Incident Response Plan Template

This document describes the plan for responding to information security incidents at the [AGENCY NAME]. It defines the roles and responsibilities of participants, characterization of incidents, relationships to other policies and procedures, and reporting requirements. The goal of this any subcontractor Incident Response Plan is to detect and react to computer and network security incidents, determine their scope and risk, respond appropriately to the incident, communicate the results and risk to all stakeholders, and reduce the likelihood of the incident from reoccurring.

Scope

This plan applies to the [AGENCY NAME]'s Servers, Systems, Applications, Networks and Data. The scope includes any person or device that has access to any system, network or data that is operated or supported by [AGENCY NAME].

Goals

The main goals of this plan are as follows:

- Proactive Goals
    - Assure integrity of critical information assets.
    - Detect intrusion, misuse, and other negative events.
    - Recover systems, data, and services.
    - Contain intrusions and negative incidents.

- Reactive Goals
    - Investigate the source or cause of an incident.
    - Facilitate and control communication with internal and external agencies.
    - Investigate in a manner that will allow prosecution where appropriate.
    - Develop and follow a Suspicious Activity Reporting procedure.

- Reactive Proactive Goals
    - Allow for trend analysis, on-going risk assessment, and mitigation.
    - Educate the Cyber Security Incident Response Team (CSIRT)
    - Heighten awareness of appropriate team members.
    - Update Decision Tree

Priorities

The following priorities serve as a starting point for defining our organization's response:

1. Protect client information and assure organizational data integrity.
2. Maintain the [AGENCY NAME]'s reputation and control external communication.
3. Prevent damage to systems.
4. Minimize disruption of computing resources.

Maintenance

The Director of the Computer, Network and Telecommunications Support Department will be responsible for the maintenance and revision of this document.

Relationship to other Policies

This plan incorporates aspects of several [AGENCY NAME] Administrative Rules and Regulations and Superintendent Policies. They include SP 1002 (Employee Use of Technology and the Internet), ARR 3080.0 (Acceptable Use Agreement), ARR 3600 (Employee Use of Equipment and Facilities), ARR 6130 (Student Use of Technology) and ARR 3090 (Electronic Document Retention and Archiving). This plan also relates to [AGENCY NAME]'s Vulnerability and Patch Management Policy and Disaster Recovery and Business Continuity Plans.

Definitions

Event

An event is an exception to the normal operation of IT infrastructure, systems, or services. Not all events become incidents.

Incident

An incident is an event that, as assessed by the IT security staff, violates the Acceptable Use Agreement or other policies, standards, or code of conduct, or threatens the confidentiality, integrity, or availability of Information Systems or agency data.

Incidents may be established by review of a variety of sources including, but not limited to:

Network and Server monitoring systems, service degradations or outages, or reports from various sources, [AGENCY NAME] staff or outside organizations.

Discovered incidents will be declared and documented via electronic mail or in an IT Ticket/Documentation System.

Complete IT service outages may also be caused by security-related incidents. Service outage procedures are detailed in the Business Continuity Plan.

Incidents will be categorized according to their potential for sensitive or restricted data exposure or criticality of resource using a severity rating outlined later in this document. The initial severity rating may be adjusted during plan execution.

Detected vulnerabilities will not be classified as incidents. The CNTS Department employs tools to scan [AGENCY NAME]'s network environment and depending on severity of found vulnerabilities may warn affected users, disconnect affected machines, or apply other mitigations. In the absence of indications of sensitive data exposure, vulnerabilities will be communicated to the Director of IT and available technology remedies will be explored to reduce that risk.

Personally Identifiable Information (PII)

For the purpose of meeting security breach notification requirements, PII is defined as a person's first name or first initial and last name in combination with one or more of the following data elements:

- Social security number
- State-issued driver's license number
- State-issued identification card number
- Financial account number in combination with a security code, access code or password that would permit access to the account
- Medical and/or health insurance information

Roles and Responsibilities

Director of IT

The Director of IT, working jointly with the Assistant Superintendent of Technology Services, is responsible for classifying the incident as one potentially requiring immediate action (and thus an emergency meeting of the CSIRT) or a minor incident requiring review in a CSIRT meeting.

Chief Information Security Officer (CISO)

The Director of IT is also [AGENCY NAME]'s Chief Information Security Officer. As such, he may engage an IT security consulting company to provide virtual CISO services via a highly credentialed information security consultant who is familiar with [AGENCY NAME]'s computing environment, IT staff, and methods and processes. The CISO will be called upon in case of a cyber-security incident to:

- Determine the physical and electronic evidence to be gathered as part of the Incident Investigation.

- Manage and collect forensic evidence, and participate as contact person between [AGENCY NAME] and law enforcement.
- Provide guidance throughout the response process, including coordinating forensic investigations, and communication with Law Enforcement.

Incident Response Coordinators (IRC)

Depending on the nature of the incident, [AGENCY NAME]'s Systems Engineer and/or Network Coordinator will be responsible for assembling all the data pertinent to an incident, communicating with appropriate parties, ensuring that the information is complete, and reporting on incident status both during and after the investigation.

Incident Response Handlers (IRH)

Incident Response Handlers are members of the IT Division staff or outside contractors who gather, preserve and analyze evidence so that an incident can be brought to a conclusion.

Insider Threats

Insiders are current or former employees, contractors, or business partners who have access to restricted data and may use their access to threaten the confidentiality, integrity or availability of [AGENCY NAME]'s IT information or systems. This particular threat is defined because it requires special organizational and technical amendments to the Incident Response Plan as detailed below.

Law Enforcement

Law Enforcement includes federal and state law enforcement agencies, and U.S. government agencies that present warrants or subpoenas for the disclosure of information. Interactions with these groups will be coordinated with [AGENCY NAME]'s Legal Counsel (see below).

Legal Counsel

[AGENCY NAME]'s Legal Counsel will be the liaison between [AGENCY NAME]'s Cabinet, the incident handling team, and outside Law Enforcement, and will provide counsel on the extent and form of all disclosures to law enforcement and the public.

Users

Users are members of the [AGENCY NAME] community or anyone accessing an Information System, Data or [AGENCY NAME] networks who may be affected by an incident.

Methodology

This plan outlines the most general tasks for Incident Response and may be supplemented by specific internal guidelines and procedures that describe the use of security tools and/or channels of communication. These internal guidelines and procedures are subject to amendment as technology changes.

Staffing for an Incident Response Capability

The CNTS Department will utilize its staff and third-party augmentation (outside security consulting services) to investigate each incident to completion and communicate its status to other parties while it monitors the tools that detect new events.

Training

The continuous improvement of incident handling processes implies that those processes are periodically reviewed, tested and translated into recommendations for enhancements.

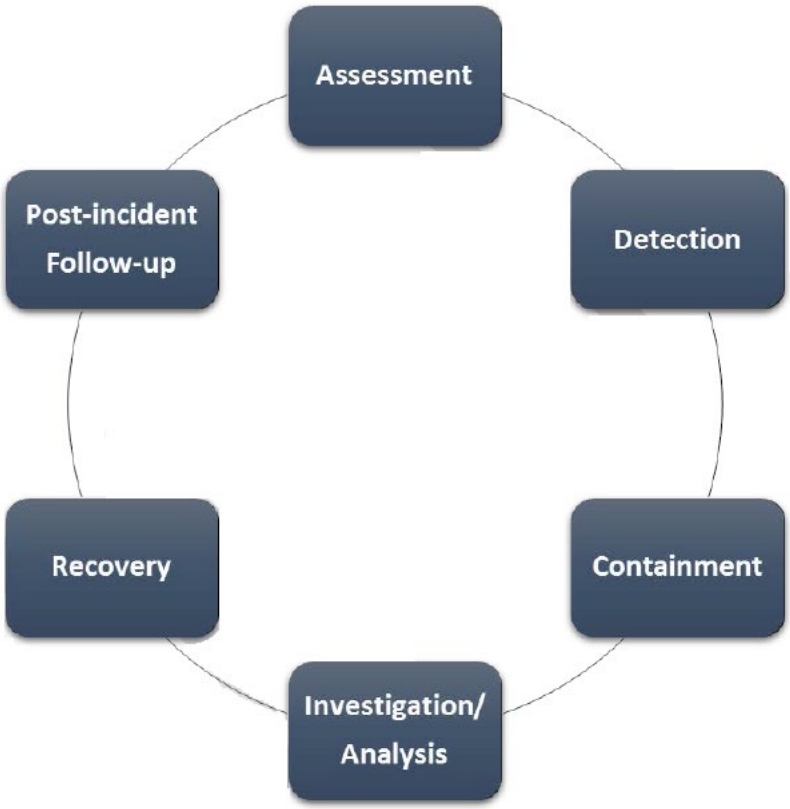
The CNTS staff will be periodically trained on procedures for reporting and handling incidents to ensure that there is a consistent and appropriate response to incidents, and that post-incident findings are incorporated into procedural enhancements.

Intrusion Detection Procedure

- All of [AGENCY NAME]'s employees will be trained to "broadcast awareness," meaning they will inform all appropriate persons in real time of suspicious activities. All suspected and/or confirmed instances of attempted and/or successful intrusions must be immediately reported to IT.
- The IT department members will be trained by the Director of IT on how to report potential issues to the CSIRT for investigation as they troubleshoot and maintain [AGENCY NAME]'s systems.
- All incidents will be carefully assessed by the Director of IT to determine appropriate action and ensure necessary reporting requirements are met. Reporting based on system availability and customer information breach is described below.
- Based on the nature and scope of the incident, technical staff and the Director of IT shall decide whether the incident can be resolved locally or whether additional assistance is required from the CSIRT or other outside sources.
- Operating system, user accounting, and application software audit logging processes must be enabled on all host and server systems.
- Alarm and alert functions of any firewalls and other network perimeter access control systems must be enabled.

Incident Response Phases – Remedial and Containment Action

Guided by NIST SP 800-61 (Computer Security Incident Handling Guide), [AGENCY NAME]'s IT overall response to a Cyber Security Incident encompasses six phases: Assessment, Detection, Containment, Investigation, Remediation and Recovery, and post-incident follow-up.



Assessment (See Appendix D)

Many activities can indicate a possible attack. For example, a network administrator performing legitimate system maintenance might appear similar to someone launching some form of attack. In other cases, a misconfigured system might lead to a number of false positives in an intrusion detection system, which could make it more difficult to spot genuine incidents.

The purpose of this phase is to:

- Take steps to determine whether this is an actual incident or a false positive.
- Gain a general idea of the type and severity of attack. Information will be gathered to be researched and used to begin containing the damage and minimizing the risk.
- Record actions thoroughly. These records will later be used for documenting the incident (whether actual or false).

Detection

Detection is the discovery of the event with security tools or notification by an inside or outside party about a suspected incident. This phase includes the declaration and initial classification of the incident.

Containment

A quick response can make the difference between a minor and a major security incident. The exact response will depend on the nature of the attack. As a starting point, however, the following will be the priority of the response plan:

1. Protect human life and people's safety.
2. Protect Client and Agency data - including proprietary, sensitive, and managerial data.
3. Protect hardware and software against attack. This includes protecting against loss or alteration of system files and physical damage to hardware.
4. Minimize disruption of computing resources. Although uptime is very important in [AGENCY NAME]’s environment, keeping systems up during an attack might result in greater problems. For this reason, minimizing disruption of computing resources should be a lower priority than protecting agency data and systems.

There are a number of measures that can be taken to contain the damage and minimize the risk to our environment. Those measures will be invoked by the Director of IT, depending on the situation at hand.

Investigation & Analysis

In order to recover effectively from an attack, it is necessary to determine how seriously the affected systems have been compromised. This will influence how to further contain and minimize the risk, how to recover, how quickly and to whom the incident must be communicated, and whether to seek legal redress.

An attempt will be made to:

- Determine the nature of the attack (this might be different than the initial assessment suggests).
- Determine the attack point of origin.
- Determine the intent of the attack. Was the attack directed at [AGENCY NAME] to acquire specific information, or was it random?
- Identify the systems that have been compromised.
- Identify the files that have been accessed and determine the sensitivity of those files.
- Determine whether unauthorized hardware has been attached to the network or whether there are any signs of unauthorized access through the compromise of physical security controls.
- Examine key groups (domain administrators, administrators, and so on) for unauthorized entries. Use tools like "Change Notifier" for Active Directory to detect unauthorized changes to the Active Directory domain accounts.
- Search for security assessment or exploitation software. Cracking utilities are often found on compromised systems during evidence gathering.
- Look for unauthorized processes or applications currently running or set to run using the startup folders or registry entries.
- Search for gaps in, or the absence of, system logs.
- Review intrusion detection system logs for signs of intrusion, which systems might have been affected, methods of attack, time and length of attack, and the overall extent of potential damage.
- Examine other log files for unusual connections; security audit failures; unusual security audit successes; failed logon attempts; attempts to log on to default accounts; activity during nonworking hours; file, directory, and share permission changes; and elevated or changed user permissions.
- Compare systems to previously conducted file/system integrity checks. This will enable identifying additions, deletions, modifications, and permission and control modifications to the file systems or security logs.

Recovery

The goal of this phase is to return the system to normal operation. System recovery will generally depend on the extent of the security breach. Working with the Director of IT, the IT team will determine whether the existing system can be restored, or if it is necessary to completely rebuild the affected system.

Post-incident Follow Up

Once the documentation and recovery phases are complete, the CSIRT will review the process thoroughly and determine which steps were executed successfully and where mistakes were made. This review will identify processes that need to be modified and reflected in the Response Plan.

Severity Rating Category

For the purposes of this Plan, a Cybersecurity incident is an event that is perceived or proven to be an attack on the security of [AGENCY NAME]'s computing systems. Such events can be a virus, phishing, or other attacks initiated by an outside party for the purpose of gaining unauthorized access to data, systems or other aspects of [AGENCY NAME]'s business records, network, or computing systems. To simplify the response process, the Director of IT will assign one of the following four severity ratings to incidents as they are reported.

Severity	Symptoms	Action
Reportable (1)	• Minimal impact to small segment of user population; completely localized, with few individuals affected; presenting little or no risk to other entities. • No loss or compromise of sensitive data. • An isolated cybersecurity attack that can be handled by compensating controls.	• Remedial action. • Notification of IT management

	(Examples include a cybersecurity attack that resulted in a single event with no data loss/business compromise; Phishing, virus to a local machine; all incidents that will not affect operation of business.)	
Minor (2)	• Some adverse impact to business • Impact is localized or contained, or minimal risk of propagation. • No apparent release or compromise of sensitive data. (Example: Any security incident which has been successfully responded to and which does not have the potential, over time, to affect inherent operational or reputational risk.)	• Remedial action. • Notification of IT management • Report to the CSIRT in writing
Major (3)	• Penetration or denial of service attacks attempted with limited impact on operations or larger widespread instances of a new cybersecurity attack not handled by compensating controls or training. • Event that adversely impacts a non-critical [AGENCY NAME] system or service • A cybersecurity attack that results in financial loss or public reputational damage	• Remedial action. • Notification of IT Management & Security Team • Report Incident to Assistant Superintendent of Technology Services and Cabinet • Involve the Communications Department if needed • Report to the CSIRT in writing • Log in FBI incident database

	(Examples include: a phishing scam that has resulted in financial loss, or a cybersecurity attack that impacts business to such a degree that limited impact is observed.)	
Critical (4)	• Successful penetration or denial of service attacks detected with significant impact on operations. • Significant risk of negative financial or public relations impact may result. • Any incident which has disabled or will disable, partially or completely the central computing facilities, and/or the communications network for a period of more than 12 to 48 hours. (Examples include a cybersecurity attack as notified by the FBI or some other law enforcement agency, a cybersecurity risk that exposes confidential data to the public, or a cybersecurity risk that becomes public knowledge leading to significant business impact.)	• Invoke Business Continuity Plan (BCP) if all services are down. • Remedial and containment action. • Notification of IT management & Security • Notify Cabinet and Communications Department • Notify authorities (i.e., FBI and local police) • Document incident and report to the CSIRT in writing

Appendix A - Primary and Alternate Emergency Contact List

Department	Primary Contact	Alternate Contact
1. Information Technology		
2. Information and Systems Security		
3. Applications Development		
4. Applications Support		
5. Network and Telecommunications		
6. Systems and Databases		
7. Technical Support		
8. FBI Internet Crime Complaint Center	http://www.ic3.gov	
9. Sacramento Valley Hi-Tech Crimes Task Force	http://www.sacvalleyhitech.com/ 916-784-3002	

Appendix B – Incident Response Procedure

1. **Incidence Discovery Phase**
    a. The IT staff member or affected department staff member who discovers the incident will contact the Director of IT immediately to report the incident.
    b. The staff member should include the following information:
        i. Is the equipment affected business critical?
        ii. What is the severity of the potential impact?
        iii. Name of the system or person being targeted, along with the operating system, IP address and physical location.
        iv. IP address and any information about the origin of the attack.
2. **CSIRT Notification Phase**
    a. The Emergency Contact List is used to contact the Cyber Security Incident Response Team (CSIRT).
3. **Analysis and Assessment Phase (Incident Review)**
    a. The Director of IT will review the Incident Response Handling Procedure Flowchart (Appendix C) and determine if the incident is Reportable, Minor, Major or Critical.
    b. The following items will be considered when determining the incident severity:
        i. Is the incident real or perceived?
        ii. Is the incident still in progress?
        iii. What data or property is threatened and how critical is it?
        iv. What is the impact on the agency if the attack succeeds? (Minimal, serious or critical?)
        v. What system or systems are targeted and where are they located on the network?
        vi. Is the incident inside the trusted network, outside, or in the DMZ?
        vii. Is the response urgent?
        viii. Will the response alert the attacker? Do we care?
        ix. What type of incident is this (virus, worm, intrusion, abuse, damage, etc.?)
    c. Categorize the incident:
        i. Reportable – Disruption to a single person with minimal risk
        ii. Minor – Localized or minimal security risk without threat of compromised data
        iii. Major – Threat to sensitive data
        iv. Critical – Threat to critical systems or entire infrastructure possibly requiring implementation of the Business Continuity Plan.
    d. If the incident is major or critical, the Incident Response Team will meet in person or discuss the situation over the phone. The Incident Assessment Checklist will be completed to help determine a response strategy.

4. **Containment Phase**
    a. Containment action may require the following:
        i. Disconnection of the affected system(s)
        ii. Password changes
        iii. Block ports or connections from external IP addresses
5. **Incident Remediation and Response Phase (See Page 6)**
    a. The IRT will establish and follow one or more of the below procedures based on determination after completing the checklist. The team may create additional procedures which are not foreseen in this document. If there is no applicable procedure the team must document what was done and later establish a procedure for the incident.
        i. Worm/Virus/Spyware response procedure
        ii. Active/Inactive intrusion response procedure
        iii. System abuse procedure
        iv. System failure procedure
        v. Property theft response procedure
        vi. Website, Database or Network DOS response procedure
        vii. Event Log Review Procedure
    b. IRT members will use forensic techniques, including reviewing system logs, looking for gaps in logs, reviewing intrusion detection logs, and interviewing witnesses and the incident victim to determine how the incident was caused. Only authorized personnel should be performing interviews or examining evidence. Authorized personnel may vary by situation.
    c. Team members will recommend changes to prevent the occurrence from re-occurring or infecting other systems.
    d. Upon the approval of the Director of IT (and, if necessary, the Assistant Superintendent of Technology Services or Cabinet), the changes will be implemented.
6. **Notification Phase – (implemented sooner if needed)**
    a. Notify affected users
    b. Notify Assistant Superintendent of Technology Services
    c. Notify Cabinet members and Superintendent if Major or Critical incident
    d. Notify external affected stakeholders if data breach has occurred.
    e. Notify proper external agencies (police, FBI or other appropriate agencies).
    f. May be completed before or after System Restoration Phase (or both).
7. **System Restoration Phase**
    a. Team members will restore the affected system(s) to an “un-affected” state. They may do one or more of the following:
        i. Re-install the affected system(s) from scratch and restore data from backups. Preserve evidence before doing this. Save a copy of the server as evidence if possible.

ii. Require users to change passwords if they have been compromised.
iii. Ensure the system has been hardened by shutting off or uninstalling unused services or features.
iv. Ensure the system is fully patched and protected.
v. Ensure the virus protection is running.
vi. Ensure the system is logging events correctly and at the proper levels.

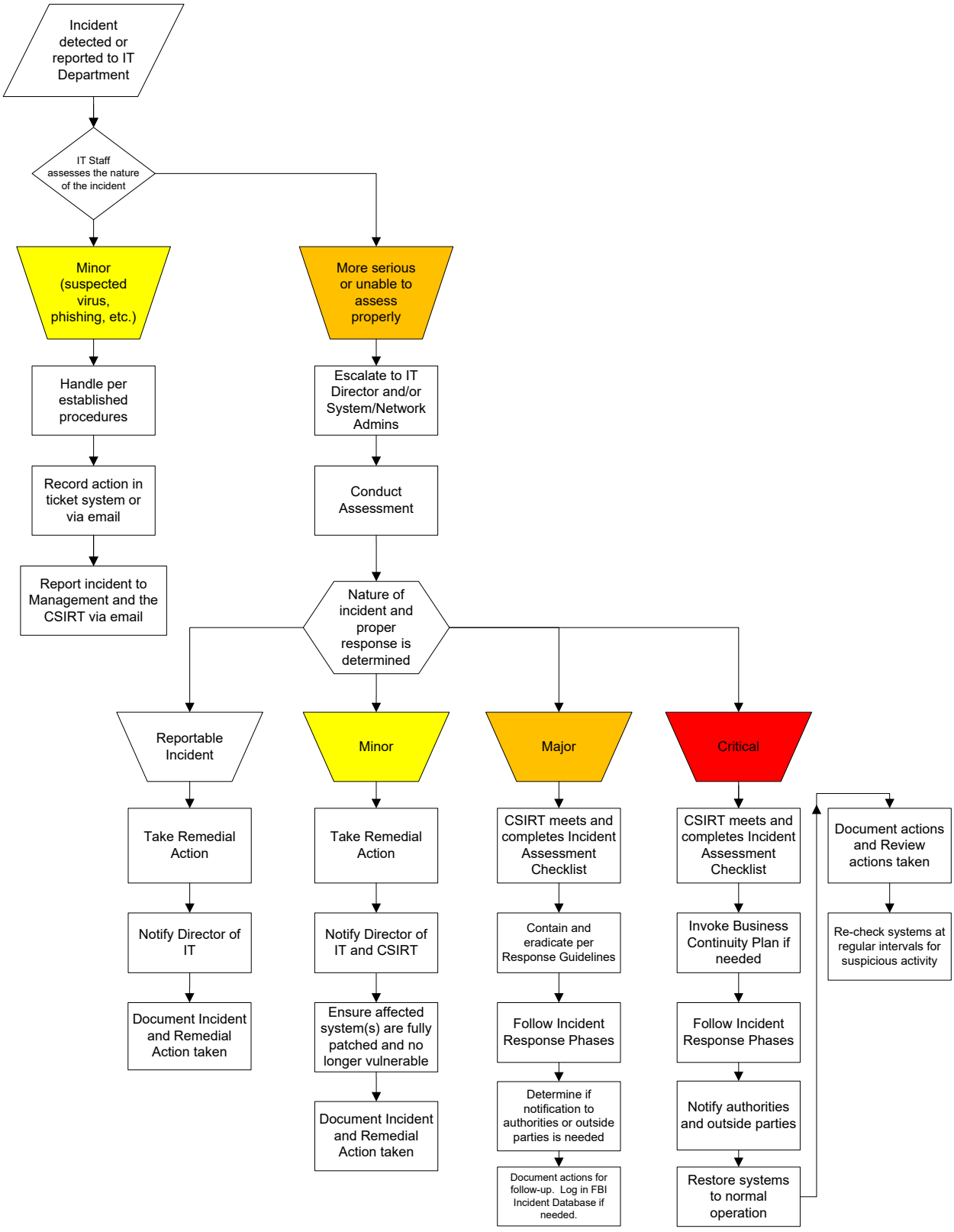
8. Documentation Phase

a. The following documentation will be kept by using the Incident Assessment Checklist:
   i. How the incident was discovered.
   ii. Severity Rating Category of the incident (Reportable, Minor, Major, Critical)
   iii. How the incident occurred (email, firewall, etc.)
   iv. Where the attack came from (IP address, physical address, other related info)
   v. What the response plan was.
   vi. What was done in response.
   vii. Whether the response was effective.
   viii. Recommendations for procedure improvement.
b. Evidence Preservation – make copies of logs, email, other evidence. Keep lists of witnesses. Keep evidence as long as necessary to complete prosecution.

9. **Assessment and Review Response Phase**

a. Assess damage and cost to organization and cost of containment efforts.
b. Review response and update policies
   i. Consider whether an additional policy could have prevented the intrusion. Should any security policies be updated?
   ii. Consider whether a procedure or policy was not followed which allowed the intrusion. Consider what could be changed to ensure the procedure or policy is followed in the future.
   iii. Was the incident response appropriate? Could it be improved?
   iv. Were the incident response procedures detailed and did they cover the entire situation? Can they be improved?
   v. Was every appropriate party informed in a timely manner?
   vi. Could changes be made to prevent re-infection? Have all systems been fully patched, locked down, passwords changed, antivirus updated, etc.?
   vii. What lessons have been learned from this experience?

Appendix C - Incident Response Procedure Flowchart



Appendix D - Incident Assessment Checklist

The activities described in this checklist are designed to assist in the initial assessment process performed and/or conducted by the Cyber Security Incident Response Team (CSIRT) Lead.

Completion of this checklist is essential for any incident that calls for the execution of the Information Security Incident Response Protocol. Once the Incident Response Team is assembled, the Assessment Checklist is reviewed for completion to ensure all pertinent facts are established.

A. Description of Incident - Data relevant to the Incident should be collected for use in the process of Incident determination.
A1. Record the current date and time.
A2. Provide a brief description of the Incident.
A3. Who discovered the Incident? Provide name and contact information.
A4. Indicate when the incident occurred and when it was discovered.
A5. How was the Incident discovered?
A6. Describe the evidence that substantiates or corroborates the Incident (e.g., eye-witness, time-stamped logs, screenshots, video footage, hardcopy, etc.).

A7. Identify all known parties with knowledge of the Incident as of current date and time.
A8. Have all parties with knowledge of the Incident been informed to treat information about the Incident as “sensitive or confidential”?
B. Types of Information, Systems and Media - Provide information on the nature of the data that is relevant to the Incident.
B1. Provide details on the nature of the data (e.g., email, agency data, client data, etc.).
B2. Does the information (if compromised) constitute a violation of regulatory requirements or [AGENCY NAME]’s policies? Describe what is known.
B3. Was the compromised information maintained by [AGENCY NAME] or a 3rd Party (i.e., outside agency, etc.)? Provide details.
B4. How was the information held? Identify the types of information systems and/or the media on which the information was stored (e.g., server, laptop, USB drive, etc.).

B5. If the information was held electronically, was the data encrypted or otherwise disguised or protected (e.g., redacted, partial strings, password required, etc.)? If so, describe measures taken.
B6. What steps are required or being taken to preserve evidence of the Incident? Describe.
C. Risk/Exposure - Attempt to determine to what extent risk and/or exposure is presented by this Incident.
C1. Can we reasonably determine the risk or exposure?
C2. To what degree are we certain that the data has or has not been released?
C3. Do we have contact with someone who has "firsthand" knowledge of the circumstance (e.g., the owner of a stolen device, laptop, etc.)? Provide name and contact information.
C4. What firsthand knowledge have we determined? Describe what is known.
C5. Can we identify and do we have contact with the party that received the data or caused the compromise? Describe what is known.
C6. Identify the impacted parties, if possible.

C7. What is the risk or exposure to [AGENCY NAME]? Describe.
C8. What is the risk or exposure to the Client? Describe.
C9. Can we determine to what extent news outlets may know of this Incident? Describe.
D. Next Steps - Determine what information or action is required to better assess or address this Incident.
D1. Do we have enough information to establish the category and severity of the Incident? - If “yes”, declare the Incident category and severity. - If “no”, describe what else might be required.
D2. If additional data collection data is required, assign responsibility to CSIRT member for collection and reporting to CSIRT.
D3. Is there any deadline or reporting requirement (self-imposed or regulatory) we need to address?
D4. What communications need to be established?
D5. Are there any immediate issues that have not been addressed? Describe.

E. Documentation – Document the incident and determine preventative steps so the incident can be avoided in the future.
E1. What steps were taken to address the incident? What response plan was followed?
E2. Was the response plan effective? If so, why?
E3. How could the response plan be improved?
E5. Have changes been made to prevent a re-occurrence of the incident or re-infection? Have all of the systems been patched, locked down, etc.?
E6. Should any security policies be updated?
E7. What did we learn from this experience?

Appendix E - Technical Controls

[these are just example older controls – enter your own here, which may include additional categories not listed]

1. Virus Protection

- Trend Micro Deep Security for servers in the virtual infrastructure
- Trend Micro Deep Security for virtual desktops in the virtual infrastructure
- Sophos Antivirus for desktops and laptops
- Both systems are configured for on-line scanning
- Weekly scans for Sophos
- Daily virus definition updates
- Malicious activity alert notifications are sent to the IT Service Desk for investigation.
- Antivirus detection on Internet connection through Palo Alto firewall

2. Spam Filtering

- Microsoft Office 365 for filtering incoming SPAM email messages
- Barracuda Anti-Spam server for filtering list server SPAM

3. Content Filtering

- Lightspeed Systems used for Web filtering and activity reporting
- Palo Alto firewalls used to monitor all Internet activity
- Access controls and policies are used to control Internet traffic.
- Content filters are used to block pornographic, inappropriate and malicious websites.

4. Spyware screening

- Palo Alto Networks Spyware prevention
- Sophos anti-virus and MalwareBytes

5. Intrusion Prevention System

- Palo Alto firewalls

6. Periodic User Alerts

- The CNTS Department sends out periodic alerts to all [AGENCY NAME] employees, alerting them about potential phishing, malware or other security exploits that may be received via electronic mail.
- Employees are reminded to <u>never</u> click on any links included in email messages and always double check with a tech support staff if a message appears suspicious but may be work related. Otherwise they should delete the email message.