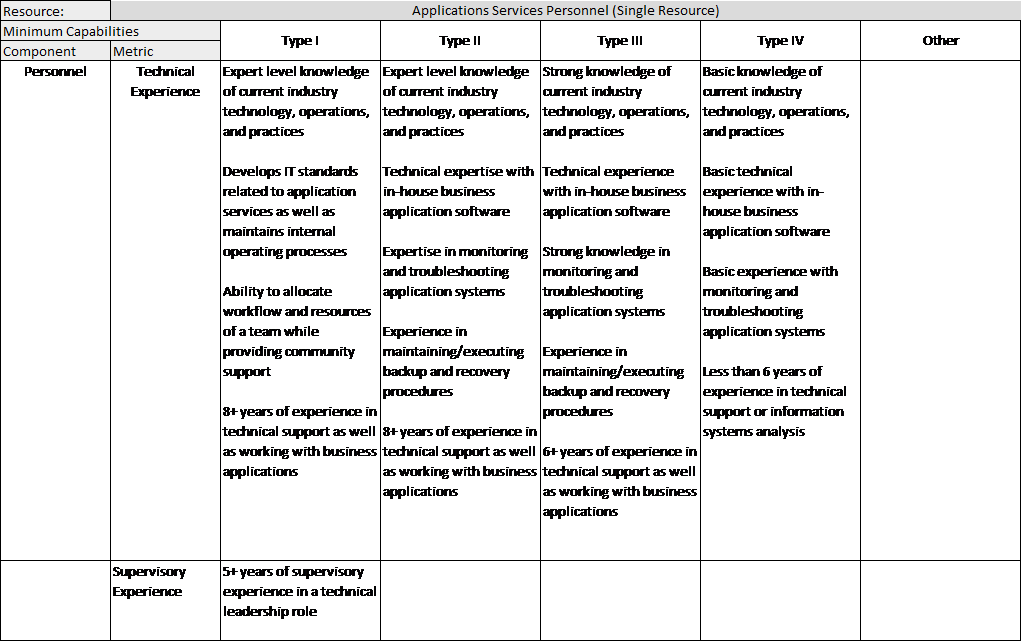
**(RS.RP) (RS.CO) (RS.MI) (RS.IM) (RC.RP) (RC.IM) (RC.CO)**

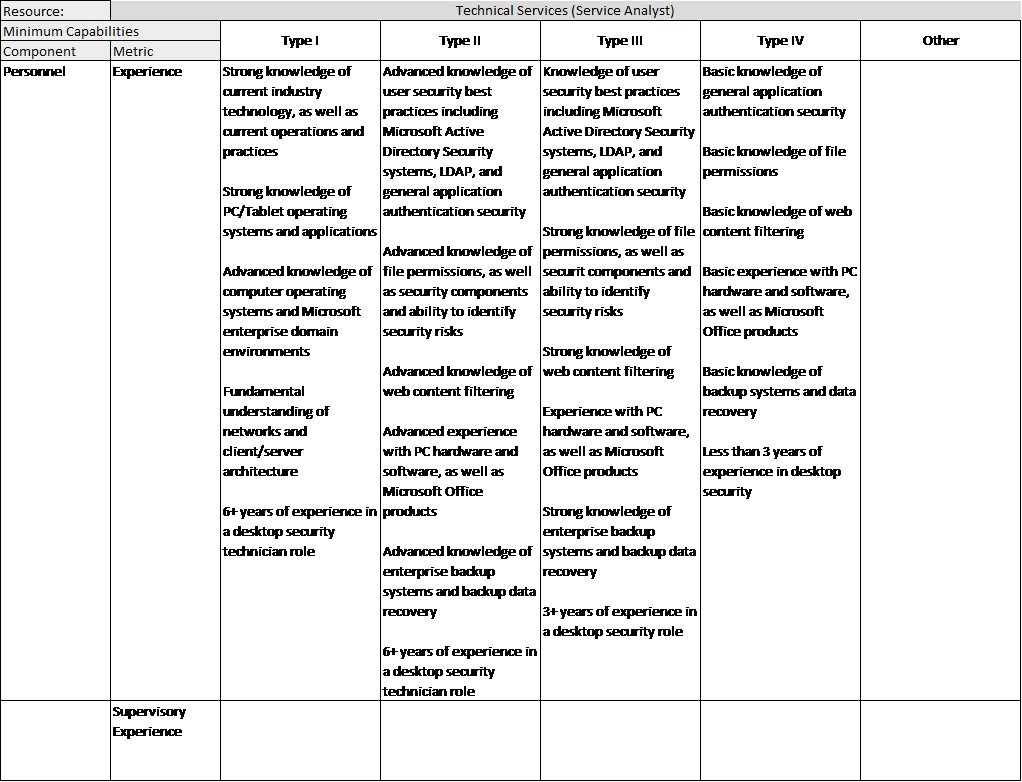
|  |  |
| --- | --- |
| **Alert Color/Formula Score** | **Color Indication** |
| **Green - Low :**  **-8 to -5** | **No unusual activity exists beyond the normal concern for known hacking activities, known viruses, or other malicious activity**.  Examples:  Normal probing of the network  Low-risk viruses  Actions:  Continue routine preventive measures, including the application of vendor security patches and updates to anti-virus software signature files on a regular basis.  Continue routine security monitoring.  Ensure personnel receive proper training on cybersecurity policies. |
| **Blue - Guarded :**  **-4 to -2** | **Indicates a general risk of increased hacking, virus, or other malicious activity.** The potential exists for malicious cyber activities, but no known exploits have been identified, or known exploits have been identified but no significant impact has occurred.  Examples:  A critical vulnerability is discovered but no exploits are reported.  A critical vulnerability is being exploited but there has been no significant impact.  A new virus is discovered with the potential to spread quickly.  There are credible warnings of increased probes or scans.  A compromise of non-critical system(s) did not result in loss of data.  Actions:  Continue recommended actions from previous level.  Identify vulnerable systems.  Implement appropriate countermeasures to protect vulnerable systems.  When available, test and implement patches, install anti-virus updates, etc., in the next regular cycle. |
| **Yellow - Elevated :**  **-1 to +2** | **Indicates a significant risk due to increased hacking, virus, or other malicious activity that compromises systems or diminishes service.** At this level, there are known vulnerabilities that are being exploited with a moderate level of damage or disruption, or the potential for significant damage or disruption is high.  Examples:  An exploit for a critical vulnerability exists that has the potential for significant damage.  A critical vulnerability is being exploited and there has been a moderate impact.  There is a compromise of a secure or critical system(s) containing sensitive information.  There is a compromise of a critical system(s) containing non-sensitive information if appropriate.  A virus is spreading quickly throughout the Internet, causing excessive network traffic.  There is a distributed denial of service attack.  Actions:  Continue recommended actions from previous levels.  Identify vulnerable systems.  Increase monitoring of critical systems.  Immediately implement appropriate countermeasures to protect vulnerable critical systems.  When available, test and implement patches, install anti-virus updates, etc., as soon as possible. |
| **Orange - High :**  **+3 to +5** | **Indicates a high risk of increased hacking, virus, or other malicious cyber activity that targets or compromises core infrastructure, causes multiple service outages, causes multiple system compromises, or compromises critical infrastructure.** At this level, vulnerabilities are being exploited with a high level of damage or disruption, or the potential for severe damage or disruption is high.  Examples:  An exploit for a critical vulnerability exists that has the potential for severe damage.  A critical vulnerability is being exploited and there has been significant impact.  Attackers have gained administrative privileges on compromised systems.  There are multiple damaging or disruptive virus attacks.  There are multiple denial of service attacks against critical infrastructure services.  Actions:  Continue recommended actions from previous levels.  Closely monitor security mechanisms, including firewalls, web log files, anti-virus gateways, system log files, etc., for unusual activity.  Consider limiting or shutting down less critical connections to external networks such as the Internet.  Consider isolating less mission-critical internal networks to contain or limit the potential of an incident.  Consider the use of alternative methods of communication, such as phone, fax, or radio in lieu of email and other forms of electronic communication.  When available, test and implement patches, anti-virus updates, etc., immediately. |
| **Red - Severe :**  **+6 to +8** | **Indicates a severe risk of hacking, virus, or other malicious activity resulting in widespread outages and/or significantly destructive compromises to systems with no known remedy or debilitates one or more critical infrastructure sectors.** At this level, vulnerabilities are being exploited with a severe level or widespread level of damage or disruption of Critical Infrastructure Assets.  Examples:  Complete network failures  Mission-critical application failures  Compromise or loss of administrative controls of critical system  Loss of critical supervisory control and data acquisition (SCADA) systems  Potential for or actual loss of lives or significant impact on the health or economic security of the state  Actions:  Continue recommended actions from previous levels.  Shut down connections to the Internet and external business partners until appropriate corrective actions are taken.  Isolate internal networks to contain or limit the damage or disruption.  Use alternative methods of communication, such as phone, fax, or radio as necessary in lieu of email and other forms of electronic communication. |
| **The Alert Level is determined using the following threat severity formula:**  Severity = (Criticality + Lethality) - (System Countermeasures + Network Countermeasures)  · **Lethality: How likely is it that the attack will do damage?**  **(Value = Potential Damage)**  o 5: Exploit exists. Attacker could gain root or administrator privileges. Attacker could commit denial of service.  o 4: Exploit exists. Attacker could gain user level access privileges. Attacker could commit denial of service.  o 3: No known exploit exists. Attacker could gain root or administrator privileges. Attacker could commit degradation of service.  o 2: No known exploit exists. Attacker could gain user level access privileges.  o 1: No known exploit exists. Attacker could not gain access.  · **Criticality: What is the target of the attack?**  **(Value = Target)**  o 5: Core services such as critical routers, firewalls, VPNs, IDS systems, DNS servers, or authentication servers  o 4: Email, web, database, and critical application servers  o 3: Less critical application servers  o 2: Business desktop systems  o 1: Home users  · **System Countermeasures: What host-based preventive measures are in place?**  **(Value = Countermeasure)**  o 5: Current operating system with applicable patches applied. Server has been hardened and verified via vulnerability scan. Running host-based IDS or integrity checker. Anti-virus signature exists and has been applied to target systems.  o 4: Current operating system with applicable patches applied. Operating system has been hardened. Anti-virus signature exists and has been applied to target systems.  o 3: Current operating system with fairly up-to-date patches applied. Anti-virus signatures are current.  o 2: Current operating system but missing some applicable patches. Anti-virus signature either does not exist or has not been applied to target systems.  o 1: Older operating systems, including Windows NT 3.51, Solaris 2.6, Windows 95/98/ME. No anti-virus software protection.  · **Network Countermeasures: What network-based preventive measures are in place?**  **(Value = Countermeasure)**  o 5: Restrictive (i.e., "deny all except what is allowed") firewall. Firewall rules have been validated by penetration testing. All external connections including VPNs go through (not around) the firewall. Network-based IDS is implemented. Email gateway filters attachments used by this virus.  o 4: Restrictive firewall. External connections (VPNs, wireless, Internet, business partners, etc.) are protected by a firewall. Email gateway filters attachments used by this virus.  o 3: Restrictive firewall. Email gateway filters common executable attachments.  o 2: Permissive firewall (i.e., ''accept all but'') or allowed service (e.g., HTTP, SMTP). Email gateway does not filter all attachments used by this virus.  o 1: No firewall implemented. Email gateway does not filter any attachments.  **Using the result from the formula defined above, the Alert Level Indicator would generally reflect severity levels as follows:**  · **Alert Level Indicator - Severity**  o **Green - Low : -8 to -5**  o **Blue - Guarded : -4 to -2**  o **Yellow - Elevated : -1 to +2**  o **Orange - High : +3 to +5**  o **Red - Severe : +6 to +8** | |

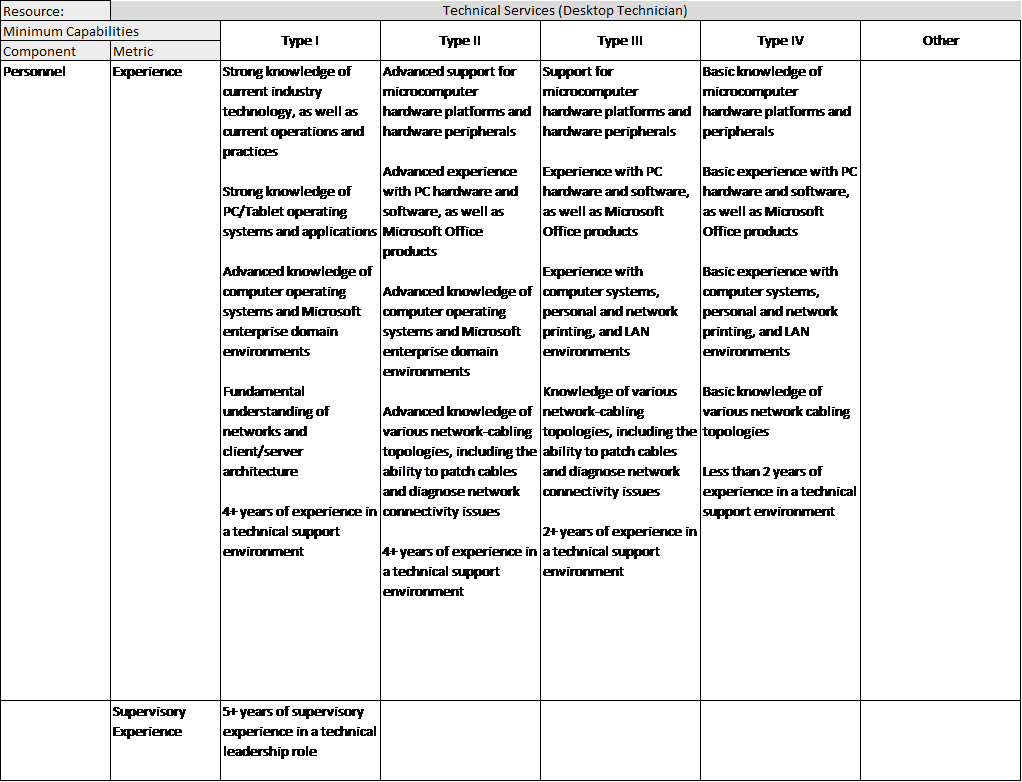
**APPENDIX EIGHT: Resource Typing**

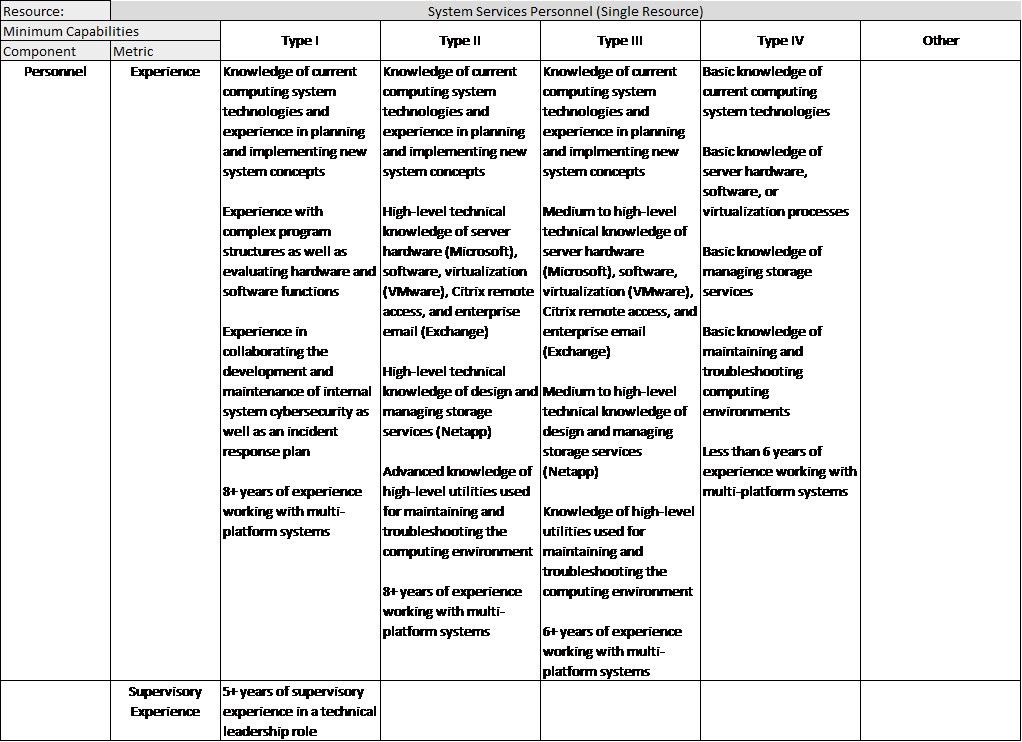
**(RS.RP) (RC.RP)**

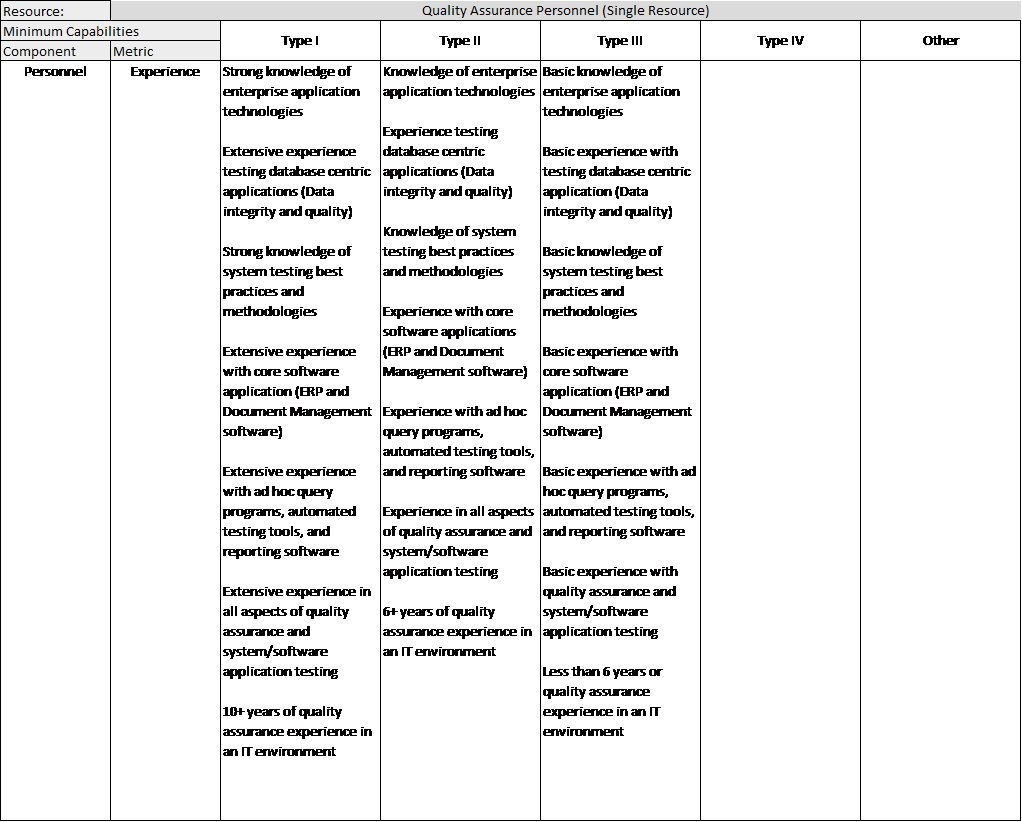


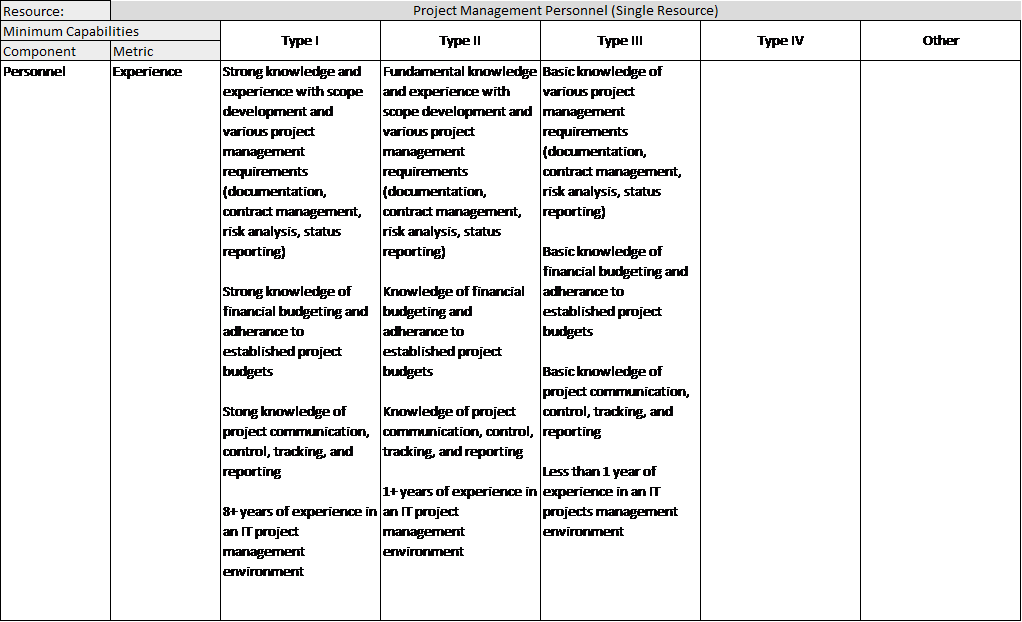


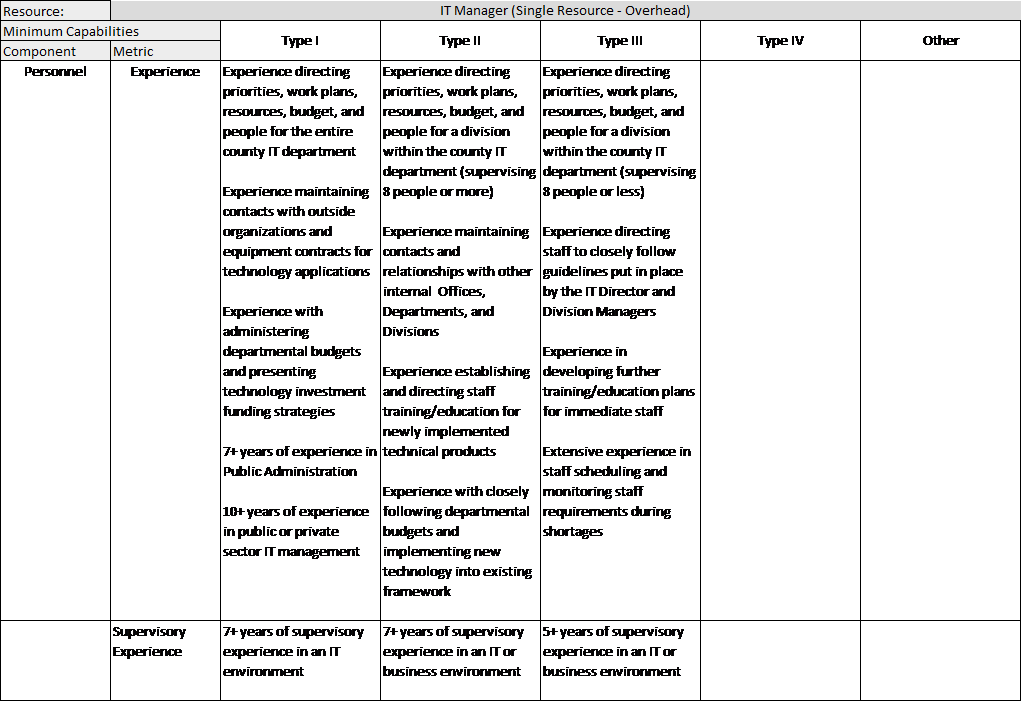


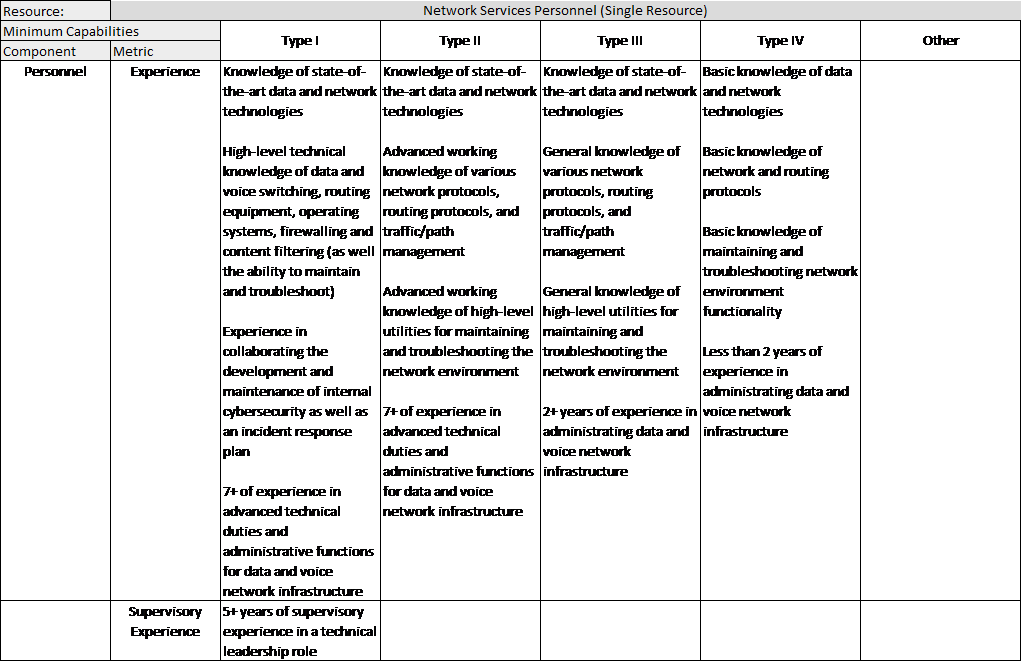


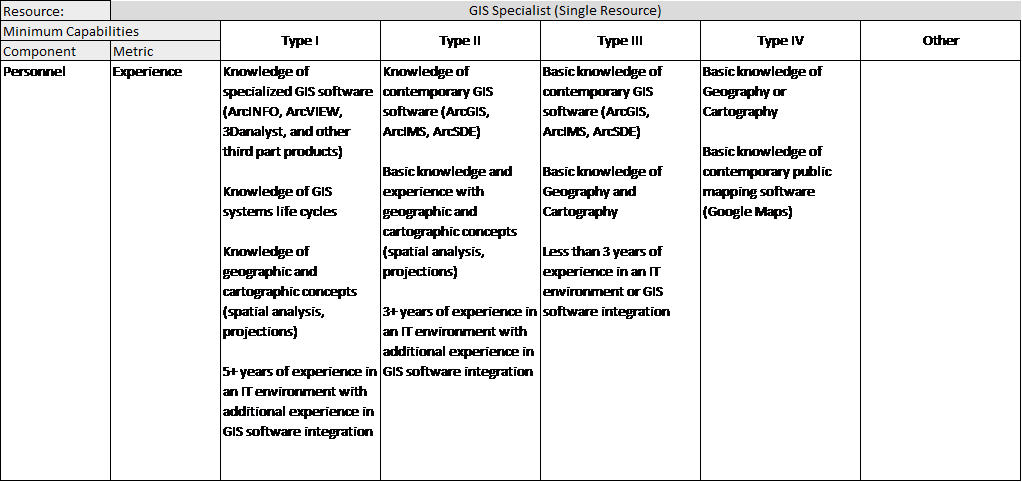


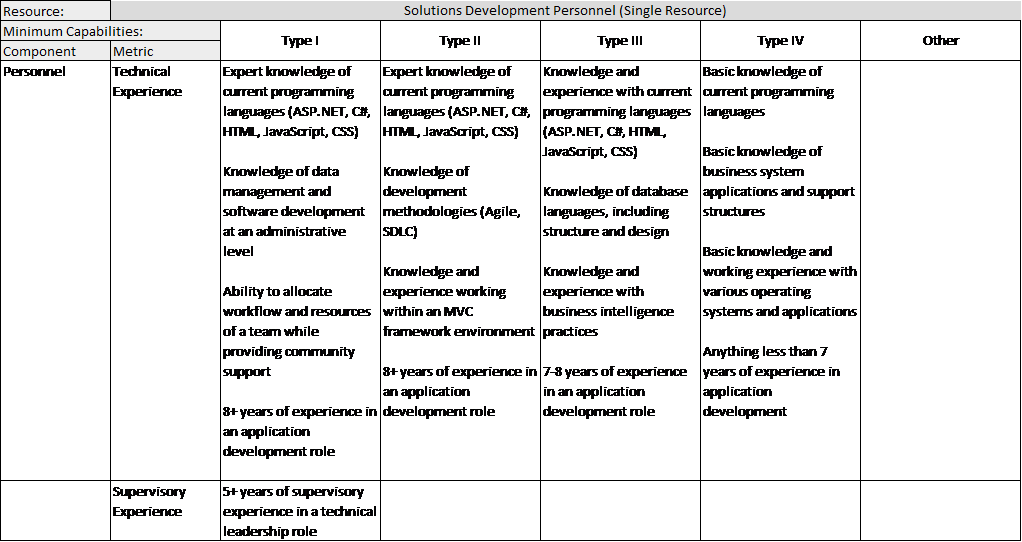












**APPENDIX NINE: Roles and Responsibilities**

**(RS.RP) (RS.CO) (RC.RP) (RC.CO)**

|  |  |
| --- | --- |
| **General: All agencies/organizations assigned to this plan** | * Designating and training representatives for their agency to serve as primary points of contact in the event of a cyber incident. * Developing and maintaining procedures to ensure that a current inventory of agency resources and contact lists are available as part of their COOP plans. * Developing and maintaining procedures to identify, locate, commit, and deploy any agency support resources if requested as part of their COOP Plan. * Providing personnel, equipment, and other assistance to support emergency response and recovery operations within the agency’s capabilities. * Providing situational and operational situation reports in accordance with existing procedures and as requested by the jurisdiction. * Should the resources of the incident within the jurisdiction become overwhelmed, outside resources may be called upon. * Support agencies will provide assistance in the form of personnel, equipment, and/or technical assistance as requested by the incident command. * Identifying and coordinating support staffing requirements appropriate to the emergency situation to include coordination of agencies’ trained resources as available. If a cyber-threat and/or incident has caused activation of the EOC to any extent, Emergency Management, in consultation with Incident Command, will be responsible for measures necessary to monitor and document the situation. * Coordinating response to requests for assistance from the affected agencies, community-level government, and private sector entities through normal EOC procedures. * Provide assistance to other agencies and local officials for data collection, documentation, and damage assessment for affected IT systems and in the disaster area(s) to include information on mitigation and recovery. * Assist documentation preparation for departmental funding needs. * Obtain and compile documentation/information necessary for effective and efficient strategy management by EOC staff. * Develop, maintain, and distribute any appropriate plans and policies related to a cyber incident response. |

|  |  |
| --- | --- |
| **Emergency Management (once activated)** | * Coordinates with the State Emergency Operations Center (EOC). * Respond to the consequences of an incident through the guidelines of the Emergency Operations Plan. * Tracks paperwork for financial purposes. * Facilitates the coordination of recovery efforts. * Facilitates communications with other emergency entities involved in cyber incidents. * Support the coordination of acquiring needed resources, coordinate public information support, and maintaining situational awareness. Examples of resources needed:   + Public Information Support. A Joint Information Center or Joint Information System (JIC/JIS) will most likely be needed during large scale cyber incidents involving multiple agencies. The EOC may facilitate and support these needs. Multiple PIOs from the affected agency and/or jurisdictions may need to work together (in person or remotely) as a team to respond to media inquiries and produce unified messaging using a variety of methods.   + Emergency Management, in conjunction with incident command, may produce situational awareness for other government agencies. Daily situation reports, weekly briefings or other documents may be produced to provide a common operating picture.   + The Policy Group in the EOC serves as decision-maker. |
| **EOC** | * The EOC is responsible for implementing the Emergency Operations Plan, Resource Mobilization and all supporting plans. During a cyber incident, the IT Department may be asked to assign personnel to the EOC. * The jurisdictions law enforcement agency and Information Technology Department are the primary agencies for cyber incident response. * Through the EOC, the Information Technology and Emergency Management Departments will be responsible for leading the consequence management portion of the incident. * The EOC will tailor supporting personnel and materials specific to the cyber incident. The command staff and/or Information Technology Department staff will provide subject matter expertise related to the cyber threat, analysis, and recommendations to the EOC and ultimately the policy group. |
| **IT Department** | * Provide leadership in the development, delivery and maintenance of an information security program by safeguarding the information assets against unauthorized use, disclosure, modification, damage or loss. * Responsible for governance, risk, compliance, and risk management related to cyber security within the jurisdiction. * Develop information security policies related to prevention, protection, detection, response and recovery. * Maintain the Cyber Security Incident Response Plan and ensure COOP plans address a cyber incident. * Responsible for ensuring incident command is implemented at the start of an incident which allows the structure to flex overtime based on the severity of the incident. * Establish a command post / war room and share this information with leadership and the Emergency Management Department. |
| **DHSEM** | * Assists local EOC in by providing requested state level resources. * Maintains WebEOC and resources lists. * Conduit to state and FEMA funding assistance. * State Emergency Operations Center may be activated based on the incident. |
| **CIAC** | * Conduit with the United States Computer Emergency Response Team (US - CERT) and the Multi - State Information Sharing and Analysis Center (MS - ISAC). * Analyze cyber vulnerabilities, exploits, and attack methodologies; * Provide technical assistance; * Defend against an attack; and * Provide indications and warning of potential threats, incidents, and attacks. * Support the coordination of acquiring needed resources and maintaining situational awareness. |
| **Department Staff (other than IT Staff)** | * An IT staff member employed by each affected department or office may be designated to provide support as necessary. |
| **National Guard**  **(Upon approval for activation by the Governor through the proper State process)** | * May provide the following cyber incident response capabilities: * Cyber analysis including detailed examination of networks, systems, processes, and infrastructure. * Threat and vulnerability assessment, including gaps in proper cyber posture. * Information sharing, to include information regarding adversary tactics, techniques, and procedures. * Digital forensics and investigation. * Infrastructure and network monitoring support. * Incident response, mitigation, and recovery. |
| **FBI** | * FBI Cyber Task Forces synchronize domestic cyber threat investigations in the local community through information sharing, incident response, and joint enforcement and intelligence actions. * FBI CyWATCH – Receives cyber threat and incident reporting, assesses it for action, and engages with the appropriate components within FBI Cyber Division, FBI Field Offices, other government agencies and designated Federal Cyber Centers. * May stand up a Cyber Incident Command Center (CICC) for enhanced coordination if the cyber incident is considered a significant or major incident defined by applicable Presidential Policy directive(s) * May provide specialized and deployable on-scene forensic analysis to further attribution (would also depend on severity level). * Forensics of digital evidence in support of criminal investigation. |
| **DHS** | * The Department of Homeland Security (DHS): When cyber incidents occur, DHS provides assistance to potentially impacted entities, analyzes the potential impact across critical infrastructure, investigates those responsible in conjunction with law enforcement partners, and coordinates the national response to significant cyber incidents.<https://www.dhs.gov/national-cybersecurity-and-communications-integration-center> * DHS’s National Cybersecurity and Communications Integration Center (NCCIC) is a 24/7 cyber situational awareness, incident response, and management center that is a national nexus of cyber and communications integration for the federal government, intelligence community, and law enforcement. * NCCIC’s Industrial Control Systems Cyber Emergency Response Team (ICS-CERT). Cybersecurity and infrastructure protection experts from ICS-CERT provide assistance to owners and operators of critical systems by responding to incidents and helping restore services, and by analyzing potentially broader cyber or physical impacts to critical infrastructure. * NCCIC’s National Cybersecurity Assessment and Technical Services (NCATS) offers cybersecurity scanning and testing services that identify vulnerabilities within stakeholder networks and provide risk analysis reports with actionable remediation recommendations. * NCCIC’s National Coordinating Center for Communications (NCC) leads and coordinates the initiation, restoration, and reconstitution of national security and emergency preparedness telecommunications services and/or facilities under all conditions. * The National Infrastructure Coordinating Center (NICC), which is part of the DHS National Operations Center, is the dedicated 24/7 coordination and information sharing operations center that maintains situational awareness of the nation’s critical infrastructure for the federal government. The NICC and the NCCIC share cyber and physical security information to enhance the efficiency and effectiveness of the U.S. government’s work to secure critical infrastructure and make it more resilient. * The Cyber Security Advisor (CSA) Program was created in recognition that a regional and national focused cyber security presence is essential to protect critical infrastructure. CSAs offer immediate and sustained assistance to prepare and protect SLTT and private entities. CSAs represent a front line approach to key cyber infrastructures throughout the U.S. and its territories. CSAs are regionally located based on the Federal Emergency Management Agency (FEMA) regions. Region VIII CSA is located in Denver. CSAs work closely with their Physical Security Specialist counterparts – the Protective Security Advisor (PSA) – who are located in every State. |
| **Federal Government** | * The Federal Government plays a significant role in managing intergovernmental (Federal, State, local, and tribal) and, where appropriate, public - private coordination in response to a cyber - incident. DHS / NPPD / NCSD, other elements of DHS, the Intelligence Community, FBI, DOD, and other Government agencies work closely together and individually to coordinate response during a cyber-incident or attack, identify those responsible, and otherwise respond appropriately. Responsibilities include:   + Providing indications and warning of potential threats, incidents, and attacks   + Information - sharing both inside and outside the government, including best practices, investigative information, coordination of incident response, and incident mitigation   + Analyzing cyber vulnerabilities, exploits, and attack methodologies   + Providing technical assistance   + Conducting investigations, forensics analysis, and prosecution   + Attributing the source of cyber - attacks   + Defending against the attack   + Supporting recovery efforts |

**APPENDIX TEN: Terms and Definitions**

|  |  |
| --- | --- |
| **Term** | **Definition** |
| **Bot-network Operators** | Bot-network operators take over multiple systems in order to coordinate attacks and to distribute phishing schemes, spam, and malware attacks. The services of these networks are sometimes made available on underground markets (e.g., purchasing a denial-of-service attack or servers to relay spam or phishing attacks). |
| **Cybersecurity** | The protection of information and property from theft, corruption, or natural disaster while allowing the information and property to remain accessible and productive to its intended users.  In addition, cybersecurity includes the safeguarding of computer systems, as well as the data contained within, and maintaining:  **Confidentiality** - The term used to prevent the disclosure of information to unauthorized individuals or systems.  **Integrity** - Means that data cannot be modified undetectably. Integrity is violated when a message is actively modified in transit.  **Availability** - Refers to the information's need to be available for any information system to serve its purpose. This means that the computing systems used to store and process the information, the security controls used to protect it, and the communication channels used to access it must be functioning correctly. |
| **Data Theft** | Describes when information is illegally copied or taken from a business or other individual. Commonly, this information is user information such as passwords, social security numbers, credit card information, other personal information, or other confidential corporate information |
| **Denial of Service (DOS) Attack** | The prevention of authorized access to a system resource or the delaying of system operations and functions. This often involves cyber criminals generating a large volume of data requests. |
| **Distributed Denial of Service (DDoS)** | Employs thousands of hijacked computers or internet-connected devices to deliver the data requests. |
| **Hacktivist** | A hacker who attacks information systems with the intent to advance a particular social or political agenda. |
| **Industrial Control System** | An information system used to control industrial processes such as manufacturing, product handling, production, and distribution. Industrial control systems include supervisory control and data acquisition systems (SCADA) used to control geographically dispersed assets. |
| **Malware** | A virus, worm, Trojan horse, or other program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim’s data, applications, or operating system.  Common types of malware include:  n **Virus** - (e.g. Melissa):  o Malware that is parasitic in nature and replicates by copying itself to other programs  o Not able to self-replicate, requires a host file  n **Worm** - (e.g. ILOVEYOU, Code Red):  o Causes maximum damage to corporate information  o Self-replicates across networks, without a host file, through inbuilt email or scan engines  n **Trojan** - (e.g. Bowling for Elves):  o An "impostor," a program that appears legitimate, but contains malicious code, and does not self-replicate  o Can be a carrier for a virus |
| **Phishing** | Soliciting private information from customers or members of a business, bank or other organization in an attempt to fool them into divulging confidential personal and financial information. People are lured into sharing user names, passwords, account information or credit card numbers, usually by an official-looking message in an email or a pop-up advertisement that urges them to act immediately, usually by clicking on a link provided. |
| **Ransomware** | A subset of malware in which the data on a victim's computer is locked, typically by encryption, and payment is demanded before the ransomed data is decrypted and access returned to the victim. |
| **Social Engineering** | A euphemism for non-technical or low-technology means (such as lies, impersonation, tricks, bribes, blackmail and threats) used to attack information systems via an organization’s staff. |
| **Spammers** | Individuals or organizations distribute unsolicited e-mail with hidden or false information in order to sell products, conduct phishing schemes, distribute spyware/malware, or attack organizations (i.e., denial of service). |
| **Supervisory Control and Data Acquisition (SCADA)** | A process control application or system that collects data from sensors and machines locally or in remote locations and sends the data to a central computer for management and control. |
| **Website Defacement** | An attack on a website that changes the visual appearance of the site or a webpage. These are typically the work of system crackers, who break into a web server and replace the hosted website with one of their own. Most times, the defacement is harmless, however, it can sometimes be used as a distraction to cover up more sinister actions such as uploading malware or deleting essential files from the server. |

# ANNEX A: Information Technology Employee Code of Conduct

## Purpose and Scope

The purpose of the Information Technology (IT) Employee Code of Conduct is to outline responsibilities, guidelines, and standards of conduct for all IT employees who have access to sensitive information. We intend that this code will emphasize that you are a professional who is resolved to uphold ethical obligations and ideals. You should be committed to maintain the integrity and confidentiality of the computer systems with which you interact for the benefit of all involved. While IT employees must always be guided by their own professional judgment, we hope that consideration of this code will help when difficulties arise.

This IT Employee Code of Conduct applies to all IT employees. The code is directed specifically at those who have access to sensitive information, such as those who are responsible for the maintenance of computer networks, databases, electronic mail (e-mail), Internet connectivity, telephones (including cellular phones), pagers, voice mail, fax transmissions, modems, multimedia, video, and all other computer-related communications. Technologies, facilities, and other information resources used for information processing, transfer, storage, and communications are also included.

The IT Director, chief appointed or elected official, and/or legal counsel reserve the right to amend this Code of Conduct at any time and for any reason.

### Code of Conduct

Due to the nature of IT’s role, IT employees will come into contact with privileged information on a regular basis. The IT employee has the duty to the owners of the information to protect the confidentiality of all such information. This includes making changes, preventing unauthorized access, or not divulging that information to a third party. IT employees shall not use, seek or access information without a clear business purpose as would be reasonably acceptable to the IT Director and/or the department who is the custodian of such information.

All appropriate effort should be made by the IT employee, in accordance with industry-accepted practices, to enforce security measures to protect computer systems and the data contained in them. This includes regularly maintaining software and hardware, preventing unauthorized user access, analyzing levels of system performance and activity, and other security-related duties.

IT employees must uphold the policies, procedures, and laws that govern the systems and networks with which they interact, and make all efforts to ensure the same from the users of the systems.

IT employees will not exercise their powers to access private information other than is necessary for their role, and then only to a degree that is necessary to perform that role, while remaining within established policies and procedures. Any private information obtained by the IT employee may not be used for personal use, and must be kept confidential.

IT employees will not access other employee’s offices or work spaces unless they have permission to do so. In addition, prior to providing desk side support, IT employees will contact the staff member they are going to be working with to ensure that they are available. If the staff member cannot be reached or is otherwise unavailable, the IT employee will reschedule the visit to a time when the staff member is available or the IT employee will touch base with a supervisory employee in the same division or department of the staff member to let them know what they are doing.

The IT employee must keep users informed about computing matters that may affect them, such as sharing of common resources, maintenance, security, conditions of acceptable use, occurrence of system monitoring, and any legal matters. This information must be presented in a manner designed to ensure user understanding and awareness.

An IT employee will answer questions and give support in a timely and effective manner, while openly declaring any limitations of personal knowledge and conflicts of interest.

## Incidents of Inappropriate Use

This section of the code governs the role of the IT employee dealing with incidents of suspected inappropriate use of communication and computing facilities.

IT employees who encounter cases of suspected inappropriate use who are advised by a third party, or in the course of their duties, **shall immediately inform the IT Director or designee** and shall be governed by the procedures below for dealing with inappropriate use.

**Account locking and suspension of access:** This action will prevent users from accessing their account and subsequently the information therein. User accounts, including IT employee accounts, may be locked by the IT Director or designee after consultation with the chief appointed and/or elected official, legal counsel, and/or the appropriate Department Director(s) when:

· There is a threat to system or network security that requires the account to be disabled.

· There are reasonable grounds to believe that the account is responsible for an event or series of events that seriously degrade system or network performance to the extent that it compromises the other users’ ability to continue work.

· There are reasonable grounds to believe that the security of the account itself has been jeopardized.

· To seal the account and evidence contained within because there is reason to believe that criminal or other charges, such as a breach in appropriate access and use of confidential information, will be laid against the user of the account.

· An existing problem, that would otherwise not require this reaction, has persisted despite trying to contact the account owner repeatedly.

· There are reasonable grounds to believe that the account has engaged in unauthorized use and/or personal use of sensitive information.

· Accounts that have been locked in connection with one of the above scenarios will be unlocked as soon as the conditions that required the lock no longer exist.

**Access to electronic files and communications:** the organization has the right to access electronic communications for organization-related purposes, which may include, but are not limited to:

· Retain or delete any or all computer files, e-mail messages, or electronic data on systems after an employee leaves the organization.

· Comply with demands and requests, such as subpoenas, search warrants, legal holds, open records requests, audits, and other requests to which the organization is legally required to respond.

· Obtain information relating to situations involving the health or safety of people or property, actions brought on behalf of the organization and any of its employees, and actions brought against the organization and any of its employees.

· Maintain system integrity, including maintenance, virus tracking, performance of ordinary system repair, and enhancement.

· Perform internal investigations, such as safety and security, as requested by the chief appointed and/or elected official, the legal counsel, or any Department Director.

### Incident Log

IT employees are obligated to maintain an incident log which will be reviewed on a regular basis by the IT Director or designee. All incidents of suspected inappropriate use should be recorded in the log, along with any follow-up actions. All incidents should be logged until the time that they are resolved, especially if disciplinary action is considered, recommended, or implemented. Incident reports should consist at minimum of the following information:

· Date and time of the incident.

· Information about the accounts involved.

· Name and job title of the account holder.

· The type of use/abuse suspected.

· IT employee’s name.

· Any further action suggested, requested, or required.

### Procedures for Dealing with Incidents of Suspected Abuse

IT employees who discover, or who are privy to information about, an incident that appears to be an inappropriate use of communication and computing facilities will follow these steps:

1. Record all relevant details and any follow-up action in the incident log. Promptly inform the IT Director or designee who will inform the Department Director of the affected department of any computing incidents that clearly compromise system or network integrity. Incidents include, but are not limited to: data loss or theft, inappropriate systems or information access, notification from outside individuals or institutions of any incident, and any other breach or violation of IT procedures of which the IT employee is aware.

2. If appropriate, the IT Director or designee will arrange for the affected computer device to be removed from the network and will notify appropriate personnel in IT and the appropriate Department Director.

3. In cases where disciplinary action is not required, the IT Director or Designee will notify the account owner of the incident and their Department Director, and request an explanation via e-mail, phone, or fax. If repeated attempts to contact the account owner fail to resolve the issues, the account may be locked.

4. In cases where disciplinary action is required, the IT Director or designee will notify the offender’s Department Director and recommend a course of action.

5. The IT Director or designee will perform any follow-up action as directed and authorized. This may include temporary restriction of access to accounts by the account owner, deletion or examination of material in the user account, deletion of accounts, or other appropriate steps.

## Disciplinary Action

Any employee, who is found to have violated this Code of Conduct, the guidelines herein, or the organization’s Personnel Policies and Procedures, may be subject to disciplinary action, up to and including termination of employment.

## Agreement

I have read and understand the Code of Conduct. I understand that if I violate the rules explained herein, I may face legal or disciplinary action according to applicable law or the organization’s policy.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Employee Name (print)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Employee Signature Date