CYBERSECURITY INCIDENT MANAGEMENT PLAN

Date

Company Name

DATA DEFENDERS®
Defenders of the Information World™

Version #

Table of Contents

1 Introduction

This Information Security Incident Response Plan (IRP) is a component of CUSTOMER's overall Information Security Program strategy. This IRP is intended to complement existing CUSTOMER Standard Operating Procedures (SOPs). It does not supersede existing processes unless explicitly called out in an investigation or incident.

There are three objectives of this IRP.

- **Objective #1 -** The first objective is that this IRP is developed in accordance with CUSTOMER as well as other regulatory policies to be used as a tool to help ensure and maintain the confidentiality, integrity, and availability of the CUSTOMER's information systems and information assets.
- **Objective #2 -** The second objective of this IRP is to provide an overarching framework for incident response that will be applied to every CUSTOMER agency as well as specific guidance and direction defined for three general categories of incidents as uniquely outlined for each CUSTOMER agency.
- **Objective #3 -** The third objective of this IRP is to provide a mechanism for mitigating such events in as timely a manner as possible to minimize the negative impact to CUSTOMER's business operations.

As a key concern of the CUSTOMER's overall information security strategy, it is essential to have in place a structured, well-planned approach to the execution and management of Information Security Incident Responses. This document provides an Information Security Incident Response Plan that is consistent with the CUSTOMER's Information Security Policy.

This IRP will provide the following guidance:

- A structured mechanism for determining if an event should be categorized as an incident to be handled by the CIRT or an operational event to be addressed within normal CUSTOMER IT management procedures.
- A structured yet flexible mechanism for triaging, containing, remediating, and recovering from incidents in the most appropriate and efficient manner.
- A structured mechanism for mitigating the adverse impacts of incidents to CUSTOMER and its business operations by applying appropriate safeguards as part of the incident response, in conjunction with a business continuity plan.
- A structured mechanism for ensuring and conducting the lessons learned Follow-Up phase after IR activities have concluded to improve the implementation and use of information security safeguards and advance the overall Information Security Incident Response framework and to minimize the probability of similar events occurring in the future.

This IRP is developed in two parts:

- **IRP General Framework**

The General Framework provides CUSTOMER's overall incident response paradigm. This general framework will serve as the foundation of CUSTOMER's Incident Response Plan.

- **IRP Categorized Incident Guidelines**

  These Categorized Incident Guidelines will define a specific response plan for each Major Incident Category as defined below. Information Security related incidents can be categorized into the following three major categories.

  - Malware Infection
  - Network/System Security Breach
  - Data Loss/Privacy Breach

  Categorizing incidents that occur into one of these major incident categories serves to direct the related response execution down an appropriate path meant to establish efficiencies in the response effort and to provide guidance and direction for the response activities that are to be executed based on the category of the incident.

1.1 IRP Process Description Summary

The IRP within the Information Security Office (ISO) will provide some or all of the following services as appropriate based on CUSTOMER needs:

- Incident handling
- Incident analysis and/or support
- Incident response on site
- Incident response support
- Incident response coordination

Reports should be created at the conclusion of the IRP execution process that will provide:

- Details on the nature of the incident
- Details on the incident handling process performed
- Lessons learned and continuous improvement plans

1.2 IRP Overview

This IRP document is divided into the following sections:

- **Purpose and Scope**

  This section defines the overall purpose and scope of this IRP including what the IRP document will cover. Anything not specifically listed in this section will be considered out of scope for this document.

- **Computer Incident Response Team (CIRT) Structure**

  This section defines the structure of the CIRT for the general framework and each major incident category. The major components of the CIRT will be identified including specific individuals, their roles, and responsibilities.

- **CIRT Contact List**

  This section defines a listing of contact information for each CIRT team member. The listing will provide a brief description of each team member's role and responsibility and a suggestion of when to contact each team member during the course of the IR activity.

- **IRP General Framework**

  This section defines the various phases of the IRP activities to be executed by the CIRT as part of its response efforts. This section will define the following phases of the IRP activity:

  - **Preparation Phase**

    This section provides guidance for conducting activities to prepare for incident response. The preparation phase will include:

    1. Document Policies and Procedures Preparation
    2. IRP Communication Protocols Preparation
    3. IRP Software Tools Preparation
    4. Critical System Images Preparation
    5. IRP Training Preparation
    6. CIRT Contact List Preparation
    7. IRP Testing

  - **Detection and Analysis Phase**

    This section defines general processes and procedures to collect and review incident artifacts or indicators of compromise to determine if the event under review is an incident or a normal operational concern to be handled by IT ops. The detection and analysis phase will include the following activities:

    1. Incident Triage
    2. Indicators of Compromise Review
    3. Escalation Decision Tree
    4. Evidence Collection, Preservation, and Handling

  - **Containment, Eradication, and Recovery Phase**

    This section defines the general activities to be executed during the IRP to contain the incident and any malicious activities associated with the incident, eradicate any software or system/network configuration changes made, and implement any technical/procedural countermeasures necessary to prevent any furtherance of efforts directly associated with the incident.

- **IRP Communication Protocol**

  This section defines the communication protocols to be used during IR activities to ensure that communications occur appropriately and securely between CIRT team members.

- **IRP Resources List**

  This section defines a listing of resources that can be used to support the IR activity such as secure communication bridge information, indicators of compromise artifacts/evidence storage resources, document templates for status reports, progress reports, resource requests, and more.

- **Incident Remediation Declaration**

  This section defines who will declare that all remediation activities are complete.

- **Post Incident Review**

  This section defines the post incident review objectives and provides guidance for conducting the review process to ensure that all pertinent information related to IR activity experiences can be appropriately shared, acknowledged, and captured to be used in the IR improvement process.

- **Document Management**

  This section defines who is responsible and what steps they will take to manage documentation for each incident.

1.3 IRP Purpose and Scope

1.3.1 Purpose

This IRP will serve as the official process of Information Security Incident Response for CUSTOMER. This document will introduce the General IRP Framework and will document the workflow, roles, procedures, and policies needed to implement a high quality incident response process. This document is a living document and should be analyzed and assessed on a regular basis. This IRP will define overall guidance, specific direction, oversight, support, and the appropriate resources to manage all activities related to the objective of mitigating an incident.

This policy defines the steps that the CIRT will use to ensure that security incidents are triaged, contained, investigated, and remedied. It also provides a process for documentation, appropriate reporting internally and externally, and communication as well as IRP follow-up so that organizational learning occurs. Finally, it establishes responsibility and accountability for all steps in the IRP.

1.3.2 Scope

This IRP applies to all Units and Departments for CUSTOMER, and any and all parts of its technology infrastructure that experiences an information security incident. It also applies to any computing device regardless of ownership, which either is used to store confidential data, or which, if lost, stolen, or compromised, and based on its privileged access, could lead to the unauthorized disclosure of confidential

data. Examples of systems in scope include, but are not limited to, a user's personally owned home computer that is used to store confidential data, or that contains passwords that would give access to confidential data. Additionally, the scope of this document is to define the Incident Response Process, from detection and analysis to post incident analysis.

The IRP provides the management structure for responding to any incident that impacts any part of CUSTOMER's business operation/facility. While the focus is on a physical incident, the notification and escalation framework can be applied to other situations as needed, such as loss of workforce, loss of a critical provider, or loss of technology.

The IRP is focused on the response and support for restoring business operations following a significant event. Emergency services/life safety are addressed within the CUSTOMER's Emergency Resources Emergency Action Guide (EAG).

1.4 IRP Terminology Definitions

Data Privacy Breach – An incident involving unauthorized access to CUSTOMER personable identifiable information or other protected privacy or privileged information.

Event – An issue involving unexpected operations of CUSTOMER information assets or processes.

Information Security Event – An identifiable occurrence of a system, service, or network state indicating a possible breach of information security policy or failure of safeguards, or a previously unknown situation that may be information security related.

Information Security Incident – A single or series of unwanted or unexpected Information Security Events that have a significant probability of compromising business operations and threatening information security.

Incident – An occurrence that actually or potentially results in adverse consequences to (adverse effects on) (poses a threat to) an information system or the information that the system processes, stores, or transmits and that may require a response action to mitigate the consequences.

1.5 IRP Ownership

The Information Security Office is responsible for creating this plan, reviewing the plan no less than yearly, auditing adherence to this plan, and updating this plan.

1.6 Exceptions

Exceptions to this plan must be approved by the CUSTOMER.

2 Computer Incident Response Team (CIRT) Structure

For each incident, it will be necessary to activate the appropriate components of the CIRT to respond to the incident as quickly and efficiently as possible. Individuals from some or all of these departments or teams will be brought together at different times during the IRP execution process. Both internal and external resources may be needed to respond to Incidents.

2.1 IRP CIRT Roles

All members should follow existing CUSTOMER production processes and procedures in responding or reporting production issues and incidents.

INCIDENT MANAGEMENT RESPONSIBILITIES AND ACTIONS

- ***Chief Information Security Officer (CISO)*** – All information security incidents must be reported to the CISO. If protected information is involved in an incident, the CISO will provide oversight or delegate during the investigation. The CISO is responsible for escalating incidents, defining/calling the notification tree, or determining whether incident response team activation is appropriate. The CISO assigns/shares this responsibility with the Incident Response Manager.
- ***Incident Response Manager (IRM)*** – This role is designated by the CISO. The IRM is also referred to as the Incident Response Team Leader (IRTL). The IRM is responsible for tracking and managing security incidents and for coordination and notification with other involved parties. The IRM is the single point of contact for gathering and distributing information related to the incident. They can escalate incidents or execute the call tree notifications.
- ***Incident Response Handler*** – This role's primary responsibility is to assist the IRM with all of the documentation and communication required throughout the IR lifecycle.
- ***Tactical Incident Response Team Members (TIRTM)*** – These individuals are responsible for performing technical analysis, support, and other technical tasks related to security incidents. This may include, but is not limited to log analysis, collection of technical information or evidence, technical incident interpretation, or coordination efforts.
- ***IT Technician*** – The IT Technician may be a CUSTOMER employee or a contractor. The functional role is to collect necessary information from a system involved in an incident and assist the System Owner with remediation efforts as appropriate.
- ***Forensic Analyst*** – The Forensic Analyst's role is to collect forensic evidence and to provide detailed forensic analysis of collected artifacts.

- ***System Owner*** – This can be a System, Network, or Database Administrator who provides information about the criticality of systems involved in an incident. The System Owner will also be responsible for the eradication and recovery phases of the Incident Response Lifecycle.

AUXILIARY ROLES

- ***ISO Security Lead*** – The ISO Security Lead serves as the interface between the IRM and any CUSTOMER contractors who may participate in an incident investigation.
- ***CUSTOMER Human Resources*** – Human Resources will be the point of contact with all internal (employee related) incidents.
- ***Incident Reporter*** – This can be any CUSTOMER employee, contractor, or third party. Upon suspecting an incident, the Incident Reporter is responsible for contacting the appropriate parties.
- ***NCC*** – Technical representatives from the NCC may be asked to participate in incident handling and to provide additional details/logs for analysis.
- ***Law Enforcement*** – Local or federal authorities (FBI, Secret Service) may be involved in the incident depending on the scale and/or physical security breach.
- ***Legal Counsel*** – CUSTOMER's legal counsel may be asked to advise on legal issues and/or review proposed breach notification materials for legal sufficiency. This legal analyst must be familiar with local, state, and federal computer crime statutes, electronic evidence standards, investigative procedures, and civil and criminal litigation processes.
- ***President's Office/Elected Official's Office*** – The President's Office/Elected Official's Office may be involved with incidents requiring public or CUSTOMER-wide communications.
- ***Subject Matter Expert (SME)*** – The SME can be a CUSTOMER employee or contractor who can provide additional business or technical details about systems or information involved in an incident.
- ***Support/Help Desk*** – The support desk or help desk should have knowledge of the Incident Response process as they will in many cases be the potential first point of contact for customer support related to an incident. They will need to understand what denotes a security incident and when to call an IR lead.
- ***Executive Management*** – Executive Management's role will vary and is limited to those that have a stake in the incident. They will provide administrative support and authorization to those involved in the investigation.
- ***COOP/BCP/DR*** – Role is to provide assistance and subject matter expertise in business continuity and disaster recovery.
- ***Physical Security*** – Role is the subject matter expert and point personnel for physical security.

2.2 CIRT Contact List

The CIRT contact list is in section 5.

2.3 Team Notification

Once an incident has been declared by the CISO or designate, the IRM will notify the Incident Response Team (IMT) and coordinate with the CISO to prioritize and categorize the incident and define the notification tree. In some situations, partial IMT is already convened to triage event(s) into incident.

Contact information for call tree members shall be verified once a quarter. Please refer to COOP and BCP/DR documentation for most recent contact information. See “Contact Information” in section 5.

3 IRP General Process Framework

This section defines the IRP phases, activities, and related procedures to be executed when an information security incident has been declared to have occurred within CUSTOMER operations.

3.1 IRP Phase Descriptions

There are four phases of executing an IRP as defined in the following table.

IRP EXECUTION PHASES	PHASE DESCRIPTION
Preparation Phase	Preparation phase activities focus on developing and implementing the process and procedures, information, and personnel ahead to time into an organized method to deal with most likely scenarios while building the capabilities to handle variations and unknowns. This phase also connects to the broader information security functions since it includes prevention steps. The Preparation Phase includes understanding and acquiring the required skill sets as well as acquiring and deploying all the critical tools needed to ensure appropriate preparedness and should also include continuous testing of the IRP and training of CIRT members on the IRP.
Detection and Analysis Phase	Detection and analysis phase activities focus on the activation of the CIRT to address the immediate situation. This phase places the CIRT in a position to oversee all activities immediately following (or in conjunction with) the activation. It involves assessing the situation and analyzing the impacts to determine best course of action, plan implementation, return to normal operating conditions, or perform further assessment. Analysis and log review are critical steps.
Containment, Eradication, and Recovery Phase	This is the core phase of an incident and involves all steps to correct and reestablish full operations.
Post Incident Phase	Post-Incident efforts are focused on lessons learned to improve the process starting back with the preparation phase.

3.2 Preparation Phase

The objective of the preparation phase is to prepare the CIRT to respond to an incident as quickly and efficiently as possible. Although this IRP is defined to address incidents that fall into any of the aforementioned categories, the general framework of this IRP can be used to address any declared incident. It is important that the CIRT be prepared to address a wide variety of issues and this general framework can be used for such purposes. The following subsections define the key items that are necessary to ensure this state of readiness.

3.2.1 Pre-Established CUSTOMER/Agency Policies and Procedures

The following is a list of policies and procedures that should be reviewed by the CIRT, if they exist, or developed by CUSTOMER level management if they do not exist.

- CUSTOMER's current Information Security Policy
- Policies and procedures governing financial expenditures
- Policies and procedures governing the hiring and termination of employees and contractors
- Policies and procedures governing the deployment of new technologies
- Policies and procedures governing technology change management
- Policies and procedures governing the training of employees
- Policies and procedures governing the institution of the new policies and procedures

3.2.2 IRP Communication Protocol

The IRP Communication Protocol, defined at either the Agency or CUSTOMER Level, provides guidance and direction for initiating and managing communications before, during, and after an incident has been declared. The protocol provides guidance and direction for initiating and conducting communications throughout the lifecycle of the incident and should be developed in alignment with the lifecycle of the incident response process. The protocol should define three levels/phases of communication to occur during the lifecycle of an incident:

- Pre-Incident Declaration Communication
- Incident Response Execution Communication
- Post Incident Response Communications

Generally, the protocol will define the following:

- Primary communication receivers in each phase of the incident lifecycle.
- What information should be provided within communications occurring in each phase on the incident lifecycle.

Preparation for executing communications during the lifecycle of incident response should include:

- Creating separate email accounts to ensure timely and secure communications.
- Defining procedures for setting up Telephone Conference Bridge capabilities.
- Developing document templates such as status report templates, analysis report templates, and resource request templates. Please note that these can be adapted or completely adopted from templates that may currently exist within the workflow of CUSTOMER.

See section 3 for the IRP Communications Protocol Flowchart.

3.2.3 IRP Software Tools

Software tools should be installed to automate the incident response as much as possible. The following lists includes, but is not limited to, examples of some of the tools that should be installed during the preparation phase.

- Virus Scanning Tools
- Monitoring, Reporting, and Alerting Tools
- Forensic Data Collection Toolkits
- Intrusion Detection Tools
- Netflow Data Capturing and Analysis Tools

3.2.4 Critical System Images

During the development and execution of the Eradication Plan (discussed in section 2.5.1.5), it may be necessary to rebuild compromised systems to ensure that the threat/malicious activity has been completely removed. To quickly facilitate this possibility, it is strongly recommended that forensic images of all critical systems be captured and stored away for use during system restoration activities. Recommended tools to use to accomplish this are:

- Acronis True Image
- Acronis Snap Deploy
- Norton Ghost
- EnCase Enterprise

3.2.5 IRP Training

The IRP should be distributed to all CIRT members. All CIRT members are required to read the plan and execute the acknowledgement form at the end to confirm their understanding.

An essential component of IRP preparedness is increasing security awareness among CUSTOMER employees to recognize and report IT security incidents. Training and educational activities for CUSTOMER employees should be divided into four levels:

- **Training and Education for Senior-Level Management**

  This training will target senior-level management. This training will focus on regulatory compliance requirements addressed by the IRP as well as an executive overview of the IRP. The objective of this training should be to create a general understanding the IRP and its relationship to the various CUSTOMER units and the responsibilities of those units during the execution of the IRP. The goal is to illicit prescribed support from senior-level management to ensure full participation throughout the organizational chain during IRP execution.

- **Training and Education for Mid-Level Managers**

  This training will target mid-level managers and will address staffing allocation and requirements for IRP execution as well as the allocation of other critical resources need to support the IRP execution. This training will include a more detailed review of the IRP focused on incident reporting and communications.

- **Training for CUSTOMER IT Staff**

  This training will target each agency's IT staff. This training will focus on IRP major incident activities, incident reporting, and IRP communications. The goal is to prepare all systems, network, and application administrators, engineers, and architects to be able to participate in an incident response at some level.

- **Training for all other CUSTOMER Employees**

  This training will target all remaining CUSTOMER employees with the goal of creating awareness of Acceptable Usage Policies as well the incident reporting structure.

To ensure and confirm preparedness, the CUSTOMER should conduct an annual tabletop test of the IRP. This test would facilitate both the reiteration of the plan steps to the team and provide a chance to review and possibly update incorrect steps or actions in the plan.

3.2.6 CIRT Contact List

Each CUSTOMER agency will develop a CIRT contact list and append it to this IRP. The CIRT contact list must be reviewed and maintained every six months to ensure that the CIRT member listings are accurate and up-to-date. The CIRT Contact List should maintain the following contact information for each CIRT member:

- CIRT Member Name, CUSTOMER Job Title, CIRT Role
- CIRT Member Primary Phone Number, Cell Phone Number, Home Phone Number (if Necessary)
- CIRT Member Office Address
- CIRT Member Primary and Secondary Email Address
- CIRT Member Backup Team Member (all information required above should also be listed for the backup)

3.2.7 IRP Testing

This IRP should be tested on an annual basis. It is the responsibility of the CISO to conduct this testing to ensure the consistent viability of this IRP.

3.3 Detection and Analysis Phase

The detection and analysis phase defines the specific tasks to be performed by the CIRT when alerted that an event has occurred in the CUSTOMER environment. These tasks are designed to guide the CIRT through the stages of the IRP execution process starting with the initial assessment of the event to determine if it is an actual incident requiring full incident declaration and activation of the CIRT to execute the IRP.

The need and sequence of execution of each task is dependent upon the actual event circumstances.

The detection and analysis phase consists of three major tasks:

- Incident Triage
- Indicators of Compromise Review
- Evidence Collection, Preservation, and Handling

3.3.1 IRP Response Process Initiation

The IRP can only be triggered by the Chief Information Security Officer (CISO). The response times are specified in the "Operational Level Agreements" section. Team members will be notified of incidents or security events that could potentially be escalated to incidents via:

- Appropriate help desk (HD)
- Email to pre-determined address
- Phone call to ISO Incident Response (IR) core team

When notifying the IR lead, the minimum that will be required is:

- Initiator's contact information
- Description of potential incident
- Affected systems observed
- Date and time of event

Additional information will be required based on the type of incident. This includes but is not limited to:

- System information including system logs, running processes, and memory allocation
- If authorized, physical or remote access to affected systems
- Details on applications or services running on the affected systems
- Time to assist with any follow-up questions or response activities if necessary

Based on categorization and prioritization, the Incident Response team will follow checklists and workflows which are meant to be used as guidelines. Those sections and documents are listed below and in the appendix.

3.3.2 External Process Interactions

The ISO Incident Response process will interface and collaborate with other Agencies and teams to identify, contain, eradicate, and recover from an incident. While the CUSTOMER priority is to return operations as quickly as possible, information should be collected to be used in troubleshooting and analysis. The following list is not inclusive and references other processes used by CIRT members and other teams assisting in investigation or return to service.

- Vulnerability management process
- Firewall change process
- Operations: Antivirus process remediation
- Operations: Patch management process
- External forensic analyst processes
- External law enforcement
- Physical security

3.3.3 Incident Triage

All events must be triaged to determine if the event falls within the definition of an information security incident as defined by Section 1.7 IRP Terminology Definitions, Item 4. The goal of the Incident Triage activity is to gain as much pre-response intelligence about the event to determine the following:

1. If the event is an incident as defined by Item 1.7 (4) or an operational issue that should be addressed by and solely within functional boundaries of the CUSTOMER IT support Team.
2. The extent of the event's impact on the CUSTOMER's business operations and technology infrastructure.
3. The most immediate course of action for responding to the event once it's declared an incident.

The following steps must be performed when conducting an Incident Triage.

STEP 1. Collect a full account of all initial reports and indicators related to the event. This will help to define the scope and scale of the event.

I. Collect help desk trouble tickets filed within the same time period as the suspected event occurrence and addressing subjects similar to the event.

II. Conduct a search on trouble ticket files within that time frame.

III. Conduct a topical search for trouble tickets that are the same as the event.

IV. Conduct interviews of users directly affected by the event to assess the event's impact.

V. Review any available SEIM-based monitoring output/alerts to provide additional insight into

the depth and breadth of the event.

STEP 2. Conduct initial assessment of the event's impact on CUSTOMER business and technology operations. Identify areas of the technology infrastructure that are experiencing functional issues.

I. Conduct a full scale accounting of technology components whose current operational state appears to be different from its normal and expected operational state.

II. Identify all information assets that are potentially at risk.

III. Corroborate user impact accounts with accounting of technology operational issues to obtain as complete intelligence as possible about the event.

STEP 3. Assess the threat or impact to key or critical business processes, information, or technological resources by answering the following questions.

I. What business functions have been impacted by the event?

II. What business functions are potentially threatened by the event?

III. What technology components are impacted by the event?

IV. Are those business functions or technological components subject to any internal or external operational policies or regulations? If so, identify those policies or regulations and determine reporting requirements.

V. Is this event isolated to a particular business function or specific technology component?

VI. Was the incident initiated by internal of external activities?

The resulting information collected from this task should be used to decide if the event can be declared an incident or if the event should be handled through normal CUSTOMER IT operations for the effected units. Any information artifacts collected about the event should be stored on the CIRT's central data storage repository allocated for this IRP.

The CISO will make the declaration of an incident, if necessary. Incident prioritization will be addressed during the incident triage phase to determine if the event is an operational issue or an actual incident. All declared incidents should be handled with the highest priority regardless of the categorization or business impact. All incidents should be handled according to the predefined response plan outlined in this IRP.

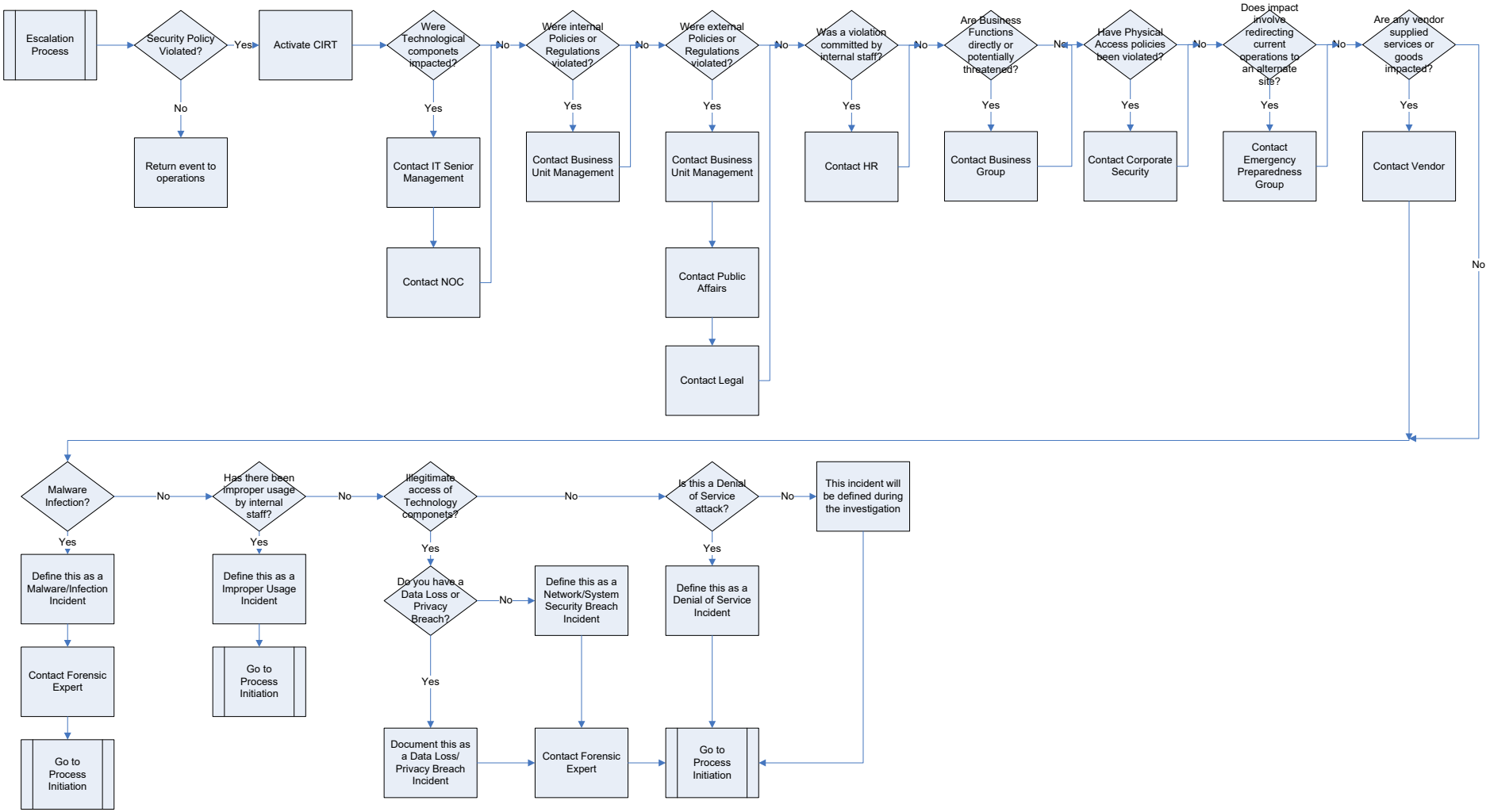
3.3.4 Escalation Decision Tree

If the event is declared an incident, then the next step is to consult the Escalation Decision Tree (EDT) to determine to what extent the CIRT should be activated. The consultation of the EDT is a continuous process throughout the lifecycle of the IRP execution meant to guide the activation of components of the CIRT. The activation of any CIRT components is based on the existence and review/confirmation of characteristics of the event that are aligned with EDT triggers. Overall, the following questions should be answered.

- Is this an incident or an event?
- If the event is declared an incident, then what incident category should be assigned to the incident?
- What EDT Triggers exist in the intelligence gathered from the triage phase?
- What components of the CIRT need to be activated?

Using the artifacts gathered during the triage process, consult the EDT and determine if any of the results from the incident triage process contain any trigger points that match up with the trigger/decision points in the EDT. Those trigger/decision points will identify the initial components of the CIRT team that need to be activated to participate in the IRP. As the investigation proceeds this list may grow or shrink depending on additional evidence gathered.

Escalation Decision Tree



3.3.5 Indicators of Compromise Review

An Indicator of Compromise (IOC) is a digital/physical artifact or remnant of an intrusion that can be identified on a host or network. IOCs can either be measurable events or stateful properties.

Examples of measurable events are:

- A registry key is created
- A file is deleted
- An HTTP Get Request is received
- An IDS rule is fired

Examples of stateful properties are:

- MD5 hash of a file
- Value of a registry key
- Existence of a mutex

Two categories of IOCs should be searched for during the review.

- **Direct IOCs**

  Direct IOCs are artifacts that directly reflect some completed or attempted interaction with the network, OS, application, or data components that are directly associated with the incident under investigation. The following are some of the areas of a compromised device that should be reviewed to identify Direct IOCs:

  I. Related Log Files
  II. Volatile Memory
  III. Windows Registry
  IV. Startup Folders
  V. Volatile TCP Connectivity Records
  VI. File System

- **Indirect IOCs**

  Indirect IOCs are artifacts that indirectly reflect or indicate that there may be other more direct artifacts on the compromised system. Indirect IOCs are considered circumstantial and may require further analysis to identify more Direct IOCs. The following are some the areas of the compromised device that should be reviewed to identify Indirect IOCs:

  I. Related Log Files

II. Volatile Memory

III. Netflow Data Artifacts

All IOCs should be collected using forensically sound methods and tools to preserve their integrity for future use in the investigation. Your forensic expert will identify these methods and tools to be used to assist in the investigation of the incident.

3.3.6 Evidence Collection, Preservation, and Handling

At all times during the IRP, it is important to properly record and preserve all information collected including, but not limited to, digital artifacts (e.g., data, files, logs), forensic system images, paper records, and video material. These materials may be used in criminal hearings, so it needs to be gathered and stored in a forensically sound manner to maintain its integrity throughout the investigation.

When collecting evidence, ensure that the following procedures are adhered to, to guarantee the integrity of the evidence during the investigation:

- For systems suspected of being compromised, make complete forensic images of those systems using generally accepted image creation tools. Duplicate copies of these forensic images should be made with the original forensic images stored away in a secure manner. The duplicates of these forensics images will be used during the analysis phase of the investigation.
- For any digital artifacts such as files, logs, or data of any kind, generate hash values of these digital artifacts and store away these hash values along with their respective data in a secure manner. Make duplicate copies of the digital artifacts and hash values to be used during the analysis phase of the investigation.
- For any photographic images or videos, generate hash values and store away these hash values along with their respective photographic images and videos in a secure manner. Make duplicate copies to be used during the analysis phase of the investigation.
- For paper records, time stamp all paper records received and make duplicate copies of these records to be used during the analysis phase of the investigation. Store the original records away in a secure manner.

PLEASE NOTE: for hashing any digital information it is generally accepted to use either SHA1 or MD5 algorithms to generate hash values.

GUIDELINES FOR COLLECTING DATA

When collecting any kind of data from systems that are suspected to be associated with the incident under investigation, application of the following guidelines ensure that all data is collected in a forensically sound manner and preserved that way.

- **Guidelines for Collecting Volatile Data**

  I. Use safe and tested tools you know work and have some general legal precedence.

  II. Collect volatile data from potentially compromised systems before disconnecting those systems from the network or power.

  III. Create two or three CDs containing volatile collection tools and write-protect them.

  IV. Generate a checksum and validation for each of your tools and store it safely within your toolkit.

  V. Volatile data should be stored either on "Read-Only" CDs or on offline storage drives that require two-factor authentication to access the data and access should be limited to the least number of CIRT members requiring access.

- **Questions to ask regarding evidence collection and analysis**

  I. Was the evidence gathered and verified in a forensically sound manner?

  II. Was the chain of custody maintained?

  III. Is the ownership and licensing appropriate for the forensic tool used?

  IV. Was the proper examination environment maintained and controlled by those members of CIRT who were conducting the investigation?

  V. Can the results of the technical analysis be duplicated using other tools?

  VI. Does the analyst understand what the tools they use are actually doing, or are they merely taking for granted what an automated process is reporting?

  VII. Do other professionals use the same techniques and methodology?

  VIII. Is the analyst technically capable of defending/supporting their interpretation of the evidence?

When collecting and handling evidence of any kind during an investigation, establishing and maintaining chain of custody is an essential part of maintaining the integrity of the evidence collected during an investigation. Chain of custody primarily identifies all individuals that handled the evidence in any way during the investigation staring from the initial collection of the evidence. If its integrity is ever questioned, this chain of custody record can be used to determine at what point during the existence of the evidence its integrity could have been impacted.

When establishing and maintaining chain of custody, the following questions should be asked:

- **Questions to ask when considering chain of custody**

  I. Who collected the evidence?

  II. How and where was the evidence taken?

  III. Who took possession of it? At what date and time did they do so?

IV. How was the evidence stored and protected?

V. Who took it out of storage, and for what purpose?

When handling evidence, ensure that a minimum number of CIRT members involved in the IRP have access to the evidence. A log of access to secure locations should be kept. The log should be kept secure and managed by the CIRT Senior-Level Managers.

3.3.7 Initial Intelligence Report

An initial analysis report will be crafted and sent to all members of the CIRT team and any auxiliary members who might be involved in the responding to the incident. In scenarios where time is critical, email or conference calls will be used to disseminate information to get resources on board and continue to the "Containment, Eradication, and Recovery" phase.

3.4 Containment, Eradication, and Recovery Phase

This section describes the tasks that are performed for the containment, eradication, and recovery of a declared incident. Each incident will require specific activities within each task to bring it to a resolution. The CIRT will define, apply, and document all these unique activities.

3.4.1 Containment

The goal of the containment activity is to eliminate any additional damage caused by the incident. The objective of containment is to isolate the offending system or activity without changing any software settings. This will allow forensic copies of the items to be made that can be used for further investigation.

Perform containment activities as soon as appropriate during the response process. Containment tasks may be executed while the Analysis phase is still in progress. Please be mindful that business units/Agencies that use the system(s) should be involved in any discussions and decisions involving containment activities. The CIRT will develop a containment plan based on incident intelligence gathered during the Triage phase with direct input and feedback from the affected business unit/Agency needed to review the business impact of containment for the impacted systems. The impact of containment activities needs to be discussed and evaluated before the containment tasks are executed. This review will determine short-term or long-term containment.

3.4.1.1 Short Term Containment

Short term containment will temporarily remove a system from production use. Compromised systems/processes should be isolated with minimal changes made to any data, software, or system configurations. Steps that can be taken to isolate compromised systems/processes include:

I. Pulling the power cord. (Assess the impact of disconnecting power from a system before you do so. Consider the impact of the loss of volatile data or database corruption.)

II. Isolating a network segment of infected workstations.

III. Disconnect network connections from infected server and/or reroute its traffic to an alternate device.

IV. Shutting down any wireless access for entire subnets.

V. Complete network shutdown of compromised network devices and deployment of new network devices that have a heightened level of security countermeasures enabled including active monitoring.

VI. Complete wireless network shutdown of compromised wireless network devices and deployment of new wireless network devices that have a heightened level of security countermeasures enabled including active monitoring.

Once this has been performed, a forensic copy of the system should be created and stored with the incident artifacts.

3.4.1.2 Long Term Containment

The objective of Long Term Containment is to contain the threat while allowing the impacted systems to be used for business purposes. In this scenario, the impacted system is too critical to take offline so the threat will need to be contained while the system remains online and functional. Before performing these steps, you will need to make a forensic copy of the impacted system(s). Some actions that can be taken are:

I. Removing accounts or backdoors left by the attacker

II. Collect volatile data from memory

III. Run Vulnerability/Malware Scanners against the compromised system constantly

IV. Change passwords for all system accounts

V. Capture and examine net flow data to and from the compromised systems

VI. Installing security patches on impacted and neighboring systems

VII. Disabling one or more applications from a system

VIII. Network filtering of specific protocols or ports

IX. Redirect network traffic to systems set up as honey pots to continue monitoring potentially malicious activities

3.4.1.3 Making and Storing Forensic Copies

Making forensic copies of data will help to preserve the state of the data for use in the investigation. Use generally accepted/approved disc duplicators and image creators for this as well as qualified forensic examiners. The following list of tools are generally accepted.

I. EnCase

II. FTK

III. X-Ways Forensics

IV. DD

Use duplicate copies of any data images you make in the investigative process. Store the original images securely away according to pre-established evidence storage and chain of custody procedures.

3.4.1.4 Incident Analysis Guidelines

When conducting the analysis, it should be done in an area that is completely under the control of the CIRT member conducting the analysis. All systems that are used to conduct the analysis should be used only for the analysis purposes. Maintain logs of entry in and out the area as well as system access logs. Conduct the analysis using duplicates of forensic images to assist you in the Eradication Phase. Some additional information you can try to identify might be:

I. Identify possible attack source(s)

II. Identify port and protocol of any network traffic

III. Validate system status (OS version, application versions, patching status, security software status)

IV. Identify vulnerabilities

3.4.1.5 Incident Eradication

The objective of Eradication is to remove the threat from the impacted system and harden it against future incidents.

Proper steps should be taken to remove malicious and other content from affected systems. Once these steps are complete, you will need to ensure that the system is clean. Please be mindful that business units/Agencies that use the system(s) should be involved in any discussions and decisions involving eradication activities as these activities may affect system availability and/or performance. The CIRT will develop an eradication plan based on incident intelligence gathered during the Triage and Analysis activities with direct input and feedback from the affected business unit/Agency. The impact of eradication activities needs to be discussed and evaluated before the eradication tasks are executed.

I. Depending on threat prevalence and eradication confidence levels, the compromised systems may need to be completely rebuilt to ensure that the threat/malicious activity has been totally eradicated. Use the images created during the execution of the recommendations from section 2.3.4 Critical System Images.

II. The CIRT and/or third party computer forensic professional will review logs from network or boundary protection devices. Review the logs from SIEM, console, or copies to reduce the risk of compromise of the investigative process. The chain of custody must be preserved at all times.

III. The CIRT will maintain any original evidence or the best possible source of evidence. A team member will be designated as evidence custodian. This individual will assure the authenticity of evidence obtained during an investigation through the chain of custody process so that findings based on this evidence may ultimately be admissible in legal proceedings. At the conclusion, evidence collected will be turned over to the appropriate department(s). The respective department will be responsible for maintaining custody of the evidence for the period proscribed by law.

IV. The CIRT will use vulnerability analysis tools to perform exhaustive scans. Caution should be used as scans may alert an active hacker.

V. The CIRT will check other systems with similar operating systems and/or vulnerability levels for possible compromise.

VI. Remove all malicious artifacts

VII. Review incident analysis

VIII. Perform vulnerability analysis

IX. Improve security controls

The CIRT will harden the system to prevent future incidents by reviewing all artifacts gathered about the incident and document configuration changes that will prevent this incident from occurring in the future. To prevent future incidents, these changes should be integrated into CUSTOMER's policies, procedures, and/or standards.

Once these activities have been completed, the system is ready to be returned to production use.

3.4.2 Incident Recovery

The objective of this step is to carefully reinstall the clean or treated system back into production. While doing this, it is important to prevent another incident from occurring. The system will need to be tested, monitored, and validated to properly complete this activity. Monitoring activities of all recovered systems will be increased, accelerated, and escalated to identify any further malicious threats/activities.

The CIRT will be in charge of creating the recovery, monitoring, and system reintroduction plans. The following are recommended for implementing recovery plans.

STEP 1. The system owners will determine the best time to put the system back in production

STEP 2. The CIRT will determine what tests need to be run

STEP 3. The CIRT will determine how long the tests will be run

STEP 4. The CIRT will define what criteria needs to be met to validate the system

The plan will be executed and if the tests reveal that the system is infected or compromised, the process will need to return to the Eradication Phase.

Once the system has been successfully placed back in production, then all of the activities of this step will need to be documented and stored with the incident artifacts.

3.5 IRP Incident Categorization

The objective of Incident Categorization is to subject the declared incident to a pre-defined set of response guidelines after the incident has been categorized. The purpose is to provide a streamlined and flexible set of guidelines and directions that can be applied to the incident response plan. The following three major incident categories have been defined for this IRP:

- **Malware Infection**
- **Network/System Security Breach**
- **Data Loss/Privacy Breach**

While this categorization system has been defined to aid the response process, elements of an incident may cross categorization boundaries which may require application of guidance from other categories. Please see the following appendices for specific guidelines and directions for each incident category.

- **Appendix A. Malware Infection IRP**
- **Appendix B. Network/System Security Breach IRP**
- **Appendix C. Data Loss/Privacy Breach IRP**

The incident categories are briefly described in the following subsection. Specific incident categorization guidelines and directions are provided in the appendices list above.

3.5.1 Malware Infection Incident Category Description

A malware infection is an incident where malicious software, designed to spread without the user's knowledge, is installed onto a computer. Malicious software or malware can include viruses, worms, and Trojan horses.

3.5.2 Network/System Security Breaches Incident Category Description

A network/system security breach is any incident that results in unauthorized access of data, applications, services, networks, and/or devices by bypassing their underlying security mechanisms. A security breach occurs when an individual or an application illegitimately enters a private, confidential, or unauthorized logical IT perimeter. This category can include a Denial of Service (DOS) attack.

3.5.2.1 Denial of Service (DOS)

A Denial of Service is a sub-category of the network/system security breach and is an attack that successfully prevents or impairs the normal authorized functionality of networks, systems, or applications by exhausting

resources. This activity includes being the victim of or participating in the DOS. An operational anomaly that is caused by this type of security incident may include:

- An unusual or sudden spike in firewall utilization
- Any internet web server service crashing or restarting
- An identified Distributed Denial of Service (DDoS) attack against CUSTOMER's internet presence
- An unexpected or unusual event for which the cause is not immediately apparent and which has some potential computer security implication

3.5.3 Data Loss/Privacy Breaches Incident Category Description

Data loss/privacy breach is an incident involving the unauthorized access, removal, or duplication of personable identifiable information or other protected privacy or privileged information. This category can also include improper usage and loss of confidential data incidents.

3.5.3.1 Improper Usage

Improper usage is a sub-category of data loss/privacy breach and is defined as any violation of an Agency's acceptable use policy or any other Agency's IT policy. Incidents related to this category include the following:

- Investigation of inappropriate or improper technology usage
- Analysis and investigation of downloading/retaining pornography on hard drives
- Analysis of systems in response to a harassment complaint
- Investigation of employee usage of unauthorized software

3.5.3.2 Loss of Confidential Information

This category includes any suspected breach of any confidential information (PHI, PII, CJIS, or confidential information). An incident response team will be formed parallel to the incident being confirmed. Incidents related to the violation of employee privacy or the possible breach of confidentiality of data may include:

- A laptop with confidential business information is stolen
- Unexplained public disclosure or known unauthorized disclosure of CUSTOMER data or confidential information
- A hostile termination occurs of an employee or contractor with significant access to or knowledge of CUSTOMER's systems or networks

4 IRP Communications Protocol

Additional guidelines for implementing and managing an IRP communications protocol are as follows:

- All communications should be on a need to know basis.
- All communications should be secured. All emails should be encrypted. All emails should include trailing text explaining the sensitive nature of the data and penalties for forwarding or duplicating it without explicit permission.
- The participating team members should be instructed not to forward or share emails with non-participating personnel unless they have explicit permission from the Incident Response Coordinator.
- A standard form and distribution list should be used for status reporting. Multiple status reports will be sent out to different audiences during the incident investigation. Some of these are:
    1. A status report detailing the incident investigation will be sent to the members of the CIRT.
    2. A status report may be sent to the user community (as approved by the CISO and/or CUSTOMER Senior Management).
    3. A status report may be sent to external interested parties.

Following these guidelines will help facilitate a more efficient and secure response process. Please see Appendix D Sample Report Templates.

5 IRP Resource List

Resources to be used during the execution of the IRP are listed below.

- **Conference Bridge Information**

  Instructions on how to set up a conference bridge:

  (Add conference bridge instructions here)

- **IRP Data Repository Information**

  Instructions on where and how to access the data repository:

  (Add data repository instructions here)

- **IRP Status Report Templates**

  Status Reports templates that will be used for reporting information during the Incident Response:

  (Add template repository instructions here)

6 Incident Remediation Declaration

The CUSTOMER CISO will declare the incident completely remediated and resolved and at such time, all incident response activities will cease and the CIRT will be deactivated.

7 Post Incident Review

All IRP activities will be reviewed during this phase. The objective is to learn from the experience and improve the IRP execution process. This is an objective session meant to allow CIRT members to freely give unrestricted and unopposed input and feedback. All CIRT members are required to provide feedback about their activities and in some cases, a 360 degree review may be necessary to ensure that a full and thorough review is conducted. This "lessons learned" session should be conducted no more than one week from the time that the incident is declared remediated.

The objectives of the lessons learned session are to:

- Review the timeline of all IRP activities.
- Review the incident reporting/alerting communication and related activities.
- Review the incident details, description, and impact.
- Review IRP activities including steps taken to contain and eradicate the incident.
- Review what actions were performed and by whom.
- Identify and review successful IRP activities.
- Identify and review IRP activities that need improvement. Develop an IRP activities improvement plan and timeline/deadline for implementation.
- Verify that all necessary documentation has been created. If not, assign the creation of the documentation.
- Explore and identify changes that need to be made to existing documentation or standards. Potential changes may include updates to the security policy; software and hardware standards; patch or malware detections; and software deployment schedules.

A final IRP report should be created from input and feedback from this "lessons learned" session. All documentation produced from this meeting will be archived with the incident artifacts.

8 Documentation Management

The Information Security Office will maintain custody of published reports in the secured database. They will be organized and named by incident type and specific incident number associated with each case. The following is a list of resources available for managing incident documentation.

- Reporting templates (see section 5 for details)
- Incident tracking in database
- Incident status in database

Reports and metrics will be available to the Information Security Office, CIRT, and the Executive Management involved.

APPENDIX A. MALWARE INFECTION IRP

This Malware Infection Incident Response Plan (Malware IRP) is developed to provide guidance and direction for responding to a malware infection. This Malware IRP will provide the following benefits:

- A structured yet flexible mechanism for triaging, containing, remediating, and recovering from malware infection incidents in the most appropriate and efficient manner.
- A structured mechanism for mitigating the adverse impacts of malware infection incidents to the CUSTOMER and its business operations can be minimized by appropriate safeguards as part of the incident response, in conjunction with a business continuity plan.
- A structured mechanism for ensuring and conducting the lessons learned phase of Malware IRP activities to minimize the probability of similar events occurring in the future. The secondary benefit here is to improve the implementation and use of information security safeguards and improve the overall Information Security Incident Response framework.

A.1. Malware IRP Preparation Phase

The objective of this phase is to prepare the CIRT to quickly address and remediate malware infection incidents. The following are recommendations that can be implemented to simplify and streamline the CIRT's response.

- Install a Security Information and Event Management (SEIM) solution such as McAfee enterprise with ePolicy Orchestrator.
- Install SEIM software agents on all critical systems, at a minimum. The agents can be managed by your SEIM software.
- Organize managed systems into groups. This will allow you to deploy solutions based on group needs and identify related systems in case your malware infestation is spreading.
- Create policies for the managed groups. Policies will define and direct automated responses to reported issues.
- Generate and review reports from your SEIM software.
- Create a secure storage area that can be used to store malware, artifacts, instance, variants, and other evidence collected during the incident investigation.

A.1.1 Software Tools

As recommended in the IRP General Framework, and in support of the response effort, software tools should be installed to help automate the incident response. The following lists includes, but is not limited to, some of the tools that should be installed during the preparation phase.

- Virus Scanning Tools

- Monitoring, Reporting, and Alerting Tools
- Forensic Data Acquisition and Volatile Data Collection Toolkits
- Intrusion Detection Tools
- Netflow Data Capturing and Analysis Tools

A.1.2 Critical System Images

Depending on the severity of the malware infection, it may be necessary to rebuild compromised systems to ensure that the malware has been completely removed. To quickly facilitate this possibility, it is strongly recommended that forensic images of all critical systems be captured and stored away for use during system restoration activities. Recommended tools to use to accomplish this are:

- Acronis True Image
- Acronis Snap Deploy
- Norton Ghost
- EnCase Enterprise

A.1.3 Application Whitelisting

Application Whitelisting can be a preventative countermeasure to stop the replication of malware by blocking its ability to be executed on any system that employed whitelisting controls.

The goal of whitelisting it to prevent unauthorized software and/or malicious code from running on any desktop or server in the technology infrastructure. This strategy will enable the CIRT to quickly respond to and mitigate the negative impact of malware infections by implementing an application whitelisting capability. The implementation of Application Whitelisting in the technology infrastructure will greatly diminish vulnerability to malicious executables running in its environment because of the restriction imposed on unapproved applications running on it desktops and servers. Application Whitelisting is used to grant trusted software specific authorization to run on a desktop or server. The goal of whitelisting it to prevent unauthorized software and/or malicious code from running on any desktop or server in the CUSTOMER technology infrastructure. The following is a high-level list of action items that provide a framework for phasing in Application Whitelisting into CUSTOMER's environment:

Conduct Software Inventory

A detailed software inventory of every desktop and server in CUSTOMER's domain is the first step in implementing application whitelisiting. This inventory has several benefits. First, it positions the agency to be able to identify and uninstall any applications that have been decommissioned for use. Second, It allows CUSTOMER to identify the software applications that support its workflow supporting any future effort to streamline the workflow.

Define Workflow Priority

Defining workflow priority will inherently and directly determine the software application's accessibility needs across the agency domain and support information compartmentalization enabling a higher level of information protections. Defining workflow priority also supports defining application whitelisting priority meaning the identifying sub-areas in the agency domain where whitelisting can be piloted before the implementation is expanded throughout the domain.

A.2. Malware Infection Triage

There are a number of events and informational sources that can provide indicators that a malware infection has occurred. The following list identifies some of those events and sources to be checked when attempting to confirm a malware infection. These instructions are meant to be followed by the CIRT. During this phase, you will detect the event, gather evidence, and determine if it is an incident.

- Intrusion Prevention/Detection Systems (IPS/IDS)
- Unusual and unexplained system performance activities
- Incident reporting through the service desk
- Audit or monitoring tools detecting unauthorized activities
- Security Information Event Management

IRPORTANT NOTE: Create a temporary repository for storage of all IRP artifacts. See section 4 IRP Resource List for instructions on establishing this repository. Additionally, ensure that the CIRT is following the evidence/artifacts collection procedures as outlined in Section 2.4.6 Evidence Collection, Preservation, and Handling.

Conduct the following steps to triage the malware infection incident:

STEP 1. Collect a full account of all initial reports and indicators related to the malware infection. This will help to define the scope and scale of the malware infection.

I. Collect Help Desk Trouble Tickets filed within the same time period as the suspected incident occurrence and addressing subjects similar to the incident.

II. Conduct a search on trouble ticket files within that time frame.

III. Conduct a topical search for trouble tickets that are the same as the incident.

IV. Conduct an interview of users directly affected by incident to assess the incident's impact.

V. Review any available SEIM-based monitoring output/alerts to provide additional insight into the depth and breadth of the incident.

STEP 2. Conduct an initial assessment of the malware infection's impact to CUSTOMER/Agency business and technology operations. Identify areas of the technology infrastructure that are experiencing functional issues.

I. Conduct a full scale accounting of technology components whose current operational state appear to be different from its normal and expected operational state.

II. Identify all information assets that are potentially at risk.

III. Corroborate user impact accounts with accounting of technology operational issues to obtain as complete intelligence as possible about the incident.

STEP 3. Assess the threat or impact of the malware infection to key or critical business processes, information, or technological resources by answering the following questions.

I. What business functions have been impacted by the incident?

II. What business functions are potentially threatened by the incident?

III. What technology components are impacted by the incident?

IV. Are those business functions or technological components subject to any internal or external operational policies or regulations? If so, identify those policies or regulations and determine reporting requirements.

V. Is this incident isolated to a particular business function or specific technology component?

VI. Was the incident initiated by internal or external activities?

A.3. CIRT Escalation Decision Tree

Follow the Escalation Decision Tree (EDT) to determine the specific components of the CIRT that need to be activated. Information gathered for the triage activity will contain triggers that will determine the CIRT components to be activated and the tasks to be conducted by those activated CIRT components.

IRPORTANT NOTE: When contacting any members of the CIRT, use only approved communication methods when communicating about this incident as outlined in Section 4 IRP Resource List and Section 5 IRP Communications Protocol.

- **Decision Point 1: Has this event violated our Security Policy?**

  Has a Security Policy been violated by the malware infection you are investigating? If you don't know, you should contact your management to identify the proper person or group to ask the question.

  If a violation has occurred, you will need to activate the CIRT. If not, contact IT support and reassign the event to IT support.

- **Decision Point 2: Were technological components impacted?**

  If yes, contact IT Senior Management and the NCC.

- **Decision Point 3: Were internal policies or regulations violated?**

  If yes, contact Agency Senior Management.

- **Decision Point 3: Were external policies or regulations violated?**

  If yes, contact Legal, Public Affairs, and Agency Senior Management.

- **Decision Point 4: Was a violation committed by internal staff?**

  If yes, contact HR.

- **Decision Point 5: Are business functions directly or potentially threatened?**

  If yes, contact the Business Unit/Agency Owner(s).

- **Decision Point 6: Have physical access policies been violated?**

  If yes, contact Corporate Security.

- **Decision Point 7: Does impact involve redirecting current operations to an alternate site?**

  If yes, contact the Emergency Preparedness Group.

- **Decision Point 8: Are any vendor-supplied services, information system, or goods impacted?**

  If yes, contact the vendor that is impacted.

A.4. Indicators of Compromise review

The forensic CIRT members should be activated to conduct an Indicator of Compromise Review. Please adhere to the guidelines stipulated in Section 3.3.6 Evidence Collection, Preservation, and Handling. Once the review is complete, you will call together the CIRT to review the evidence. They will use this to lay out a plan of action for the next phases.

A.5. Containment, Eradication, and Recovery Phases

The purpose of these separate phases is to reduce the ability for the issue to spread, remove the issue, and return the impacted systems to production. The business unit(s)/agencies affected should be involved in any discussions and decisions involving containment activities. The CIRT will develop a containment plan based on incident intelligence gathered during the triage phase with direct input and feedback from the affected business unit/Agency needed to review the business impact of containment for the impacted systems. The impact of containment activities needs to be discussed and evaluated before the containment tasks are executed. This review will determine short-term or long-term containment.

A.5.1 Malware Containment

The following is a list of recommended steps to implement during the containment phase of this Malware IRP:

Firewall Configuration

a) Inbound and outbound access to and from the network should be restricted, specifically blocking access to the URLs listed in the Analysis Results section of this document. Generally, inbound and outbound access should be restricted to only those services (open ports) and IP addresses necessary to conduct operations.

b) Systems connected to the network environment should be limited to a reasonably trusted location or location required to operate. Whitelisting is strongly recommended.

c) While segmentation is in place, network masking should be reviewed; the malware was able to migrate from segment to segment.

d) All firewalls should be audited for accessible ports and services.

e) Two firewalls were identified to be using the same username and password; each should contain their own set of user credentials.

Restricted Software in Use

a) If possible, systems should be audited for the use of unauthorized application which could potentially weaken system or network security (e.g., P2P or file sharing applications or other applications that are not necessary for normal operations).

b) Group policies should be in place to prevent users from installing software. Application whitelisting is strongly recommended. Even if malware did enter the environment, it would not likely be able to execute.

Passwords

a) All systems should follow password complexity requirements (at least one number, one upper and one lower case character, one special character, and being at least eight characters in length). This is to include all personal computers, servers, firewalls, routers, and other network devices.

b) The passwords on critical systems should be changed immediately and rotated at least every 90 days.

c) All passwords either stored or in transit must be rendered unreadable using encryption.

d) Each user should have their own unique account so that activities on a system can be tracked. Generic account names should not be in use (e.g., “officer”, “Backup”, “Administrator”, “guest”).

e) Passwords at a location must be changed if an employee who knows the password leaves the organization.

System Configuration

a) Ensure that system-hardening guidelines are in place to address known vulnerabilities and security threats. System configuration should be based on industry-standard best practices.

b) For Windows environments, ensure Windows is configured to clear the pagefile.sys upon reboot to prevent access to potential residually stored information.

c) For Windows environments, ensure Windows is configured to have Restore Points disabled.

d) On servers, systems containing sensitive data, firewalls, and routers, change logs should be implemented. Periodically audit these logs to ensure they are being properly updated and that any significant changes do not create any additional security liabilities.

e) If possible, ensure an application to the equivalent of Tripwire is installed on key systems.

f) If directories are shared, limit read/write privileges to only necessary users.

g) Disable auto run on all drives; this is commonly used in propagating malware.

h) Minimize the number of system images used to build workstations. This will facilitate quicker system baselining and re-imaging if necessary.

Remote Access

a) All remote access into the data environment must use two-factor authentication. Two-factor authentication is normally defined as an authentication method requiring something a user knows (password) and something the user has (token, certificate).

b) Third party remote access must be an on-demand solution. It must be turned off by default and only enabled when needed.

c) Auditing and logging must be enabled for remote access into the data environment.

d) Limit remote access to specific IP addresses when possible.

Logging and Monitoring

a) Windows Event logs should be configured to capture system events such as Security, Application, and System Events on all systems.

b) Ensure that the logs are retained for at least 90 days online (readily accessible) and one year offline.

c) On firewalls, all traffic going in and out of the network should be set for logging. Both accept and deny should be logged.

d) Netflow data should be captured and stored if possible.

e) The logs from all devices must be reviewed on a daily basis. Procedures should be in place for escalations of critical alerts. Most third party vendors can provide automation of this effort.

f) The use of an intrusion detection system (IDS/IPS) should be in place.

g) File-integrity monitoring (FIM) software should be in place.

h) An email proxy similar to an application like “IronPort” should be in place and properly functioning.

Patch Management

a) The Operating Systems should be patched within 30 days of vendor-released security patches/hotfixes.

External and Internal Scanning

a) Regularly conduct external and internal scanning to proactively find and remediate vulnerabilities.

b) Conduct annual external and internal penetration testing at least once a year and after any significant infrastructure or application upgrade.

c) Scanning for rogue Wi-Fi devices should be done quarterly.

A.5.2 Malware Eradication

It is strongly recommended that eradication start with initiating recurring scanning on all infected systems first. Recurring scanning should then be initiated on systems that have not demonstrated critical systems and is strongly recommended. The interval for scanning should be determined based on the critical nature of the system(s) being scanned and the rate of malware infection/re-infection. A prevalence analysis should be conducted to determine how integrated the malware has become. If prevalence is high or unable to be completely determined, it is recommended that eradication should include system restoration using system images taken during the preparation phase of the IRP.

Any and all acquired malware samples are to be immediately submitted to the virus detection vendor for signature development and DAT file updating.

Please follow the below recommendations to ensure eradication is completely successful.

Malware Removal

e) When a significant outbreak occurs, anti-virus should be configured to perform scans non-stop. For example, on average, if a scan takes 45 minutes, set the software to scan every hour. This mode of operation should be performed until there is sufficient assurance that the malware has been eradicated. This mode of operation may take a week or a month depending on the types of malware present and the method of propagation. When a new strain or type of malware is identified or manually found, submit the malware to McAfee to update the signature file and update the signature file in use. Until new malware (signature) is identified, the only true course of action is to continually scan systems.

a) If malware is, or was, suspected on a system, it is recommended the systems be rebuilt to fully confirm the removal of the threat or other additional dormant malware that may have been installed.

b) Ensure antivirus software is current on all systems and that it is set to update virus definitions. Also, ensure the virus definition license is valid and properly accessing new definitions.

c) It is strongly recommended that two types of software is used to detect malware, an anti-virus and antimalware (e.g. Microsoft Essentials and Malware Bytes).

d) Ensure that central logging is properly functioning and alerts are being properly assessed and escalated if needed.

A.5.3 System Recovery

System recovery plans should be developed and coordinated with Business Unit/Agency Management to determine business function resumption priorities.

After system recovery is complete, plan to monitor those systems for some pre-determined period of time to ensure malware re-infection does not occur. Consider:

- When the system can be put back into production.

- How restored systems will be monitored.
- How long restored systems will be monitored.
- A communication plan between the active CIRT components and Business Units/Agency to report other similar issues.

The incident will remain open until a full recovery is declared by the CISO. Once a full recovery is declared, the CIRT team will move into the Post Incident Report and Review phase.

A.6. Post Incident Review Phase

Convene a meeting with all activated CIRT members that participated in the incident to:

- Review the incident
- Answer any questions
- Determine the effectiveness of the approach to Incident Response
- Recommend updates or changes to the Incident Response Plan
- Assign responsibilities and implementation timelines for updates or changes to the IRP
- Schedule any classes for re-education on security topics in the incident

The meeting minutes, list of participants, and all assigned tasks should be recorded in the incident evidence. This should also include any status reports, analysis reports, and the final incident report.

APPENDIX B. CUSTOMER IRP CIRT Contact LIST

CUSTOMER CIRT CONTACT LIST				
CIRT ROLE/TITLE	**Primary Contact**	**Primary Contact Information**	**Alternate Contact**	**Alternate Contact Information**
CHIEF INFORMATION SECURITY OFFICER				
Primary				
Backup				
INCIDENT RESPONSE MANAGER				
Team Leader				
Team Leader Backup				
INCIDENT RESPONSE HANDLER				
Team Leader				
Team Leader Backup				
TACTICAL TEAM MEMBERS				
Team Leader				
Team Leader Backup				
Team Member				
Team Member				
IT TECHNICIANS				
Primary				
Backup				

CUSTOMER CIRT CONTACT LIST				
CIRT ROLE/TITLE	**Primary Contact**	**Primary Contact Information**	**Alternate Contact**	**Alternate Contact Information**
FORENSIC ANALYST				
Team Leader				
Team Leader Backup				
Team Member				
Team Member				
SYSTEM OWNER				
Primary				
Backup				
SYSTEM OWNER				
Primary				
Backup				
ISO SECURITY LEAD				
Primary				
Backup				
AGENCY HUMAN RESOURCES				
Primary				
Backup				
INCIDENT REPORTER				
Team Leader				

CUSTOMER CIRT CONTACT LIST				
CIRT ROLE/TITLE	**Primary Contact**	**Primary Contact Information**	**Alternate Contact**	**Alternate Contact Information**
Team Leader Backup				
Team Member				
Team Member				
NCC				
Team Leader				
Team Leader Backup				
Team Member				
Team Member				
LAW ENFORCEMENT				
Primary				
Backup				
LEGAL COUNCIL				
Primary				
Backup				
PRESIDENTS/ELECTED OFFICAL OFFICE				
Primary				
Backup				
SUBJECT MATTER EXPERT				
Primary				

CUSTOMER CIRT CONTACT LIST				
CIRT ROLE/TITLE	**Primary Contact**	**Primary Contact Information**	**Alternate Contact**	**Alternate Contact Information**
Backup				
SUPPORT/HELP DESK				
Primary				
Backup				
EXECUTIVE MANAGER				
Primary				
Backup				
COOP/BCP/DR				
Primary				
Backup				
PHYSICAL SECURITY				
Primary				
Backup				

APPENDIX C. Revision History

DATE	VERSION	DESCRIPTION	AUTHOR